Forcepoint DLP Predefined Policies and Classifiers

For your convenience, Forcepoint DLP includes hundreds of predefined policies and content classifiers.

- Predefined policies help administrators quickly and easily define what type of content is considered a security breach at their organization.

  While choosing a policy or policy category, some items are set “off” by default. They can be activated individually in the Forcepoint Security Manager.

  - *Data Loss Prevention policies*, page 2
  - *Discovery policies*, page 114
- Predefined classifiers can be used to detect events and threats involving secured data.

  This article provides a list of all the predefined content classifiers that Forcepoint DLP provides for detecting events and threats involving secured data. This includes:

  - *File-type classifiers*
  - *Script classifiers*
  - *Dictionaries*
  - *Pattern classifiers*

The predefined policies and classifiers are constantly being updated and improved. See Updating Predefined Policies and Classifiers for instructions on keeping policies and classifiers current.

Data Loss Prevention policies

Use the predefined data loss prevention policies to detect sensitive content, compliance violations, and data theft.

For acceptable use policies, see:

- *Acceptable Use*, page 3

The content protection policies fall into several categories:

- *Company Confidential and Intellectual Property (IP)*, page 4
- *Credit Cards*, page 9
- *Financial Data*, page 11
- *Protected Health Information (PHI)*, page 18
- *Personally Identifiable Information (PII)*, page 21

The regulation, compliance, and standards policies are categorized as follows:

- *EU General Data Protection Regulation (GDPR)*, page 39
- *Financial Regulations*, page 41
- *Payment Card Industry (PCI)*, page 44
- *National Privacy Regulations*, page 45
- *US and Canada Federal Regulations*, page 93

Data theft risk indicator policies are categorized as follows:

- *Employee Discontent*, page 109
- *Indicators of Compromise*, page 107
- *Suspicious User Activity*, page 105

The Web DLP, Email DLP, and Mobile DLP “quick policies” include the PCI policy, PHI policies, and PII policies listed in this document (including financial policies). The quick policies include additional policies as well. See the following for more information:

- *Web DLP policy*, page 111
- *Email DLP policy*, page 112
- *Mobile DLP policy*, page 113

Acceptable Use

The following predefined policies are available for the detection of possible acceptable use transgressions:

- Acceptable Use - Indecent Images

  Policy for detection of indecent images using image analysis. The rule for this policy is:

  - Non Acceptable Use - Indecent Images as Attachments
- Acceptable Use - Obscenities & Racism

  Policy for detection of offensive or inappropriate terms (non-editable). The rules for this policy are:

  - Non Acceptable Use - In file names - inappropriate
  - Non Acceptable Use - In file names - medium
  - Non Acceptable Use - In file names - offensive
  - Non Acceptable Use - inappropriate
  - Non Acceptable Use - medium
  - Non Acceptable Use - offensive
- Cyber Bullying and Self-Destructive Patterns

  Policy for the detection of expressions that are indicative of cyber bullying or self-destructive patterns. This policy functions on the web channel (HTTP/HTTPS) only. The rules for this policy are:

  - Cyber Bullying (Wide)
  - Cyber Bullying (Default)
  - Cyber Bullying (Narrow)
  - Suicidal thoughts (Wide)
  - Suicidal thoughts (Narrow)
- Israel Acceptable Use

  Policy for detection of Israel offensive or inappropriate terms. The rules for this policy include:

  - Israel Non Acceptable Use: All In One
  - Israel Non Acceptable Use: Hebrew
  - Israel Non Acceptable Use: Russian
  - Israel Non Acceptable Use: Arabic
  - Israel Non Acceptable Use: Iraqi

Content Protection

Forcepoint DLP includes the following types of content protection policies:

Company Confidential and Intellectual Property (IP)

The following predefined policies are available for the detection of company confidential or intellectual property data:

- Bids and Tenders

  Policy for detecting bids, proposals, and tenders, such as responses to request for proposal (RFP) and invitation for bids (IFB) documents.

  - Bids and Tenders (Wide)
  - Bids and Tenders (Default)
  - Bids and Tenders (Narrow)
- Business and Technical Drawing Files

  Policy for detection of business and technical drawing file types. The rules for this policy are:

  - Business and Technical Drawing Files: Abaqus ODB File
  - Business and Technical Drawing Files: Autodesk Design Web File
  - Business and Technical Drawing Files: Autodesk Maya Binary File
  - Business and Technical Drawing Files: Autodesk Maya Textual File
  - Business and Technical Drawing Files: Catia File
  - Business and Technical Drawing Files: Corel Draw File
  - Business and Technical Drawing Files: DWG File
  - Business and Technical Drawing Files: DXF Binary File
  - Business and Technical Drawing Files: DXF Textual File
  - Business and Technical Drawing Files: IGS Textual File
  - Business and Technical Drawing Files: JT File
  - Business and Technical Drawing Files: Microsoft Visio File
  - Business and Technical Drawing Files: Nastran OP2 File
  - Business and Technical Drawing Files: PTC Creo ASM File
  - Business and Technical Drawing Files: PTC Creo DRW File

- Business and Technical Drawing Files: PTC Creo FRM File
- Business and Technical Drawing Files: PTC Creo PRT File
- Business and Technical Drawing Files: Siemens NX PRT File
- Business and Technical Drawing Files: SolidWorks File
- Business and Technical Drawing Files: STL Binary File
- Business and Technical Drawing Files: STL Textual File
- Business and Technical Drawing Files: STP File
- Business and Technical Drawing Files: WHIP File
  - Business and Technical Drawing Files: X_T Textual File

- Confidential Warning

  Policy for detection of sensitive text in the header or footer of a document. The rules for this policy are:

  - Confidential in Header or Footer
  - Key Phrases in Header or Footer
  - Dictionary Phrases in Header or Footer
  - Proprietary in Header or Footer

- Confidential Warning (Arabic)

  The policy detect secret or confidential documents by identifying “confidential” terms in English or Arabic, such as “Confidential” or “سري“, in the Header or the Footer of Office documents. The rule for this policy is:

  - Confidential Arabic in Header or Footer

- Digitally Signed PDF Files

  Policy for detection of digitally signed PDF files. The rule for this policy is:

  - Digitally Signed PDF File (Native)

- Energy

  Policies for detection of sensitive data in the Oil and Gas industry and, in particular, information pertaining to oil prospecting and drilling.

  - Petroleum and Gas-Sensitive Information

    Detect leakage of sensitive data in the Oil and Gas industry and, in particular, information pertaining to oil prospecting and drilling. The rules for this policy are:

    - Petroleum and Gas-Sensitive Information: CAD Files: DWG File
    - Petroleum and Gas-Sensitive Information: CAD Files: DXF Binary File
    - Petroleum and Gas-Sensitive Information: CAD Files: DXF Textual File
    - Petroleum and Gas-Sensitive Information: CAD Files: IGS Textual File
    - Petroleum and Gas-Sensitive Information: CAD Files: JT File
    - Petroleum and Gas-Sensitive Information: CAD Files: PTC Creo ASM File
    - Petroleum and Gas-Sensitive Information: CAD Files: PTC Creo DRW File

        - Petroleum and Gas-Sensitive Information: CAD Files: PTC Creo FRM File
        - Petroleum and Gas-Sensitive Information: CAD Files: PTC Creo PRT File
        - Petroleum and Gas-Sensitive Information: CAD Files: SolidWorks File
        - Petroleum and Gas-Sensitive Information: CAD Files: STL Binary File
        - Petroleum and Gas-Sensitive Information: CAD Files: STL Textual File
        - Petroleum and Gas-Sensitive Information: CAD Files: STP File
        - Petroleum and Gas-Sensitive Information: CAD Files: WHIP File
        - Petroleum and Gas-Sensitive Information: CAD Files: X_T Textual File
        - Petroleum and Gas-Sensitive Information: Disclaimer
        - Petroleum and Gas-Sensitive Information: Form 567
        - Petroleum and Gas-Sensitive Information: Form 715
        - Petroleum and Gas-Sensitive Information: Latitude-Longitude Location Coordinates
        - Petroleum and Gas-Sensitive Information: Logs and Survey Reports
        - Petroleum and Gas-Sensitive Information: Microsoft Visio
        - Petroleum and Gas-Sensitive Information: Petroleum File Extension
        - Petroleum and Gas-Sensitive Information: Pipeline Flow Diagram
        - Petroleum and Gas-Sensitive Information: Prospecting Related Term
    - Smart Power Grids / SCADA

      Policy for promoting protection of sensitive information pertaining smart power grids and supervisory control and data acquisition (SCADA) systems. The rules for this policy are:

        - Smart Power Grids: Confidential in Header or Footer
        - Smart Power Grids: Proprietary in Header or Footer
        - Smart Power Grids: C family or Java (default)
        - Smart Power Grids: C family or Java (wide)
        - Smart Power Grids: Software Design Documents with SCADA terms
        - Smart Power Grids: CAD Files: STL Textual File
        - Smart Power Grids: CAD Files: STL Binary File
        - Smart Power Grids: CAD Files: STP File
        - Smart Power Grids: CAD Files: IGS text Format
        - Smart Power Grids: CAD Files: X_T text Format
        - Smart Power Grids: Executable or Link Library
        - Smart Power Grids: Microsoft Visio File
        - Smart Power Grids: Python (Default)
        - Smart Power Grids: Python (Wide)
        - Smart Power Grids: XML with SCADA terms
        - Smart Power Grids: Spreadsheets with SCADA terms
- License Keys

  Policy to identify Microsoft license keys. The policy helps mitigate software piracy and unauthorized usage of corporate assets. The rule for this policy is:

    - Microsoft license keys

- Media

  Policies for detection of sensitive data in the Media industry.

  - Movie manuscripts

    Policy for detection of movie and TV scripts dissemination. The rule for this policy is:

    - Movie and TV Manuscripts
- Mergers and acquisitions

  Policy for detection of information suspected to be related to mergers and acquisitions. The rules for this policy are:

  - Mergers and Acquisitions information
  - Mergers and Acquisitions information (narrow)
- Mergers and Acquisitions for Discovery

  Policy for detection of information suspected to be related to mergers and acquisitions. The rule for this policy is:

  - Mergers and Acquisitions information
- Network Security Information

  Policy for detection of network security documents and network diagrams. This policy detects network diagrams by searching for IP addresses, MAC addresses and various terms common to such documents. In order to achieve complete coverage, first 2 rules and one of the MAC address rules must be selected. The rules for this policy are:

  - Network Information and Security
  - Network Information and Security
  - MAC Addresses (Wide)
  - MAC Addresses (Default)
  - MAC Addresses (narrow)
- Patents

  Policy for detection of patents and patent applications. The rule for this policy is:

  - Patents detection
- Project Documents

  Policy for detection of project document in traffic. This may cause false positives. The rule for this policy is:

  - Project Document
- Security Software Files

  Policy for detection of security software files. The rule for this policy is:

  - Security Software Files: Splunk Enterprise Security Event Log
- Software Source Code and Design

  Policies for detection of source codes and software design documents.

  - Software Design Documents

    Policy for detection of software design documents in traffic. The rules for this policy are:

- Software Design Documents

- Software Source Code

  Policy for detection of software source code. The rule for this policy is:

  - Software Source Code: C family or Java (Default)
  - Software Source Code: C family or Java (Wide)
  - Software Source Code: C family or Java (By file extension)
  - Software Source Code: F# Source (By content)
  - Software Source Code: F# Source (By file extension)
  - Software Source Code: Perl Source (By content)
  - Software Source Code: Perl Source (By file extension)
  - Software Source Code: Python (Default)
  - Software Source Code: Python (Wide)
  - Software Source Code: x86 Assembly Source Code

- SPICE Source Code

  Policy for detection of integrated circuits design source code in SPICE (Simulation Program with Integrated Circuits Emphasis). This may cause false positives. the rules for this policy are:

  - SPICE Source code (Berkeley version)
  - SPICE Source code

- SQL Queries Detection

  Policy for detection of SQL and Oracle queries and database. This may cause false positives. the rules for this policy are:

  - SQL Detection (Wide)
  - SQL Detection (Default)
  - SQL Detection (Narrow)

- Verilog Source Code

  Policy for detection of Verilog source code dissemination. This policy is comprised of 2 rules, each covering a different aspect of the detected texts. In order to achieve complete coverage, all rules must be selected. This may cause false positives. The rules for this policy are:

  - Verilog Source code 1
  - Verilog Source code 2

- VHDL Source Code

  Policy for detection of source code dissemination in VHDL, used mainly for hardware design. This may cause false positives. The rule for this policy is:

  - VHDL Source Code

- Visual Basic Source Code

  Policy for detection of Visual Basic source code. This may produce a false positive. The rules for this policy are:

  - Visual Basic Source Code (Wide)
  - Visual Basic Source Code (Default)
  - Visual Basic Source Code (Narrow)

- Strategic Business Documents

  Policy for detection of documents of prime strategic value, such as business and marketing plans. The rule for this policy is:

  - Strategic Business Documents (Wide)
  - Strategic Business Documents (Narrow)
  - Strategic Business Documents (Default)
- Telecom

  Policies for detection of sensitive data in the Telecom industry.

  - Call Detail Record

    Policy for detection of Call Detail Records (CDRs) in traffic. The rule for this policy is:

    - CDR: Suspected Call details rows
    - CDR: Suspected Call details headers
  - IMEI

    Policy for detection of serial (IMEI) numbers of cell phones. The International Mobile Equipment Identity (IMEI) is a number unique to every GSM and UMTS and iDEN mobile phone as well as some satellite phones. It is usually found printed on the phone underneath the battery. The rule for this policy is:

    - IMEI: Wide
    - IMEI: Default
    - IMEI: with proximity
  - Location Coordinates

    Policy for detection of location coordinates. The rule for this policy is:

    - Latitude-Longitude Location Coordinates
    - UTM Location Coordinates

Credit Cards

The following predefined policies are available for the detection of credit card information:

- Credit Card Magnetic Strips

  Policy for detection of electronic data from credit card strips. The rules for this policy are:

  - Credit Card Magnetic Strips
  - Credit Card Magnetic Strips: Track 1
  - Credit Card Magnetic Strips: Track 2
  - Credit Card Magnetic Strips: Track 3
- Credit Cards

  Policy for detection of credit card numbers. The rules for this policy are:

- All CCN for Printer Agent: All in one
- Credit Cards: American Express
- Credit Cards: Bancard
- Credit Cards: Diners
- Credit Cards: Discover
- Credit Cards: EnRoute
- Credit Cards: JCB 1st Format
- Credit Cards: JCB 2nd Format
- Credit Cards: Maestro, Switch or Solo
- Credit Cards: MasterCard
- Credit Cards: RuPay
- Credit Cards: Visa
- Credit Cards: Visa 13 Digits (Obsolete)
- Credit Cards: Credit Card Number (Wide Minus Default)
- Credit Cards: Credit Card Number (Wide)
- Credit Cards: Credit Card Number (Default)
- Credit Cards: Credit Card Number (Narrow)
- Credit Cards: User-Defined IIN (Wide)
- Credit Cards: User-Defined IIN (Default)
- Credit Cards: User-Defined IIN (Narrow)

- Credit Cards for Printer Agent

  Policy for detection of credit card numbers, obtained from using the printer agent OCR. The rules take into account possible errors that may be induced by the OCR software. The rule for this policy is:

  - All CCN for Printer Agent: All in one

- European Credit Cards

  All Policy for detection of credit card numbers prevalent in Europe. The rule for this policy is:

  - European Credit Cards: All Credit Cards

- Israeli Credit Cards

  Policy for detection of credit card numbers prevalent in Israel. The rule for this policy is:

  - CCN Israel: All Credit Cards
  - CCN Israel: All Credit Cards (Wide)
  - CCN Israel: American Express
  - CCN Israel: MasterCard
  - CCN Israel: Visa
  - CCN Israel: Diners
  - CCN Israel: Discover

- CCN Israel: IsraCard (Default)
- CCN Israel: IsraCard (Wide)

- Japanese Credit Cards

  Policy for detection of credit card numbers prevalent in Japan. The rule for this policy is:

  - Japanese Credit Cards: All Credit Cards

- US Credit Cards

  Policy for detection of credit card numbers prevalent in the US. The rule for this policy is:

  - US Credit Cards: All Credit Cards

Financial Data

The following predefined policies are available for the detection of financial information:

- 401(k) and 403(b) forms

  Policy for detection of 401(k) and 403(b) form that contain private information of employees. The rules for this policy are:

  - 401(k) form (Wide)
  - 401(k) form (Default)
  - 401(k) form (Narrow)
  - 403(b) form (Default)
  - 403(b) form (Wide)
  - 403(b) form (Narrow)

- Austria Finance

  Policy for detection of Austrian financial information. The rules for this policy are:

  - Austria Finance: Austrian IBAN (default)
  - Austria Finance: Austrian IBAN (wide)

- Belgium Finance

  Policy for detection of Belgian financial information. The rules for this policy are:

  - Belgium Finance: Belgian IBAN (default)
  - Belgium Finance: Belgian IBAN (wide)

- Brazil Finance

  Policy for detection of Brazilian financial information. The rules for this policy are:

  - Brazil Finance: Brazilian IBAN (default)
  - Brazil Finance: Brazilian IBAN (wide)

- Bulgaria Finance

Policy for detection of Bulgarian financial information. The rules for this policy are:

- Bulgaria Finance: Bulgarian IBAN (Default)
- Bulgaria Finance: Bulgarian IBAN (Wide)

- Croatia Finance

  Policy for detection of Croatian financial information. The rules for this policy are:

  - Croatia Finance: Croatian IBAN (Default)
  - Croatia Finance: Croatian IBAN (Wide)
- Cyprus Finance

  Policy for detection of Cypriot financial information. The rules for this policy are:

  - Cyprus Finance: Cypriot IBAN (Default)
  - Cyprus Finance: Cypriot IBAN (Wide)
- Czech Republic Finance

  Policy for detection of Czech financial information. The rules for this policy are:

  - Czech Republic Finance: Czech IBAN (default)
  - Czech Republic Finance: Czech IBAN (wide)
- Denmark Finance

  Policy for detection of Danish financial information. The rules for this policy are:

  - Danish IBANRule (Default)
  - Denmark Finance: Danish IBAN (wide)
- Estonia Finance

  Policy for detection of Estonian financial information. The rules for this policy are:

  - Estonia Finance: Estonian IBAN (default)
  - Estonia Finance: Estonian IBAN (wide)
- Financial Information

  Policy for detection of general, personal, and investment financial information in traffic. The rules for this policy are:

  - Financial Information -Personal
  - Financial Information -Investment
  - Financial Information -General
- Financial Information in Chinese

  Policy for detection of financial information in Chinese. The rules for this policy are:

  - Financial Information in Chinese (Wide)
  - Financial Information in Chinese (Default)
  - Financial Information in Chinese (Narrow)
- Finland Finance

Policy for detection of Finnish financial information. The rules for this policy are:

- Finland Finance: Finnish IBAN (default)
- Finland Finance: Finnish IBAN (wide)

- France Finance

  Policy for detection of French financial information. The rules for this policy are:

  - France Finance: French IBAN (default)
  - France Finance: French IBAN (wide)
- Germany Finance

  Policy for detection of German financial information. The rules for this policy are:

  - Germany Finance: German IBAN (default)
  - Germany Finance: German IBAN (wide)
- Greece Finance

  Policy for detection of Greek financial information. The rules for this policy are:

  - Greece Finance: Greece IBAN (default)
  - Greece Finance: Greece IBAN (wide)
- Hungary Finance

  Policy for detection of Hungarian financial information. The rules for this policy are:

  - Hungary Finance: Hungarian IBAN (default)
  - Hungary Finance: Hungarian IBAN (wide)
- Iceland Finance

  Policy for detection of Icelandic financial information. The rules for this policy are:

  - Iceland Finance: Icelandic IBAN (default)
  - Iceland Finance: Icelandic IBAN (wide)
- Ireland Finance

  Policy for detection of Irish financial information. The rules for this policy are:

  - Ireland Finance: Irish IBAN (default)
  - Ireland Finance: Irish IBAN (wide)
  - Ireland Finance: Irish Bank Account
- IRS Tax Forms

  Policy for detection of IRS Tax Forms; for example, Form W-2, Form W-4, and Form 1040. The rules for this policy are:

  - IRS Tax Forms: Form 1040 and Form 1040A (Wide)
  - IRS Tax Forms: Form 1040 and Form 1040A (Default)
  - IRS Tax Forms: Form 1040 and Form 1040A (Narrow)
  - IRS Tax Forms: Form 1040EZ (Wide)
  - IRS Tax Forms: Form 1040EZ (Default)
  - IRS Tax Forms: Form 1040EZ (Narrow)

- IRS Tax Forms: Form W-2
- IRS Tax Forms: Form W-4 (Wide)
- IRS Tax Forms: Form W-4 (Default)
- IRS Tax Forms: Form W-4 (Narrow)
- IRS Tax Forms: Form W-4P (Wide)
- IRS Tax Forms: Form W-4P (Default)
- IRS Tax Forms: Form W-4P (Narrow)
- IRS Tax Forms: Form W-4V (Wide)
- IRS Tax Forms: Form W-4V (Default)
- IRS Tax Forms: Form W-4V (Narrow)
- IRS Tax Forms: Form W-9 (Wide)
- IRS Tax Forms: Form W-9 (Default)
- IRS Tax Forms: Form W-9 (Narrow)
- IRS Tax Forms: Form W-9S (Wide)
- IRS Tax Forms: Form W-9S (Default)
- IRS Tax Forms: Form W-9S (Narrow)

- ISIN and CUSIP

  Policy for detection of International Securities Identification Number (ISIN), which uniquely identifies a security. The ISIN code is a 12-character alphanumerical code that serves as uniform identification of a security at trading and settlement. The rules for this policy are:

  - ISIN number - wide
  - ISIN number - default
  - CUSIP Numbers (default)
  - CUSIP Numbers (wide)

- Israeli Bank Accounts

  Policy for identifying Israeli bank account numbers in traffic. The rules for this policy are:

  - IL BANK: General Bank Account Numbers
  - IL BANK: Leumi Bank Account Numbers
  - IL BANK: Leumi Bank Account Numbers no support
  - IL BANK: Poalim Bank Account Numbers
  - IL BANK: Discount Bank Account Numbers
  - IL BANK: Mizrahi Bank Account Numbers
  - IL BANK: BenLeumi Bank Account Numbers
  - IL BANK: HaDoar Bank Account Numbers

- Italy Finance

  Policy for detection of Italian financial information. The rules for this policy are:

  - Italy Finance: Italian IBAN (default)

- Italy Finance: Italian IBAN (wide)

- Kazakhstan Finance

  Policy for detection of Kazakh financial information. The rules for this policy are:

  - Kazakhstan Finance: Kazakh IBAN (default)
  - Kazakhstan Finance: Kazakh IBAN (wide)

- Latvia Finance

  Policy for detection of Latvian financial information. The rules for this policy are:

  - Latvia Finance: Latvian IBAN (Default)
  - Latvia Finance: Latvian IBAN (Wide)

- Lithuania Finance

  Policy for detection of Lithuanian financial information. The rules for this policy are:

  - Lithuania Finance: Lithuanian IBAN (Default)
  - Lithuania Finance: Lithuanian IBAN (Wide)

- Luxembourg Finance

  Policy for detection of Luxembourgian financial information. The rules for this policy are:

  - Luxembourg Finance: Luxembourgian IBAN (default)
  - Luxembourg Finance: Luxembourgian IBAN (wide)

- Malta Finance

  Policy for detection of Maltese financial information. The rules for this policy are:

  - Malta Finance: Maltese IBAN (Default)
  - Malta Finance: Maltese IBAN (Wide)

- Mexico Finance

  Policy for detection of Mexican financial information. The rules for this policy are:

  - Mexico Finance: Standardized Bank Code (CLABE) (Wide)
  - Mexico Finance: Standardized Bank Code (CLABE) (Default)

- Netherlands Finance

  Policy for identifying Dutch financial information. The rules for this policy are:

  - Netherlands Finance: Netherlands IBAN (default)
  - Netherlands Finance: Netherlands IBAN (wide)

- Norway Finance

  Policy for identifying Norwegian financial information. The rules for this policy are:

  - Norway Finance: Norwegian IBAN (default)
  - Norway Finance: Norwegian IBAN (wide)

- People’s Republic of China Finance

  Policy for detection of PRC financial information. The rules for this policy are

- People’s Republic of China Finance: Union Pay Credit Card (wide)
- People’s Republic of China Finance: Union Pay Credit Card (default)
- People’s Republic of China Finance: Union Pay Credit Card (narrow)
- People’s Republic of China Finance: Financial cards Track1
- People’s Republic of China Finance: Financial cards Track2 rule for detecting bank card magnetic stripe Track2
- People’s Republic of China Finance: Financial cards Track3
- People’s Republic of China Finance: Business Registration Number - 15 digits (wide)
- People’s Republic of China Finance: Business Registration Number - 15 digits (default)
- People’s Republic of China Finance: Business Registration Number - 15 digits (narrow)
- People’s Republic of China Finance: Credit Card (Wide)
- People’s Republic of China Finance: Credit Card (Default)
- People’s Republic of China Finance: Credit Card (Narrow)

- Poland Finance

  Policy for detection of Polish financial information. The rules for this policy are:
  - Poland Finance: Polish IBAN (wide)
  - Poland Finance: Polish IBAN (default)
  - Poland Finance: IBAN and Name
- Portugal Finance

  Policy for detection of Portuguese financial information. The rules for this policy are:
  - Portugal Finance: Portuguese IBAN (Default)
  - Portugal Finance: Portuguese IBAN (Wide)
- Pricing Information

  Policy for detection of pricing information and pricelists in traffic. The rules for this policy are:
  - Pricing Information 1
  - Pricing Information 2
  - Pricing Information 3
- Qatar Finance

  Policy for detection of Qatari financial information. The rules for this policy are:
  - Qatar Finance: Qatari IBAN (default)
  - Qatar Finance: Qatari IBAN (wide)
- Romania Finance

  Policy for detection of Romanian financial information. The rules for this policy are:
  - Romania Finance: Romanian IBAN (default)

- Romania Finance: Romanian IBAN (wide)

- RTN/ABA Numbers

  Policy for detection of Routing Transit Numbers (RTN), also known as American Bankers Association (ABA) numbers. RTN numbers are nine digit bank codes, used in the United States to identify, for example, which financial institution checks and banknotes are drawn upon. The rules for this policy are:

  - RTN/ABA: Wide
  - RTN/ABA: Default
  - RTN/ABA: Narrow

- Saudi Arabia Finance

  Policy for detection of Saudi Arabia financial information. The rules for this policy are:

  - Saudi Arabia Finance: Saudi Arabia IBAN (default)
  - Saudi Arabia Finance: Saudi Arabia IBAN (wide)

- Slovakia Finance

  Policy for detection of Slovak financial information. The rules for this policy are:

  - Slovakia Finance: Slovak IBAN (default)
  - Slovakia Finance: Slovak IBAN (wide)

- Slovenia Finance

  Policy for detection of Slovenian financial information. The rules for this policy are:

  - Slovenia Finance: Slovene IBAN (Default)
  - Slovenia Finance: Slovene IBAN (Wide)

- Spain Finance

  Policy for detection of Spanish financial information. The rules for this policy are:

  - Spanish IBAN rule for detecting Spanish IBANs (default)
  - Spanish IBAN rule for detecting Spanish IBANs (wide)

- Sweden Finance

  Policy for detection of Swedish financial information. The rules for this policy are:

  - Sweden Finance: Swedish IBAN (default)
  - Sweden Finance: Swedish IBAN (wide)

- Switzerland Finance

  Policy for detection of Swiss financial information. The rules for this policy are:

  - Switzerland Finance: Swiss IBAN (default)
  - Switzerland Finance: Swiss IBAN (wide)

- Turkey Finance

  Policy for detection of Turkish financial information. The rules for this policy are:

  - Turkey Finance: Turkish IBAN (Default)
  - Turkey Finance: Turkish IBAN (Wide)

- Turkey Finance: Turkish Tax IDs (Wide)
- Turkey Finance: Turkish Tax IDs (Default)

- UK Finance

  Policy for detection of UK financial information. The rules for this policy are:
  - UK Finance: UK IBAN (default)
  - UK Finance: UK IBAN (wide)
- United Arab Emirates Finance

  Policy for detection of Emirati financial information. The rules for this policy are:
  - United Arab Emirates Finance: Emirati IBAN (default)
  - United Arab Emirates Finance: Emirati IBAN (wide)

Protected Health Information (PHI)

- Australian PHI

  Policy for detection of protected health information for Australian citizens. The rules for this policy are:
  - Australia PHI: Australia Medicare and Sensitive Disease or Drug
  - Australia PHI: Australia Medicare and Common Medical Condition
  - Australia PHI: DICOM
  - Australia PHI: SPSS Text File
- Health Data

  Policy for detection of data types pertaining to medical conditions, drugs etc. The rules for this policy are:
  - Health Data: Credit cards and Common Medical Condition
  - Health Data: Credit Card and Sensitive Disease or Drug
  - Health Data: DICOM
  - Health Data: DNA Profile (Default)
  - Health Data: DNA Profile (Narrow)
  - Health Data: DOB and Name
  - Health Data: ICD9 Code
  - Health Data: ICD9 Code and Description
  - Health Data: ICD9 Code and Name
  - Health Data: ICD9 Description and Name
  - Health Data: ICD10 Code
  - Health Data: ICD10 Code and Description
  - Health Data: ICD10 Code and Name
  - Health Data: ICD10 Descriptions and Name
  - Health Data: Medical Form (Default)

- Health Data: Medical Form (Narrow)
- Health Data: Medical Form (Wide)
- Health Data: Name and Common Medical Condition (Default)
- Health Data: Name and Common Medical Condition (Narrow)
- Health Data: Name and Sensitive Disease or Drug (Default)
- Health Data: Name and Sensitive Disease or Drug (Narrow)
- Health Data: NDC Number (Wide)
- Health Data: NDC Number (Default)
- Health Data: NDC Number (Narrow)
- Health Data: SPSS Text File

- Israel PHI

  Policy for detection of protected health information for Israeli citizens, to promote compliance with Israeli privacy rules and Israeli patients rights law of 1996. The rules for this policy are:

  - Israel PHI: DICOM
  - Israel PHI: Identity Number and General Medical Information
  - Israel PHI: Identity Number and Sensitive Medical Information
  - Israel PHI: Name and General Medical Information
  - Israel PHI: Name and Sensitive Medical Information
  - Israel PHI: SPSS Text File

- Italy PHI

  Policy for detection of protected health information for Italy citizens. The rules for this policy are:

  - Italy PHI: Codice Fiscale and Health Information
  - Italy PHI: DICOM
  - Italy PHI: Name and Health Information
  - Italy PHI: SPSS Text File

- Norway PHI

  Policy for detection of protected health information for Norwegian citizens. The rules for this policy are:

  - Norway PHI: DICOM
  - Norway PHI: ICD10 Code
  - Norway PHI: ICD10 Code and Description
  - Norway PHI: ICD10 Code and First Name
  - Norway PHI: ICD10 Code and Full Name
  - Norway PHI: ICD10 Code and Last Name
  - Norway PHI: ICD10 Code and Personal number
  - Norway PHI: ICD10 Code and PIN
  - Norway PHI: ICD10 Description

- Norway PHI: Name and Health Information
- Norway PHI: Personal Number and Health Information
- Norway PHI: SPSS Text File

- Sweden PHI

  A policy for detection of protected health information (PHI) of Swedish citizens and residents. The policy comprises rules for detection of Health information and Medical Conditions (in Swedish or English), in proximity to personally identifiable information such as personal number (personnummer), or name. The rules for this policy are:

  - Sweden PHI: DICOM
  - Sweden PHI: DNA Profile
  - Sweden PHI: ICD10 Code
  - Sweden PHI: ICD10 Code and Description
  - Sweden PHI: ICD10 Description
  - Sweden PHI: ICD10 Code and Name (Wide)
  - Sweden PHI: ICD10 Code and Name (Default)
  - Sweden PHI: ICD10 Code and Name (Narrow)
  - Sweden PHI: ICD10 Code and Personal Number
  - Sweden PHI: Name and Health Information
  - Sweden PHI: Name and Sensitive Disease or Drug
  - Sweden PHI: Personal Number and Health Information
  - Sweden PHI: Personal Number and Sensitive Disease or Drug
  - Sweden PHI: SPSS Text File

- UK PHI

  Policy for detection of UK protected health information.The rules for this policy are

  - UK PHI: DICOM
  - UK PHI: NHS Number (Wide)
  - UK PHI: NHS Number (Default)
  - UK PHI: NHS Number (Narrow)
  - UK PHI: SPSS Text File

- US PHI

  A policy for detection of protected health information of US citizens. The rules for this policy are

  - US PHI: DICOM
  - US PHI: Medical Form (Wide)
  - US PHI: Medical Form (Default)
  - US PHI: Medical Form (Narrow)
  - US PHI: Name and Common Medical Condition (Default)
  - US PHI: Name and Common Medical Condition (Narrow)

- US PHI: Name and HICN
- US PHI: Name and Sensitive Disease or Drug (Default)
- US PHI: Name and Sensitive Disease or Drug (Narrow)
- US PHI: SPSS Text File
- US PHI: SSN and Sensitive Disease or Drug
- US PHI: SSN and Common Medical Condition

Personally Identifiable Information (PII)

The following predefined policies are available for the detection of private information:

- Australia PII

  Policy for detection of Australian private information. The rules for this policy are:

  - Australia PII: Credit File (Wide)
  - Australia PII: Credit File (Default)
  - Australia PII: Credit File (Narrow)
  - Australia PII: Driver License Number and Name
  - Australia PII: Email Address and Password (Wide)
  - Australia PII: Email Address and Password (Default)
  - Australia PII: Tax File Number (Wide)
  - Australia PII: Tax File Number (Default)
- Austria PII

  Policy for detection of Austrian private information. The rules for this policy are:

  - Austria PII: CCN and Name
  - Austria PII: Crime and Name
  - Austria PII: Email Address and Password (Wide)
  - Austria PII: Email Address and Password (Default)
  - Austria PII: Ethnicity and Name
  - Austria PII: Sensitive Disease and Name
  - Austria PII: Social Security Number (Wide)
  - Austria PII: Social Security Number (Default)
  - Austria PII: Social Security Number and Name (Wide)
  - Austria PII: Social Security Number and Name (Default)
- Belgium PII

  Policy for detection of Belgian private information. The rules for this policy are:

  - Belgium PII: Email Address and Password (Wide)
  - Belgium PII: Email Address and Password (Default)

- Belgium PII: ID Card Number
- Belgium PII: Name and ID Card Number (Wide)
- Belgium PII: Name and ID Card Number (Default)
- Belgium PII: Name and Passport Number (Wide)
- Belgium PII: Name and Passport Number (Default)
- Belgium PII: Passport Number

- Biometric Files

  Policy for detection of biometric files. The rules for this policy are:

  - Biometric Files: NIEM-Conformant XML
  - Biometric Files: OASIS XML Common Biometric Format (XCBF)

- Bosnia and Herzegovina PII

  Policy for detection of Unique Master Citizen Numbers. The rules for this policy are:

  - Bosnia and Herzegovina PII: Unique Master Citizen Number (Wide)
  - Bosnia and Herzegovina PII: Unique Master Citizen Number (Default)

- Brazil PII

  Policy for detection of Brazilian private information. The rules for this policy are:

  - Brazil PII: Name and CPF
  - Brazil PII: Name and Sensitive Disease
  - Brazil PII: CPF and Sensitive Disease
  - Brazil PII: Email Address and Password (Wide)
  - Brazil PII: Email Address and Password (Default)
  - Brazil PII: Identity Card Number (Default)
  - Brazil PII: Identity Card Number (Narrow)
  - Brazil PII: National Register of Legal Entities Number (Wide)
  - Brazil PII: National Register of Legal Entities Number (Default)

- Bulgaria PII

  Policy for detection of Bulgarian private information. The rules for this policy are:

  - Bulgaria PII: Unified Civil Number (Wide)
  - Bulgaria PII: Unified Civil Number (Default)

- Canada PII

  Policy for detection of Canadian private information. The rules for this policy are:

  - Canada PII: Credit File (Wide)
  - Canada PII: Credit File (Default)
  - Canada PII: Credit File (Narrow)
  - Canada PII: Email Address and Password (Wide)
  - Canada PII: Email Address and Password (Default)
  - Canada PII: SIN

- Canada PII: SIN and Name (Default)
- Canada PII: SIN and Name (Narrow)
- Canada PII: Name and Alberta Driver's License Number
- Canada PII: Name and British Columbia Driver's License Number
- Canada PII: Name and Manitoba Driver's License Number
- Canada PII: Name and New Brunswick Driver's License Number
- Canada PII: Name and Newfoundland and Labrador Driver's License Number
- Canada PII: Name and Nova Scotia Driver's License Number
- Canada PII: Name and Ontario Driver's License Number
- Canada PII: Name and Prince Edward Island Driver's License Number
- Canada PII: Name and Quebec Driver's License Number
- Canada PII: Name and Saskatchewan Driver's License Number

- Chile PII

  Policy for detection of Chilean private information. The rules for this policy are:
  - Chile PII: Email Address and Password (Wide)
  - Chile PII: Email Address and Password (Default)
  - Chile PII: National Identity Number (RUN/RUT) (Wide)
  - Chile PII: National Identity Number (RUN/RUT) (Default)
- Colombia PII

  Policy for detection of Colombian private information. The rules for this policy are:
  - Colombia PII: Email Address and Password (Wide)
  - Colombia PII: Email Address and Password (Default)
  - Colombia PII: Identification Number (Wide)
  - Colombia PII: Identification Number (Default)
- Costa Rica PII

  Policy for detection of Costa Rican private information. The rules for this policy are:
  - Costa Rica PII: Email Address and Password (Wide)
  - Costa Rica PII: Email Address and Password (Default)
  - Costa Rica PII: Identification Number (Default)
  - Costa Rica PII: Identification Number (Narrow)
  - Costa Rica PII: Legal Identification Number (Default)
  - Costa Rica PII: Legal Identification Number (Narrow)
- Croatia PII

  Policy for detection of Unique Master Citizen Numbers and Personal identification numbers. The rules for this policy are:
  - Croatia PII: Unique Master Citizen Number (Wide)
  - Croatia PII: Unique Master Citizen Number (Default)

- Croatia PII: Personal identification number (Wide)
- Croatia PII: Personal identification number (Default)

- Cyprus PII

  Policy for detection of Cypriot private information. The rules for this policy are:
  - Cyprus PII: Tax Identification Code (Wide)
  - Cyprus PII: Tax Identification Code (Default)
- Czech Republic

  Policy for detection of Czech Republic private information. The rules for this policy are:
  - Czech Republic PII: Email Address and Password (Wide)
  - Czech Republic PII: Email Address and Password (Default)
  - Czech Republic PII: Rodne Cislo (Wide)
  - Czech Republic PII: Rodne Cislo (Default)
- Denmark PII

  Policy for detection of Danish private information. The rules for this policy are:
  - Denmark PII: CPR Number and Name - Wide
  - Denmark PII: CPR Number and Name - Default
  - Denmark PII: CPR Number and Name - Narrow
  - Denmark PII: CPR Number (Wide)
  - Denmark PII: CPR Number (Default)
  - Denmark PII: CPR Number (Narrow)
  - Denmark PII: Email Address and Password (Wide)
  - Denmark PII: Email Address and Password (Default)
- EIN

  Policy for detection of Employer Identification Numbers (EIN). The rule for this policy is:
  - Rule for detecting EIN (Employer Identification Numbers).
- Email Addresses

  Policy for detection of email addresses in email body or attachments. The rules for this policy are:
  - Email: Multiple Recipients
  - Email: Multiple Recipients with different domains
  - Email: Multiple Email addresses
  - Email: Multiple Email addresses with different domains
- Estonia PII

  Policy for detection of Estonian private information. The rules for this policy are:
  - Estonia PII: Personal Identification Code (Wide)
  - Estonia PII: Personal Identification Code (Default)
- Finland PII

Policy for detection of Finnish private information. The rules for this policy are:

- Finland PII: Email Address and Password (Wide)
- Finland PII: Email Address and Password (Default)
- Finland PII: Social Security Number (Wide)
- Finland PII: Social Security Number (Default)

- France PII

  Policy for detection of French private information.The rules for this policy are:

  - France PII: Credit Card Number and Name
  - France PII: Email Address and Password (Wide)
  - France PII: Email Address and Password (Default)
  - France PII: INSEE Code
  - France PII: Name and Sensitive Disease
  - France PII: INSEE Code and Sensitive Disease
  - France PII: Name and INSEE Code

- Germany PII

  Policy for detection of German private information. The rules for this policy are:

  - Germany PII: Credit Card Number and Name
  - Germany PII: Email Address and Password (Wide)
  - Germany PII: Email Address and Password (Default)
  - Germany PII: Ethnicity and Name
  - Germany PII: Sensitive Disease and Name
  - Germany PII: Crime and Name h.

- Greece PII

  Policy for detection of Greek private information. The rules for this policy are:

  - Greece PII: AFM Number (Default)
  - Greece PII: AFM Number (Wide)
  - Greece PII:AFM Number and Name (Default)
  - Greece PII: AFM Number and Name (Wide)
  - Greece PII: Email Address and Password (Wide)
  - Greece PII: Email Address and Password (Default)
  - Greece PII: ID Number (Default)
  - Greece PII: ID Number and Name (Default)
  - Greece PII: ID Number and Name (Wide)
  - Greece PII: Sensitive Medical Information and Name (Wide)
  - Greece PII: Sensitive Medical Information and Name (Default)

- Hong Kong PII

  Policy for detection of Hong Kong private information. The rules for this policy are:

- Hong Kong PII: Email Address and Password (Wide)
- Hong Kong PII: Email Address and Password (Default)
- Hong Kong PII: ID Number (Wide)
- Hong Kong PII: ID Number (Default)
- Hong Kong PII: ID Number (Narrow)
- Hong Kong PII: ID Number and Address (Wide)
- Hong Kong PII: ID Number and Address (Default)
- Hong Kong PII: ID Number and Address (Narrow)
- Hong Kong PII: ID Number and Surname (Wide)
- Hong Kong PII: ID Number and Surname (Default)
- Hong Kong PII: Hong Kong ID (formal form) and Common Surname
- Hong Kong PII: ID Number, Surname and Address (Wide)
- Hong Kong PII: ID Number, Surname and Address (Default)
- Hong Kong PII: ID Number, Surname and Address (Narrow)
- Hong Kong PII: Surname and Address (Wide)
- Hong Kong PII: Surname and Address (Default)
- Hong Kong PII: Surname and Address (Narrow)

- Hungary PII

  Policy for detection of Hungarian private information. The rules for this policy are:

  - Hungary PII: Hungarian Szemelyi Azonosito Szam (Wide)
  - Hungary PII: Hungarian Szemelyi Azonosito Szam (Default)
  - Hungary PII: Hungarian TAJ szam (Wide)
  - Hungary PII: Hungarian TAJ szam (Default)
  - Hungary PII: Hungarian Adoazonosito jel (Wide)
  - Hungary PII: Hungarian Adoazonosito jel (Default)
- Iceland PII

  Policy for detection of Icelandic private information. The rules for this policy are:

  - Iceland PII: Kennitala of Individuals (Default)
  - Iceland PII: Kennitala of Individuals (Wide)
- India PII

  Policy for detection of Indian private information. The rules for this policy are:

  - India PII: Email Address and Password (Wide)
  - India PII: Email Address and Password (Default)
  - India PII: Form 16
  - India PII: PAN (Default)
  - India PII: PAN (Wide)
- Indonesia PII

Policy for detection of Indonesian private information. The rules for this policy are:

- Indonesia PII: Email Address and Password (Wide)
- Indonesia PII: Email Address and Password (Default)
- Indonesia PII: Single Identity Number (Wide)
- Indonesia PII: Single Identity Number (Default)

- Ireland PII

  Policy for detection of Irish private information. The rules for this policy are:

  - Ireland PII: Driver Number and Name
  - Ireland PII: Email Address and Password (Wide)
  - Ireland PII: Email Address and Password (Default)
  - Ireland PII: Passport Number and Name
  - Ireland PII: Personal Public Service Number (PRSI/PPS) and Name

- Israel PII

  Policy for detection of Israeli private information. The rules for this policy are:

  - Israel PII: Email Address and Password (Wide)
  - Israel PII: Email Address and Password (Default)
  - Israel PII: Identity Number - 8- or 7-Digits (Wide)
  - Israel PII: Identity Number - 8- or 7-Digits (Default)
  - Israel PII: Identity Number (Wide)
  - Israel PII: Identity Number (Default)
  - Israel PII: Name and Identity Number

- Italy PII

  Policy for detection of Italian private information. The rules for this policy are:

  - Italy PII: Codice Fiscale
  - Italy PII: Name and Codice Fiscale
  - Italy PII: Name and health information
  - Italy PII: Codice Fiscale and health information

- Japan PII

  Policy for detection of Japanese private information. The rules for this policy are:

  - Japan PII: Corporate Number (Wide)
  - Japan PII: Corporate Number (Default)
  - Japan PII: Corporate Number (Narrow)
  - Japan PII: E-mail Address
  - Japan PII: Email Address and Password (Wide)
  - Japan PII: Email Address and Password (Default)
  - Japan PII: Individual Number (Wide)
  - Japan PII: Individual Number (Default)

- Japan PII: Individual Number (Narrow)
- Japan PII: Surname and Account
- Japan PII: Surname and Driver License Number
- Japan PII: Surname and Pension Number
- Japan PII: Surname and Ledger Number
- Japan PII: Telephone Numbers

- Kazakhstan PII

  Policy for detection of Kazakh private information. The rules for this policy are:
  - Kazakhstan PII: Taxpayer Registration Numbers (Wide)
  - Kazakhstan PII: Taxpayer Registration Numbers (Default)
  - Kazakhstan PII: Individual Identification Numbers (Wide)
  - Kazakhstan PII: Individual Identification Numbers (Default)
  - Kazakhstan PII: Business Identification Numbers (Wide)
  - Kazakhstan PII: Business Identification Numbers (Default)
- Latvia PII

  Policy for detection of Latvian private information. The rules for this policy are:
  - Latvia PII: Personal Identity Number (Wide)
  - Latvia PII: Personal Identity Number (Default)
- Lithuania PII

  Policy for detection of Lithuanian private information. The rules for this policy are:
  - Lithuania PII: Personal Code (Wide)
  - Lithuania PII: Personal Code (Default)
- Luxembourg PII

  Policy for detection of Luxembourgian private information. The rules for this policy are:
  - Luxembourg PII: National Identification Number - 11 Digits (Wide)
  - Luxembourg PII: National Identification Number - 11 Digits (Default)
  - Luxembourg PII: National Identification Number - 13 Digits (Wide)
  - Luxembourg PII: National Identification Number - 13 Digits (Default)
- Macau PII

  Policy for detection of Macau private information.The rules for this policy are:
  - Macau PII: Email Address and Password (Wide)
  - Macau PII: Email Address and Password (Default)
  - Macau PII: ID (formal form) (v7.8.1 only)
  - Macau PII: ID Number (Default)
  - Macau PII: ID Number (Narrow)
- Macedonia PII

Policy for detection of Unique Master Citizen Numbers. The rules for this policy are:

- Macedonia PII: Unique Master Citizen Number (Wide)
- Macedonia PII: Unique Master Citizen Number (Default)

- Malaysia PII

  Policy for detection of Malaysian private information.The rules for this policy are:

  - Malaysia PII: ID formal form
  - Malaysia PII: ID formal form - Wide
  - Malaysia PII: ID w proximity - Default
  - Malaysia PII: ID w proximity
  - Malaysia PII: ID formal form with BP
  - Malaysia PII: ID formal form with BP w proximity
  - Malaysia PII: Malaysian Name and sensitive health information

- Malta PII

  Policy for detection of Maltese private information. The rules for this policy are:

  - Malta PII: Identity Card Number (Wide)
  - Malta PII: Identity Card Number (Default)

- Mexico PII

  Policy for detection of Mexican private information. The rules for this policy are:

  - Mexico PII: Email Address and Password (Wide)
  - Mexico PII: Email Address and Password (Default)
  - Mexico PII: Passport Number (Wide)
  - Mexico PII: Passport Number (Default)
  - Mexico PII: RFC (Default)
  - Mexico PII: RFC (wide)
  - Mexico PII: CURP (Default)
  - Mexico PII: CURP (Narrow)
  - Mexico PII: CPISP (Default)
  - Mexico PII: CPISP (Narrow)
  - Mexico PII: CPISP (Wide)
  - Mexico PII: Social Security Number (NSS) (Wide)
  - Mexico PII: Social Security Number (NSS) (Default)
  - Mexico PII: SSP Contratos Internos Detection (Default)
  - Mexico PII: SSP Contratos Internos Detection (Wide)

- Montenegro PII

  Policy for detection of Unique Master Citizen Numbers. The rules for this policy are:

  - Montenegro PII: Unique Master Citizen Number (Wide)
  - Montenegro PII: Unique Master Citizen Number (Default)

- Netherlands PII

  Policy for detection of Dutch private information. The rules for this policy are:

  - Netherlands PII: Bank Account Number (Wide)
  - Netherlands PII: Bank Account Number (Default)
  - Netherlands PII: Citizen Service Number and CCN
  - Netherlands PII: Citizen Service Number and Crime
  - Netherlands PII: Citizen Service Number and Disease
  - Netherlands PII: Citizen Service Number and Ethnicity
  - Netherlands PII: Citizen Service Number and Password (Wide)
  - Netherlands PII: Citizen Service Number and Password (Default)
  - Netherlands PII: Citizen Service Number and Password (Narrow)
  - Netherlands PII: Driver License Number
  - Netherlands PII: Email Address and Password (Wide)
  - Netherlands PII: Email Address and Password (Default)
  - Netherlands PII: Passport Number
- New Zealand PII

  Policy for detection of New Zealand private information. The rules for this policy are:

  - New Zealand PII: Email Address and Password (Wide)
  - New Zealand PII: Email Address and Password (Default)
  - New Zealand: NHI Number (Wide)
  - New Zealand: NHI Number (Default)
- Norway PII

  Policy for detection of Norwegian private information. The rules for this policy are

  - Norway PII: Email Address and Password (Wide)
  - Norway PII: Email Address and Password (Default)
  - Norway PII: Personal Number (Wide)
  - Norway PII: Personal Number (Default)
  - Norway PII: Personal Number (Narrow)
  - Norway PII: Name and Personal Number
  - Norway PII: Name and Sensitive Disease
- People’s Republic of China PII

  Policy for detection of People’s Republic of China private information. The rules for this policy are:

  - People’s Republic of China PII: CV and Resume in Chinese
  - People's Republic of China PII: Email Address and Password (Wide)
  - People's Republic of China PII: Email Address and Password (Default)
  - People’s Republic of China PII: Identification Number

- People's Republic of China PII: Passport Number (Default)
- People's Republic of China PII: Passport Number (Narrow)

- Peru PII

  Policy for detection of Peruvian private information. The rules for this policy are:
  - Peru PII: Email Address and Password (Wide)
  - Peru PII: Email Address and Password (Default)
  - Peru PII: Unique Identification Code (CUI) (Wide)
  - Peru PII: Unique Identification Code (CUI) (Default)
  - Peru PII: Unique Identification Code (CUI) (Narrow)
  - Peru PII: Unique Taxpayer Registration Number (RUC) of Individuals (Wide)
  - Peru PII: Unique Taxpayer Registration Number (RUC) of Individuals (Default)
  - Peru PII: Unique Taxpayer Registration Number (RUC) of Non-Individuals (Wide)
  - Peru PII: Unique Taxpayer Registration Number (RUC) of Non-Individuals (Default)
- Philippines PII

  Policy for detection of Philippine private information. The rules for this policy are:
  - Philippines PII: DNA Profile
  - Philippines PII: Name and Address (Wide)
  - Philippines PII: Name and Address (Default)
  - Philippines PII: Name and Address (Narrow)
  - Philippines PII: Name and CCN (Wide)
  - Philippines PII: Name and CCN (Default)
  - Philippines PII: Name and CCN (Narrow)
  - Philippines PII: Name and Common Medical Condition (Wide)
  - Philippines PII: Name and Common Medical Condition (Default)
  - Philippines PII: Name and Crime (Wide)
  - Philippines PII: Name and Crime (Default)
  - Philippines PII: Name and Date of Birth (Wide)
  - Philippines PII: Name and Date of Birth (Default)
  - Philippines PII: Name and Password (Wide)
  - Philippines PII: Name and Password (Default)
  - Philippines PII: Name and Password (Narrow)
  - Philippines PII: Name and PhilHealth Identification Number (Wide)
  - Philippines PII: Name and PhilHealth Identification Number (Default)
  - Philippines PII: Name and Physical Information (Wide)

- Philippines PII: Name and Physical Information (Default)
- Philippines PII: Name and Sensitive Disease or Drug (Wide)
- Philippines PII: Name and Sensitive Disease or Drug (Default)
- Philippines PII: Name and SSS Number (Wide)
- Philippines PII: Name and SSS Number (Default)
- Philippines PII: Name and TIN (Wide)
- Philippines PII: Name and TIN (Default)
- Philippines PII: Password Dissemination for HTTP Traffic (Wide)
- Philippines PII: Password Dissemination for HTTP Traffic (Default)
- Philippines PII: Password Dissemination for HTTP Traffic (Narrow)
- Philippines PII: PhilHealth Identification Number (Wide)
- Philippines PII: PhilHealth Identification Number (Default)
- Philippines PII: SSS Number (Wide)
- Philippines PII: SSS Number (Default)
- Philippines PII: TIN Number (Wide)
- Philippines PII: TIN Number (Default)

- Poland PII

  Policy for detection of Polish private information. The rules for this policy are:

  - Poland PII: NIP Number (Wide)
  - Poland PII: NIP Number (Default)
  - Poland PII: NIP Number and Name
  - Poland PII: PESEL Number (Wide)
  - Poland PII: PESEL Number (Default)
  - Poland PII: PESEL and Name
  - Poland PII: Polish ID Number (Wide)
  - Poland PII: Polish ID Number (Default)
  - Poland PII: Polish ID and Name
  - Poland PII: REGON Number (Wide)
  - Poland PII: REGON Number (Default)
  - Poland PII: REGON and Name

- Portugal PII

  Policy for detection of Portuguese private information. The rules for this policy are:

  - Portugal PII: Document Number (Wide)
  - Portugal PII: Document Number (Default)
  - Portugal PII: Email Address and Password (Wide)
  - Portugal PII: Email Address and Password (Default)
  - Portugal PII: Social Security Number (Wide)

- Portugal PII: Social Security Number (Default)
- Portugal PII: Tax Identification Number of Individuals (Wide)
- Portugal PII: Tax Identification Number of Individuals (Default)

- Romania PII

  Policy for detection of Romanian private information. The rule for this policy is:
  - Romania PII: Personal numeric code
- Russia PII

  Policy for detection of Russian private information. The rules for this policy are:
  - Russia PII: Email Address and Password (Wide)
  - Russia PII: Email Address and Password (Default)
  - Russia PII: Moscow Social Card Number (Wide)
  - Russia PII: Moscow Social Card Number (Default)
  - Russia PII: Moscow Social Card Number and Serial Number
  - Russia PII: Passport Number and Name (Wide)
  - Russia PII: Passport Number and Name (Default)
  - Russia PII: Passport Number and Name (Narrow)
  - Russia PII: Passport Number
  - Russia PII: Personal Pension Account Number (Wide)
  - Russia PII: Personal Pension Account Number (Default)
  - Russia PII: Phone Number (Wide)
  - Russia PII: Phone Number (Default)
  - Russia PII: Phone Number (Narrow)
  - Russia PII: Primary State Registration Numbers of Companies (Wide)
  - Russia PII: Primary State Registration Numbers of Companies (Default)
  - Russia PII: Primary State Registration Numbers of Individuals (Wide)
  - Russia PII: Primary State Registration Numbers of Individuals (Default)
  - Russia PII: Russian Classification on Objects of Administrative (Wide)
  - Russia PII: Russian Classification on Objects of Administrative Division (Default)
  - Russia PII: Russian Unified Classifier of Enterprises and Organizations
  - Russia PII: Taxpayer Identification Number of Companies (Wide)
  - Russia PII: Taxpayer Identification Number of Companies (Default)
  - Russia PII: Taxpayer Identification Number of Individuals (Wide)
  - Russia PII: Taxpayer Identification Number of Individuals (Default)
- Serbia PII

  Policy for detection of Unique Master Citizen Numbers. The rules for this policy are:
  - Serbia PII: Unique Master Citizen Number (Wide)

- Serbia PII: Unique Master Citizen Number (Default)

- Singapore PII

  Policy for detection of Singaporean private information. The rules for this policy are:

  - Singapore PII: Email Address and Password (Wide)
  - Singapore PII: Email Address and Password (Default)
  - Singapore PII: Identification Number (Wide)
  - Singapore PII: Identification Number (Default)
  - Singapore PII: Identification Number and CCN
  - Singapore PII: Name and Address (Default)
  - Singapore PII: Name and Address (Narrow)

- Slovakia PII

  Policy for detection of Slovak private information. The rule for this policy is:

  - Slovakia PII: Email Address and Password (Wide)
  - Slovakia PII: Email Address and Password (Default)
  - Slovakia PII: Rodne Cislo (wide)
  - Slovakia PII: Rodne Cislo (default)

- Slovenia PII

  Policy for detection of Unique Master Citizen Numbers. The rules for this policy are:

  - Slovenia PII: Unique Master Citizen Number (Wide)
  - Slovenia PII: Unique Master Citizen Number (Default)

- Social Insurance Numbers

  Detects valid Canadian Social Insurance Numbers (SIN). The rules for this policy are:

  - SIN: wide
  - SIN: default
  - SIN: narrow

- Social Security Numbers

  Policy for detection of validated social security numbers. The rules for this policy are:

  - US SSN (wide)
  - US SSN (default)
  - US SSN (narrow)
  - US SSN (audit)
  - US SSN: Wide Minus Default
  - US SSN - not masked (v7.8.1 and 7.8.2 only)
  - SSN: ITIN

- South Africa PII

Policy for detection of South African private information. The rules for this policy are:

- South Africa PII: Email Address and Password (Wide)
- South Africa PII: Email Address and Password (Default)
- South Africa PII: ID Number (wide)
- South Africa PII: ID Number (default)
- South Africa PII:SA ID (narrow)
- South Africa PII: Name and Sensitive Health Information

- South Korea PII

  Policy for detection of South Korean private information. The rules for this policy are:

  - South Korea PII: DNA Profile
  - South Korea PII: Email Address and Password (Wide)
  - South Korea PII: Email Address and Password (Default)
  - South Korea PII: ID Number (Default)
  - South Korea PII: ID Number (Wide)
  - South Korea PII: ID Number (With Proximity)
  - South Korea PII: Phone Number (Default)
  - South Korea PII: Phone Number (Wide)
  - South Korea PII: Phone Number (With Proximity)

- Spain PII

  Policy for detection of Spanish private information. The rules for this policy are:

  - Spain PII: DNI, Account and Password
  - Spain PII: DNI and Credit Card Number
  - Spain PII: DNI and Crime
  - Spain PII: DNI and Disease
  - Spain PII: DNI and Ethnicity
  - Spain PII: Email Address and Password (Wide)
  - Spain PII: Email Address and Password (Default)
  - Spain PII: Name and Address (Default)
  - Spain PII: Name and Address (Narrow)
  - Spain PII: Name and Credit Card Number
  - Spain PII: Name and DNI
  - Spain PII: Name and IBAN
  - Spain PII: Name and Passport Number
  - Spain PII: Name and Email Address
  - Spain PII: Name and Phone Number
  - Spain PII: Name and Social Security Number (Wide)

- Spain PII: Name and Social Security Number (Default)
- Spain PII: Social Security Number (Wide)
- Spain PII: Social Security Number (Default)

- Sweden PII

  Policy for detection of Swedish private information. The rules for this policy are:
  - Sweden PII: Email Address and Password (Wide)
  - Sweden PII: Email Address and Password (Default)
  - Sweden PII: ID Number (Wide)
  - Sweden PII: ID Number (Default)
- Switzerland

  Policy for detection of Swiss private information. The rules for this policy are:
  - Switzerland PII: Email Address and Password (Wide)
  - Switzerland PII: Email Address and Password (Default)
  - Switzerland PII: Old Format AHV
  - Switzerland PII: New Format AHV
- Taiwan PII

  Policy for detection of Taiwanese private information. The rules for this policy are:
  - Taiwan PII: Address (Wide)
  - Taiwan PII: Address (Default)
  - Taiwan PII: Address (Narrow)
  - Taiwan PII: Email Address and Password (Wide)
  - Taiwan PII: Email Address and Password (Default)
  - Taiwan PII: ID Card Number (Wide)
  - Taiwan PII: ID Card Number (Default)
  - Taiwan PII: ID Card Number and Surname (Wide)
  - Taiwan PII: ID Card Number and Surname (Default)
  - Taiwan PII: ID Card Number, Surname and Private Information (Wide)
  - Taiwan PII: ID Card Number, Surname and Private Information (Default)
  - Taiwan PII: Surname and Address
- Thailand PII

  Policy for detection of Thai private information. The rules for this policy are:
  - Thailand PII: Email Address and Password (Wide)
  - Thailand PII: Email Address and Password (Default)
  - Thailand: National ID Number (Wide)
  - Thailand: National ID Number (Default)
- Turkey PII

  Policy for detection of Turkish private information.The rules for this policy are:

- Turkey PII: Email Address and Password (Wide)
- Turkey PII: Email Address and Password (Default)
- Turkey PII: TC Kimlik
- Turkey PII: TC Kimlik one support

- UK PII

  Policy for detection of UK private information. The rules for this policy are:
  - UK PII: Bank Account Number and Name
  - UK PII: Credit File (Wide)
  - UK PII: Credit File (Default)
  - UK PII: Credit File (Narrow)
  - UK PII: Driver Number and Name (Wide)
  - UK PII: Driver Number and Name (Default)
  - UK PII: Email Address and Password (Wide)
  - UK PII: Email Address and Password (Default)
  - UK PII: National Insurance Number and Name
  - UK PII: NHS Number (Default)
  - UK PII: NHS Number (Narrow)
  - UK PII: NHS Number (Wide)
  - UK PII: Passport Number and Name
  - UK PII: Postal Code and Name (Default)
  - UK PII: Postal Code and Name (Narrow)
  - UK PII: Sort Code and Name
  - UK PII: Tax ID Number and Name
- US PII

  Policy for detection of US private information. The rules for this policy are:
  - US PII: Credit File (Wide)
  - US PII: Credit File (Default)
  - US PII: Credit File (Narrow)
  - US PII: DNA Profile (Default)
  - US PII: DNA Profile (Narrow)
  - US PII: Email Address and Password (Wide)
  - US PII: Email Address and Password (Default)
  - US PII: Name and Address
  - US PII: Name and Crime
  - US PII: Name and Arizona Driver License Number
  - US PII: Name and Arkansas Driver License Number
  - US PII: Name and California Driver License Number
  - US PII: Name and Colorado Driver License Number
  - US PII: Name and Connecticut Driver License Number

- US PII: Name and District of Columbia Driver License Number
- US PII: Name and Florida Driver License Number
- US PII: Name and Georgia Driver License Number
- US PII: Name and Illinois Driver License Number
- US PII: Name and Indiana Driver License Number
- US PII: Name and Iowa Driver License Number
- US PII: Name and Massachusetts Driver License Number
- US PII: Name and Michigan Driver License Number
- US PII: Name and Minnesota Driver License Number
- US PII: Name and Nevada Driver License Number
- US PII: Name and New Jersey Driver License Number
- US PII: Name and New York Driver License Number
- US PII: Name and North Carolina Driver License Number
- US PII: Name and Ohio Driver License Number
- US PII: Name and Pennsylvania Driver License Number
- US PII: Name and Texas Driver License Number
- US PII: Name and Utah Driver License Number
- US PII: Name and Virginia Driver License Number
- US PII: Name and Washington Driver License Number
- US PII: Name and Wisconsin Driver License Number
- US PII: Name and Illinois State ID Number
- US PII: Name and Ethnicity
- US PII: Name and Passport Number (Wide)
- US PII: Name and Passport Number (Default)
- US PII: Name and Passport Number (Narrow)
- US PII: Passport Number (Wide)
- US PII: Passport Number (Default)
- US PII: Social Security Number
- US PII: Social Security Number and Name

- Vietnam PII

  Policy for detection of Vietnamese private information. The rules for this policy are:

  - Vietnam PII: CMND Number (Wide)
  - Vietnam PII: CMND Number (Default)
  - Vietnam PII: Email Address and Password (Wide)
  - Vietnam PII: Email Address and Password (Default)

Regulations, Compliance and Standards

Predefined Policies and Classifiers | Forcepoint DLP | v8.6.x

Forcepoint DLP includes the following types of regulatory and compliance policies:

EU General Data Protection Regulation (GDPR)

Predefined Policies and Classifiers | Forcepoint DLP | v8.6.x

The description and list of rules for each policy in this category can be found in other sections of this document.

- Austria Finance
- Austria PII
- Belgium Finance
- Belgium PII
- Biometric Files
- Bulgaria Finance
- Bulgaria PII
- Croatia Finance
- Croatia PII
- CV and Resume in English
- CV and Resume in French
- CV and Resume in German
- CV and Resume in Spanish
- Cyprus Finance
- Cyprus PII
- Czech Republic Finance
- Czech Republic PII
- Denmark Finance
- Denmark PII
- Estonia Finance
- Estonia PII
- EU finance
- Finland Finance
- Finland PII

- France Finance
- France PII
- Germany Finance
- Germany PII
- Greece Finance
- Greece PII
- Hungary Finance
- Hungary PII
- IMEI
- Ireland Finance
- Ireland PII
- Italy Finance
- Italy PHI
- Italy PII
- Latvia Finance
- Latvia PII
- Lithuania Finance
- Lithuania PII
- Luxembourg Finance
- Luxembourg PII
- Malta Finance
- Malta PII
- Netherlands Finance
- Netherlands PII
- Password Dissemination
- PCI
- Poland Finance
- Poland PII
- Portugal Finance
- Portugal PII
- Romania Finance
- Romania PII
- Slovakia Finance
- Slovakia PII
- Slovenia Finance
- Slovenia PII
- Spain Finance
- Spain PII

- Sweden Finance
- Sweden PHI
- Sweden PII
- UK Finance
- UK PHI
- UK PII

Financial Regulations

EU Finance

Policy for promoting regulatory compliance with the requirements of the Basel Committee on Banking Supervision. The policy contains rules to detect financial data like account numbers, passwords, or magnetic credit card tracks. Additional rules detect combinations of Personally Identifiable Information (PII) like credit cards and identification numbers. The rules for this policy are:

- EU Finance: 5-8 Digit Account Number
- EU Finance: 9 Digit Account Number
- EU Finance: 10 Digit Account Number
- EU Finance: CCN and National ID Number
- EU Finance: CCN and PIN
- EU Finance: Credit Card Magnetic Strip
- EU Finance: Password Dissemination for HTTP Traffic (Wide)
- EU Finance: Password Dissemination for HTTP Traffic (Default)
- EU Finance: Password Dissemination for HTTP Traffic (Narrow)
- EU Finance: Password Dissemination for non-HTTP/S Traffic (Wide)
- EU Finance: Password Dissemination for non-HTTP/S Traffic (Default)
- EU Finance: Password Dissemination for non-HTTP/S Traffic (Narrow)

FCRA

The Fair Credit Reporting Act (FCRA) is a United States federal law. The Act is designed to help ensure that consumer reporting agencies act fairly, impartially, and with respect for the consumer's right to privacy when preparing consumer reports on individuals. The policy comprises rules for detection of personal financial information. The rules for this policy are:

- FCRA: CCN: All Credit Cards
- FCRA: Credit Card Magnetic Strips
- FCRA: DL and Account
- FCRA: DL and Personal Finance Terms
- FCRA: Name and Personal Finance Terms

- FCRA: SSN and Account
- FCRA: SSN and Personal Finance Terms

FFIEC

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the Federal examination of financial institutions. The policy contains rules to detect financial data like account numbers, passwords, or magnetic credit card tracks. Additional rules detect combinations of Personally Identifiable Information (PII) like credit cards, social security numbers, driver license numbers, and private financial information. The rules for this policy are:

- FFIEC: 5-8 Digit Account Number
- FFIEC: 9 Digit Account Number
- FFIEC: 10 Digit Account Number
- FFIEC: Credit Card Magnetic Strip
- FFIEC: Credit Card Number
- FFIEC: Driver License
- FFIEC: Password Dissemination for HTTP Traffic (Wide)
- FFIEC: Password Dissemination for HTTP Traffic (Default)
- FFIEC: Password Dissemination for HTTP Traffic (Narrow)
- FFIEC: Password Dissemination for non-HTTP/S Traffic (Wide)
- FFIEC: Password Dissemination for non-HTTP/S Traffic (Default)
- FFIEC: Password Dissemination for non-HTTP/S Traffic (Narrow)
- FFIEC: PIN
- FFIEC: Social Security Number
- FFIEC: TIFF File
- FFIEC: Zip Code and Financial Term

FSA SYSC 13.7.7

The Financial Services Authority (FSA) publishes a set of rules in the Financial Services Handbook. The Senior Management Arrangements, Systems and Controls (SYSC) is one of the subsections of this handbook. Chapter 13.7.7 requires firm to establish and maintain appropriate systems and controls to manage its information security risks regarding the confidentiality, integrity, availability, and accountability of its information. This policy detects confidential and financial documents. The rules for this policy are:

- FSA SYSC 13.7.7: Confidential Documents
- FSA SYSC 13.7.7: Tables with financial information
- FSA SYSC 13.7.7: Network Information and Security
- FSA SYSC 13.7.7: Proprietary in Document

GLBA

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, is a US Federal regulation that includes provisions to protect consumers' personal financial information held by financial institutions. The policy contains rules to detect accounts, credit cards, and social security numbers. The policy comprises rules for detection of personal financial information and other personal information. The rules for this policy are:

- GLBA: CCN (Default)
- GLBA: CCN (Narrow)
- GLBA: Name and SSN
- GLBA: SSN and Personal Finance Terms
- GLBA: SSN and Account
- GLBA: RTN/ABA (wide)
- GLBA: RTN/ABA (narrow)
- GLBA: RTN/ABA (default)
- GLBA: Name and 10 digit account numbers
- GLBA: Name and 9 digit account numbers
- GLBA: Name and 5-8 digit account numbers
- GLBA: Name and Personal Finance Terms
- GLBA: Name and Sensitive Disease or drug
- GLBA: Names (Narrow) and Sensitive Disease or drug
- GLBA: Name and Contact Info

Model Audit Rule (MAR)

The National Association of Insurance Commissioners (NAIC) Model Audit Rule (MAR) requires the assessment of internal controls over financial reporting. The policy comprises rules for detection of documents containing financial reports and, in particular, of actuary reports. The rules for this policy are:

- MAR: Actuary Report
- MAR: Financial Investment Information in Excel
- MAR: Form 10-K (Non-Standard Fiscal Year)
- MAR: Form 10-K (Standard Fiscal Year)
- MAR: Form 10-Q (Non-Standard Fiscal Year)
- MAR: Form 10-Q (Standard Fiscal Year)
- MAR: SOX-Related Term

NBT 357

The Israeli NBT directive requires Israeli Banks and agencies to protect customers privacy by ensuring the integrity and confidentiality of data. The policy detects credit

card information, account numbers, International Bank accounts number (Israeli IBAN) and buy and sell instructions in Hebrew. The rules for this policy are:

- NBT 357: All Credit Cards (Default)
- NBT 357: All Credit Cards (Wide)
- NBT 357: IsraCard (Default)
- NBT 357: IsraCard (Wide)
- NBT 357: Account Number
- NBT 357: Buy and Sell instructions
- NBT 357: Israeli IBAN (default)
- NBT 357: Israeli IBAN (wide)

NYSE rule 472

Regulates communications with investors and mandates approval of communications and research reports before being released as well as the retention and archiving of such communications. The rule for this policy is:

- NYSE rule 472

SEC

Policy for detection of SEC forms 10-K and 10-Q, based on calendar fiscal year.

The rule s for this policy are:

- SEC: Form 10-K (Non-Standard Fiscal Year)
- SEC: Form 10-K (Standard Fiscal Year)
- SEC: Form 10-Q (Non-Standard Fiscal Year)
- SEC: Form 10-Q (Standard Fiscal Year)

Payment Card Industry (PCI)

PCI

Policy for promoting compliance with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS is an industry standard, accepted internationally by all major credit card issuers and is enforced on companies and organizations that accept credit card payments or process, store, or transmit cardholder data. The standard includes the mandate that credit card numbers and cardholder data be highly secured and that transactions comprising PCI data be encrypted. Forensics are not saved for the rules that are enabled by default. The rules for this policy are:

- PCI: Credit-Card Numbers (wide)
- PCI: Credit-Card Numbers (default)
- PCI: Credit-Card Numbers (narrow)
- PCI: Credit Card Magnetic Strips

PCI Audit

A permissive policy for detecting potential credit-card-numbers. The policy contains several rules to address corner cases, such as numbers that appear as part of a long sequence, with user-defined delimiters etc. Most of the rules in the policy may cause high rate of false positives and are not recommended for usage in production mode. The rules for this policy are:

- PCI Audit: No Word Boundaries
- PCI Audit: Non-Delimited
- PCI Audit: User-Defined Delimiter
- PCI Audit: CCN and Expiration Date
- PCI Audit: CCN and CVV
- PCI Audit: CCN Without Validation
- PCI Audit: Credit Card Number (Extra Wide)
- PCI Audit: Credit Card Number (Default)
- PCI Audit: Credit Card Magnetic Strip
- PCI Audit: Masked Credit Card Number
- PCI Audit: CCN in Non-English Characters
- PCI Audit: User-Defined IIN (Wide)
- PCI Audit: User-Defined IIN (Default)
- PCI Audit: User-Defined IIN (Narrow)

National Privacy Regulations

Forcepoint DLP includes regulatory policies for numerous countries.

Australia

Policies for promoting compliance with Australian Privacy regulations.

- Australian Privacy Act (2012 Revision)

  The Australian Federal Privacy Act mandates protection of private information and limits its storage, usage, and distribution. The policy detects private information of Australians. Each one of this policy's rules relates to different private information. Enable the rules you want to enforce. The rules for this policy are:

  - Australian Privacy Act: Medicare and Sensitive Disease or Drug
  - Australian Privacy Act: Medicare and Common Medical Condition
  - Australian Privacy Act: Name and Driver License Number
  - Australian Privacy Act: Name and Tax File Number (Wide)
  - Australian Privacy Act: Name and Tax File Number (Default)
  - Australian Privacy Act: Name and Address
  - Australian Privacy Act: Address and Tax File Number (Wide)
  - Australian Privacy Act: Address and Tax File Number (Default)
  - Australian Privacy Act: ABN and Address (Default)
  - Australian Privacy Act: ABN and Address (Wide)
  - Australian Privacy Act: Name and Bank Account Number
  - Australian Privacy Act: DNA profile
  - Australian Privacy Act: Name and Racial or Ethnic Origins
  - Australian Privacy Act: Name and Crime
  - Australian Privacy Act: Name and Sexual Preference
  - Australian Privacy Act: Credit File (Wide)
  - Australian Privacy Act: Credit File (Default)
  - Australian Privacy Act: Credit File (Narrow)
  - Australian Privacy Act: Name and ABN (Default)
  - Australian Privacy Act: Name and ABN (Wide)
  - Australian Privacy Act: Australian Name and Sensitive Disease or Drug
  - Australian Privacy Act: Australian Name and Common Medical Condition

Canada

Policies for promoting compliance with Canadian Privacy regulations.

- PIPEDA

  The Personal Information Protection and Electronic Documents Act is a Canadian law governing how private sector organizations collect, use and disclose personal information in the course of commercial business. The policy detects Canadian Personally Identifiable Information (PII) like social insurance numbers or credit cards, either alone or in combination with sensitive private information like health conditions.

  - PIPEDA: CCN and Common Medical Condition
  - PIPEDA: CCN and Sensitive Disease or Drug
  - PIPEDA: DOB and Address or SIN or Name
  - PIPEDA: Name and Driver License Number
  - PIPEDA: Name and Government Issues ID Card Number w proximity
  - PIPEDA: Name and Indian Status Number w proximity
  - PIPEDA: Name and Permanent Resident Card Number w proximity
  - PIPEDA: Name and Physical Information
  - PIPEDA: Name and Sensitive Disease
  - PIPEDA: SIN
  - PIPEDA: SIN and Address or DOB or Name
  - PIPEDA: SIN and CCN
  - PIPEDA: SIN and Common Medical Condition
  - PIPEDA: SIN and Sensitive Disease or drug

European Union

Policies for promoting compliance with European Union Privacy regulations.

- Denmark
  - Denmark Personal Information Protection Law

    The Denmark Personal Information Protection Law (PIP) regulates the handling of personal information. The policy comprises rules for detection of CPR numbers and Danish bank account numbers. The rules for this policy are:

    - DPIP: CPR and Name - Wide
    - DPIP: CPR and Name - Default
    - DPIP: CPR and Name - Narrow
    - DPIP: CPR numbers (Wide)
    - DPIP: CPR numbers (narrow)
    - DPIP: CPR numbers (default)
    - DPIP: Credit Cards
    - DPIP: Bank Account number - Wide

    - DPIP: Bank Account number with terms
    - DPIP: Bank Account number with strict format - Narrow
- Finland
  - Personal Data Act (523/1999)

    Finland's Personal Data Act provides restrictions on the processing, storage and transmission of personal and sensitive information, including personal ID. Under the Law, personal information relating to identity may only be processed, stored and transmitted with the consent of the individual. Personal information cannot generally be transferred outside of Finland unless the country has "comparable" protections. The policy comprises rules for detection of Finnish Social Security Numbers and DNA sequences. The rules for this policy are:

    - Finland Personal Data Act: Finnish SSN (Wide)
    - Finland Personal Data Act: Finnish SSN
    - Finland Personal Data Act: DNA Sequence
- France
  - France BNR (Ordonnance 2011-1012)

    A policy to promote compliance with the France Breach Notification Requirement (Ordonnance 2011-1012). According to this Ordinance, electronic communication service provider must inform, without delay, the French Data Protection Authority in case of any security breach. A data security breach is defined as any security breach that accidentally or unlawfully results in the destruction, loss, alteration, disclosure or unauthorized access to personal data that is being processed in the context of electronic communication services that are provided to the public. The rules for this policy are:

    - France BNR 2011-1012: CCN and Name
    - France BNR 2011-1012: INSEE numbers
    - France BNR 2011-1012: Name and Health
    - France BNR 2011-1012: INSEE and Health
    - France BNR 2011-1012: Name and INSEE
  - France Data Protection Law 2004-801

    Policy for the French Law 2004-801, which implements the EU Directive 95 on privacy. The policy contains rules to detect combinations of French full names and INSEE numbers with sensitive private information like credit card number or health conditions. The rules for this policy are:

    - France Privacy: CCN and Name
    - France Privacy: INSEE numbers
    - France Privacy: Name and Health
    - France Privacy: INSEE and Health
    - France Privacy: Name and INSEE
- Germany
  - Germany Federal Privacy Protection Act

Policy for the German Federal Privacy Protection Act, implementing the EU Directive 95 on privacy. The policy contains rules to detect combinations of German full names with sensitive private information like credit card number, ethnicity, and health conditions. the rules for this policy are:

- Germany FPP: CCN and Name
- Germany FPP: Ethnicity and Name
- Germany FPP: Health and Name
- Germany FPP: Crime and Name

- Greece
  - Greece - Hellenic DPA of 1997

    The Hellenic Data Protection Act of 1997 regulates the processing of personal data and therefore mandates the protection of private information. The policy detects Greek AFM (Αριθμός Φορολογικού Μητρώου) and ID numbers, alone or in proximity to a Greek names in Greek or Latin letters, and combinations of Greek names in proximity to sensitive medical information in Greek and English. The rules for this policy are:

    - Greece DPA: AFM Number (Default)
    - Greece DPA: AFM Number (Wide)
    - Greece DPA: AFM Number and Name (Default)
    - Greece DPA: AFM Number and Name (Wide)
    - Greece DPA: ID and Name (Default)
    - Greece DPA: ID and Name (Wide)
    - Greece DPA: Sensitive Medical Information and Name (Default)
    - Greece DPA: Sensitive Medical Information and Name (Wide)
- Hungary
  - Hungarian Data Protection Laws

    Act LXIII of 1992 on Protection of Personal Data and Disclosure of Data Public Interest mandates, among others, that personal data shall be protected against unauthorized access, transfer and public exposure. Data may only be processed, stored and transmitted with the consent of the individual. The Act sets out sanctions for violations. The policy comprises rules for detection of Hungarian Personal Numeric Code Numbers (szemelyi azonosito szam) Social Security Numbers (TAJ szam), Tax ID Numbers (Adoazonosito jel) and DNA information. The rules for this policy are:

    - Hungarian Data Protection Laws: Hungary Szemelyi Azonosito Szam (Wide)
    - Hungarian Data Protection Laws: Hungary Szemelyi Azonosito Szam (Default)
    - Hungarian Data Protection Laws: Hungary TAJ szam (Wide)
    - Hungarian Data Protection Laws: Hungary TAJ szam (Default)
    - Hungarian Data Protection Laws: Hungary Adoazonosito jel (Wide)
    - Hungarian Data Protection Laws: Hungary Adoazonosito jel (default)
    - Hungarian Data Protection Laws: DNA Sequence
- Ireland

- Ireland Data Protection Acts (DPA)

  Ireland Data Protection Acts (DPA) of 1988 and 2003, and in particular, the Personal Data Security Breach Code of Practice set by Ireland Data Protection Commissioner (DPC), mandate protection of personal information and requires that, in case where there is a risk of unauthorized disclosure, loss, destruction or alteration of personal data, the data controller must give immediate consideration to informing those affected. The policy contains rules to detect Irish Personally Identifiable Information (PII) like Personal Public Service Numbers (PPS/RSI) or passport numbers, alone or in combination with credit card numbers. The rules for this policy are:

  - Ireland DPA: Irish PRSI/PPS Number and CCN
  - Ireland DPA: Irish Driver Number and CCN
  - Ireland DPA: Irish Passport Number and CCN
  - Ireland DPA: Irish Personal Public Service Number
  - Ireland DPA: Irish Driver Number
  - Ireland DPA: Irish Passport Number
  - Ireland DPA: Irish IBAN (default)
  - Ireland DPA: Irish IBAN (wide)
  - Ireland DPA: Irish Bank Account
  - Ireland DPA: Name and Sensitive Diseases

- Italy
  - Italy Health Data Privacy Act

    The Italy Health Data Privacy Act protects persons from violation of their right to privacy through the processing of personal data. The Act helps to ensure that personal data is processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensures that personal data is of adequate quality. The policy contains rules to detect combinations of Italy Personally Identifiable Information (PII) like Codice Fiscale and full name, with sensitive health information. The rules for this policy are:

    - Italy HDPA: Codice Fiscale
    - Italy HDPA: Codice Fiscale and Health Information
    - Italy HDPA: DICOM
    - Italy HDPA: Name and Codice Fiscale
    - Italy HDPA: Name and Health Information
    - Italy HDPA: SPSS Text Files

- Netherlands
  - Netherlands Personal Data Protection Act

    Policy to promote compliance with the Dutch Personal Data Protection Act, which implements the EU Directive 95 on privacy. The policy contains rules to detect combinations of Netherlands sofinummer and sensitive private information like account number, driver license number, passport number, ethnicity and health conditions. The rules for this policy are:

    - Netherlands PDPA: Bank Account Number (Wide)

- Netherlands PDPA: Bank Account Number (Default)
- Netherlands PDPA: Citizen Service Number and CCN
- Netherlands PDPA: Citizen Service Number and Crime
- Netherlands PDPA: Citizen Service Number and Disease
- Netherlands PDPA: Citizen Service Number and Ethnicity
- Netherlands PDPA: Citizen Service Number and Password (Wide)
- Netherlands PDPA: Citizen Service Number and Password (Default)
- Netherlands PDPA: Citizen Service Number and Password (Narrow)
- Netherlands PDPA: Driver License Number
- Netherlands PDPA: Passport Number

- Poland
  - Poland LPPD

    The Law on the Protection of Personal Data (LPPD) is based on the European Union (EU) Data Protection Directive. Under the Law, personal information relating to identity may only be processed, stored and transmitted with the consent of the individual. Personal information cannot generally be transferred outside of Poland unless the country has 'comparable' protections. The law sets out civil and criminal sanctions for violations. The policy comprises rules for detection of Polish NIP numbers, PESEL numbers, Polish ID numbers, DNA information and Polish REGON numbers, alone or in proximity to a Polish name. The rules for this policy are:

    - Poland LPPD: DNA Sequence
    - Poland LPPD: NIP Number (Wide)
    - Poland LPPD: NIP Number (Default)
    - Poland LPPD: NIP Number and Name
    - Poland LPPD: PESEL Number (Wide)
    - Poland LPPD: PESEL Number (Default)
    - Poland LPPD: PESEL and Name
    - Poland LPPD: Polish ID Number (Wide)
    - Poland LPPD: Polish ID Number (Default)
    - Poland LPPD: Polish ID and Name
    - Poland LPPD: REGON Number (Wide)
    - Poland LPPD: REGON Number (Default)
    - Poland LPPD: REGON and Name

- Spain
  - Spain Data Privacy Act

    The Spanish Data Privacy Act implementing the EU Directive 95 on privacy. The policy contains rules to detect combinations of Spain National Identity Documents and sensitive private information like account numbers, ethnicity and health conditions. The rules for this policy are:

    - SPAIN DPA: DNI, Account and Password
    - SPAIN DPA: DNI and Credit Card Number
    - SPAIN DPA: DNI and Crime

- SPAIN DPA: DNI and Disease
- SPAIN DPA: DNI and Ethnicity
- SPAIN DPA: SSN, Account and Password (Wide)
- SPAIN DPA: SSN, Account and Password (Default)
- SPAIN DPA: SSN and Credit Card Number (Wide)
- SPAIN DPA: SSN and Credit Card Number (Default)
- SPAIN DPA: SSN and Crime (Wide)
- SPAIN DPA: SSN and Crime (Default)
- SPAIN DPA: SSN and Disease (Wide)
- SPAIN DPA: SSN and Disease (Default)
- SPAIN DPA: SSN and Ethnicity (Wide)
- SPAIN DPA: SSN and Ethnicity (Default)

- Sweden
  - Sweden Personal Data Act of 1998

    Sweden's Personal Data Act of 1998 was enacted to protect people against the violation of their personal integrity by processing of personal data. The act includes restrictions on the storage and transmission of personal data. The pre-defined policy comprises rules for detection of Swedish Personal Identity Number (personnummer) in traffic and DNA information. The rules for this policy are:

    - Sweden Personal Data Act: Swedish ID - wide
    - Sweden Personal Data Act: Swedish ID - default
    - Sweden Personal Data Act: DNA Sequence

  - Swedish Patient Data Act (SFS 2008:355 Patientdatalagen)

    A policy to promote compliance with the Swedish Patient Data Act (Patientdatalag, SFS 2008:355) that mandates protection of protected health information (PHI) and Personally Identifiable Information (PII) of Swedish citizens and residents. The policy comprises rules for detection of health information or medical conditions (in Swedish or English), in proximity to personally identifiable information such as personnummer or name, and for detection of SPSS files and Database files. The rules for this policy are:

    - SFS 2008:355: Database File
    - SFS 2008:355: DICOM
    - SFS 2008:355: DNA Profile
    - SFS 2008:355: ICD10 Code
    - SFS 2008:355: ICD10 Code and Description
    - SFS 2008:355: ICD10 Code and Name (Wide)
    - SFS 2008:355: ICD10 Code and Name (Default)
    - SFS 2008:355: ICD10 Code and Name (Narrow)
    - SFS 2008:355: ICD10 Code and Personal Number
    - SFS 2008:355: ICD10 Description
    - SFS 2008:355: Name and Health Information
    - SFS 2008:355: Name and Personal Number
    - SFS 2008:355: Name and Sensitive Disease or Drug

- SFS 2008:355: Personal Number
- SFS 2008:355: Personal Number and Health Information
- SFS 2008:355: Personal Number and Sensitive Disease or Drug
- SFS 2008:355: SPSS Text File

- UK
  - Information Governance Toolkit

    Policy for compliance with the NHS Information Governance Toolkit (IG Toolkit). The rules for this policy are:

    - IG Toolkit: DICOM
    - IG Toolkit: DNA Profile (Default)
    - IG Toolkit: DNA Profile (Narrow)
    - IG Toolkit: DOB and Name
    - IG Toolkit: Driver Number and Name (Wide)
    - IG Toolkit: Driver Number and Name (Default)
    - IG Toolkit: ICD9 Code
    - IG Toolkit: ICD9 Code and Full Name
    - IG Toolkit: ICD9 Description and Full Name
    - IG Toolkit: ICD10 Code
    - IG Toolkit: ICD10 Code and Full Name
    - IG Toolkit: ICD10 Description and Full Name
    - IG Toolkit: Name and Common Medical Condition (Default)
    - IG Toolkit: Name and Common Medical Condition (Narrow)
    - IG Toolkit: Name and Sensitive Disease or Drug (Default)
    - IG Toolkit: Name and Sensitive Disease or Drug (Narrow)
    - IG Toolkit: National Insurance Number and Name
    - IG Toolkit: NDC Number (Default)
    - IG Toolkit: NDC Number (Narrow)
    - IG Toolkit: NHS Number (Wide)
    - IG Toolkit: NHS Number (Default)
    - IG Toolkit: NHS Number (Narrow)
    - IG Toolkit: Passport Number and Name
    - IG Toolkit: Tax ID Number and Name
  - UK DPA

    The UK Data Protection Act 1998 provides provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The policy contains rules to detect UK Personally Identifiable Information (PII) like National Insurance numbers, passport numbers, alone or in combination with credit card numbers. The rules for this policy are:

    - UK DPA: UK National Insurance Number and CCN
    - UK DPA: UK Driver Number and CCN
    - UK DPA: UK Driver Number and CCN (Wide)
    - UK DPA: UK Passport Number and CCN

- UK DPA: UK Tax ID Number and CCN
- UK DPA: UK National Insurance Number
- UK DPA: UK Driver Number
- UK DPA: UK Passport Number
- UK DPA: UK Tax ID Number
- UK DPA: NHS Numbers (wide)
- UK DPA: NHS Numbers (narrow)
- UK DPA: NHS Numbers (default)

- EU Directive 95/46/EC

  Directive 95/46/EC on the protection of personal data regulates the processing of personal data. The policy detects combinations of national identification numbers and credit card numbers prevalent in Europe. The rules for this policy are:

  - EU Directive 95/46/EC: Dutch Citizen Service Number and CCN
  - EU Directive 95/46/EC: French INSEE Number and CCN
  - EU Directive 95/46/EC: Italian Codice Fiscale Number and CCN
  - EU Directive 95/46/EC: Norwegian Personal Number and CCN
  - EU Directive 95/46/EC: Spanish DNI Number and CCN
  - EU Directive 95/46/EC: Swiss New Format AHV and CCN
  - EU Directive 95/46/EC: Swiss Old Format AHV and CCN
  - EU Directive 95/46/EC: UK National Insurance Number and CCN

- EU Finance

  Policy for promoting regulatory compliance with the requirements of the Basel Committee on Banking Supervision. The policy contains rules to detect financial data like account numbers, passwords, or magnetic credit card tracks. Additional rules detect combinations of Personally Identifiable Information (PII) like credit cards and identification numbers. The rules for this policy are:

  - EU Finance: CCN: with National ID
  - EU Finance: CCN and PIN number
  - EU Finance: Suspected passwords
  - EU Finance: Credit Card Magnetic Strips
  - EU Finance: Password dissemination for Web traffic
  - EU Finance: 5-8 digit Account Numbers
  - EU Finance: 10 digit Account Numbers
  - EU Finance: 9 digit Account Numbers

Hong Kong

Policies for promoting compliance with Hong Kong Privacy regulations.

- Hong Kong Personal Data Privacy Ordinance

  The Hong Kong Personal Data Privacy Ordinance (PDPO) protects the privacy interests of living individuals in relation to personal data. The Ordinance covers any data relating directly or indirectly to a living individual from which it is practicable to ascertain the identity of the individual and which are in a form in

which access or processing is practicable, including, for example, Hong Kong Identity Card Number, name and address. The rules for this policy are:

- Hong Kong PDPO: ID Number (Wide)
- Hong Kong PDPO: ID Number (Default)
- Hong Kong PDPO: ID Number (Narrow)
- Hong Kong PDPO: ID Number and Address (Wide)
- Hong Kong PDPO: ID Number and Address (Default)
- Hong Kong PDPO: ID Number and Address (Narrow)
- Hong Kong PDPO: ID Number or Surname (Wide)
- Hong Kong PDPO: ID Number and Surname (Default)
- Hong Kong PDPO: ID (formal form) and Common Surname
- Hong Kong PDPO: ID Number, Surname and Address (Wide)
- Hong Kong PDPO: ID Number, Surname and Address (Default)
- Hong Kong PDPO: ID Number, Surname and Address (Narrow)
- Hong Kong PDPO: Surname and Address (Default)
- Hong Kong PDPO: Surname and Address (Narrow)
- Hong Kong PDPO: Surname and Address (Wide)

Iceland

Policies for promoting compliance with Iceland Privacy regulations.

- Iceland Privacy Act

  The Iceland Act on Protection of Individuals with regard to the Processing of Personal Information (law 77/2000) follows the EU Data Protection Directive and restricts the processing, storage, and transmission of personal and sensitive information. The predefined policy comprises rules for detecting Icelandic identification numbers (Kennitala) of individuals and DNA profiles. The rules for this policy are:

  - Iceland Privacy Act: Kennitala of Individuals (Default)
  - Iceland Privacy Act: Kennitala of Individuals (Wide)
  - Iceland Privacy Act: DNA Sequence

India

- India IT Act

  Policy for detecting sensitive personal information as defined by the India Information Technology Act. The rules for this policy include:

  - India IT Act: Credit Card Number (Default)
  - India IT Act: Credit Card Number (Narrow)
  - India IT Act: Name and Aadhaar Number
  - India IT Act: Name and Common Medical Condition
  - India IT Act: Name and Password (Wide)

- India IT Act: Name and Password (Default)
- India IT Act: Name and Password (Narrow)
- India IT Act: Name and Physical Information
- India IT Act: Name and Sensitive Disease or Drug
- India IT Act: Name and Sexual Orientation
- India IT Act: Password Dissemination for HTTP Traffic (Wide)
- India IT Act: Password Dissemination for HTTP Traffic (Default)
- India IT Act: Password Dissemination for HTTP Traffic (Narrow)
- India IT Act: Password Dissemination for non-HTTP/S Traffic (Wide)
- India IT Act: Password Dissemination for non-HTTP/S Traffic (Default)
- India IT Act: Password Dissemination for non-HTTP/S Traffic (Narrow)

Israel

Policies for promoting compliance with Israel Privacy regulations.

- Israeli Health Care

  Policy for detection of protected health information of Israeli citizens, to promote compliance with Israeli privacy rules and Israeli patients rights law of 1996.

  - Israeli Health Care: DICOM
  - Israeli Health Care: Identity Number and General Medical Information
  - Israeli Health Care: Identity Number and Sensitive Medical Information
  - Israeli Health Care: Name and General Medical Information
  - Israeli Health Care: Name and Sensitive Medical Information
  - Israeli Health Care: SPSS Text File

Japan

Policies for promoting compliance with Japan Privacy regulations.

- Japan PIP

  The Japan Personal Information Protection Law (PIP) states a set of obligations for companies handling personal data. The law protects individuals by regulating the handling of information by private sector businesses. The policy contains rules to protect Japan PII (Personally Identifiable Information), either alone or with a credit card number. The rules for this policy are:

  - JPIP: Account and Credit Card Number
  - JPIP: Credit Card Numbers
  - JPIP: Telephone Numbers
  - JPIP: Surname and Account
  - JPIP: Surname and Driver License
  - JPIP: Surname and Pension Number
  - JPIP: Surname and Ledger Number

- JPIP: E-mail Addresses
- JPIP: Individual Numbers (Wide)
- JPIP: Individual Numbers (Default)
- JPIP: Individual Numbers (Narrow)
- JPIP: Corporate Numbers (Wide)
- JPIP: Corporate Numbers (Default)
- JPIP: Corporate Numbers (Narrow)

Malaysia

Policies for promoting compliance with Malaysia Privacy regulations.

- Malaysia PDPA

  The Malaysian Personal Data Protection Act of 2009 mandates, among others, that any person in Malaysia who collects or stores any personal data in respect of commercial transactions, should take practical steps to protect the personal data from any loss or unauthorized access or disclosure. Penalties for incompliance comprise fine not exceeding 250000 ringgit or imprisonment for a term not exceeding two years or to both. The policy comprises rules for detection of Malaysian personal information, such as Malaysian ID, alone or in combination with sensitive information such as sensitive health information, credit card numbers, account number, ethnicities and religion etc. Additional rules detect combinations of names with sensitive health information or passwords.

  - Malaysia PDPA: DNA Sequence
  - Malaysia PDPA: ID number
  - Malaysia PDPA: ID Number and Account Number
  - Malaysia PDPA: ID Number and Credit Card Number
  - Malaysia PDPA: ID Number and Crime
  - Malaysia PDPA: ID Number and Ethnicity or Religion
  - Malaysia PDPA: Name and Password (Wide)
  - Malaysia PDPA: Name and Password (Default)
  - Malaysia PDPA: Name and Password (Narrow)
  - Malaysia PDPA: Name and Sensitive Health Information

New Zealand

Policies for promoting compliance with New Zealand Privacy regulations.

- New-Zealand Privacy Act

  New Zealand's Privacy Act of 1993 applies to almost every person, business or organization in New Zealand. The act sets out information privacy principles, which, among others, limit transmission and storage of personal data. The pre-defined policy comprises rules for detection and monitoring of NZ National Health Index (NHI) numbers and DNA information. The rules for this policy are:

  - New Zealand Privacy Act: NHI number (wide)

- New Zealand Privacy Act: NHI number (default)
- New Zealand Privacy Act: DNA Sequence

Norway

Policies for promoting compliance with Norway Privacy regulations.

- Norway Health Data Privacy Act

  The Norway Health Data Privacy Act protects persons from violation of their right to privacy through the processing of personal data. The Act helps to ensure that personal data is processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensures that personal data is of adequate quality. The policy contains rules to detect combinations of Norwegian Personally Identifiable Information (PII) like personnummer and full name, with sensitive health information.

  - Norway HDPA: DICOM
  - Norway HDPA: ICD10 Code
  - Norway HDPA: ICD10 Code and Description
  - Norway HDPA: ICD10 Code and First Name
  - Norway HDPA: ICD10 Code and Full Name
  - Norway HDPA: ICD10 Code and Last Name
  - Norway HDPA: ICD10 Code and PIN Number
  - Norway HDPA: ICD10 Description
  - Norway HDPA: Name and Health Information
  - Norway HDPA: Name and Personal Number
  - Norway HDPA: Personal Number (Wide)
  - Norway HDPA: Personal Number (Default)
  - Norway HDPA: Personal Number (Narrow)
  - Norway HDPA: Personal Number and Health Information
  - Norway HDPA: SPSS Text File

Philippines

Policies for promoting compliance with Philippines Privacy regulations.

- Philippines Data Privacy Act

  The Philippines Data Privacy Act of 2012 adopts generally accepted international principles and standards for personal data protection. It states that all sensitive personal information maintained by the government shall be secured with the use of the most appropriate standard recognized by the information and communications technology industry. Sensitive personal information includes information about an individual’s age, color, health, genetics, offense committed, or ID numbers. The rules for this policy are:

  - Philippines DPA: DNA Profile
  - Philippines DPA: Name and Address (Wide)

- Philippines DPA: Name and Address (Default)
- Philippines DPA: Name and Address (Narrow)
- Philippines DPA: Name and CCN (Wide)
- Philippines DPA: Name and CCN (Default)
- Philippines DPA: Name and CCN (Narrow)
- Philippines DPA: Name and Common Medical Condition (Wide)
- Philippines DPA: Name and Common Medical Condition (Default)
- Philippines DPA: Name and Crime (Wide)
- Philippines DPA: Name and Crime (Default)
- Philippines DPA: Name and Date of Birth (Wide)
- Philippines DPA: Name and Date of Birth (Default)
- Philippines DPA: Name and Password (Wide)
- Philippines DPA: Name and Password (Default)
- Philippines DPA: Name and Password (Narrow)
- Philippines DPA: Name and PhilHealth Identification Number (Wide)
- Philippines DPA: Name and PhilHealth Identification Number (Default)
- Philippines DPA: Name and Physical Information (Wide)
- Philippines DPA: Name and Physical Information (Default)
- Philippines DPA: Name and Sensitive Disease or Drug (Wide)
- Philippines DPA: Name and Sensitive Disease or Drug (Default)
- Philippines DPA: Name and SSS Number (Wide)
- Philippines DPA: Name and SSS Number (Default)
- Philippines DPA: Name and TIN (Wide)
- Philippines DPA: Name and TIN (Default)
- Philippines DPA: Password Dissemination for HTTP Traffic (Wide)
- Philippines DPA: Password Dissemination for HTTP Traffic (Default)
- Philippines DPA: Password Dissemination for HTTP Traffic (Narrow)
- Philippines DPA: PhilHealth Identification Number (Wide)
- Philippines DPA: PhilHealth Identification Number (Default)
- Philippines DPA: SSS Number (Wide)
- Philippines DPA: SSS Number (Default)
- Philippines DPA: TIN Number (Wide)
- Philippines DPA: TIN Number (Default)

Russia

Policies for promoting compliance with Russia Privacy regulations.

- Russian Federal Law No. 152-FZ

Federal Law No. 152-FZ regulates activities related to processing of personal data in the Russian Federation by means of automation equipment, and mandates protecting the confidentiality of personal information. The policy detects personal information that should be protected, like passport number, personal pension account number (SNILS), Taxpayer Identification Numbers (INN), personal phone numbers, etc., in proximity to Russian names. The rules for this policy are:

- Russia Federal Act 152-FZ: Personal Pension Account Number (SNILS) and Name
- Russia Federal Act 152-FZ: Moscow Social Card Number and Name
- Russia Federal Act 152-FZ: Passport Number and Name
- Russia Federal Act 152-FZ: Phone Number and Name
- Russia Federal Act 152-FZ: Primary State Registration Number (OGRNIP) and Name
- Russia Federal Act 152-FZ: Taxpayer Identification Number of Individuals and Name

- Russian Federation IIIP

  The law of the Russian Federation on Information, Informatization, and Information Protection of 1995 covers both the government and private sectors and imposes a code of fair information practices and other restrictions on the processing of personal and sensitive information. The pre-defined policy comprises rules for detection of a Russian passport number when appearing together with Russian full names and for detection of DNA information. The rules for this policy are:

  - Russian Federation IIIP: DNA Sequence
  - Russian Federation IIIP: Passport Number
  - Russian Federation IIIP: Passport Number and Name (Wide)
  - Russian Federation IIIP: Passport Number and Name (Default)
  - Russian Federation IIIP: Passport Number and Name (Narrow)

Singapore

Policies for promoting compliance with Singapore Privacy regulations.

- Singapore ETA

  The Singapore Electronic Transaction Act (ETA) mandates applying adequate measures to assure the confidentiality of electronic records, imposing fines and incarceration for compromising confidentiality. It also outlines the liability of directors, managers, secretaries and other officers of the body corporate in case of a breach. The rules for this policy are:

  - Singapore ETA: Identification Number (Wide)
  - Singapore ETA: Identification Number (Default)
  - Singapore ETA: Identification Number and CCN
  - Singapore ETA: Name and Address (Default)
  - Singapore ETA: Name and Address (Narrow)

- Singapore PDPA

  The Singapore Personal Data Protection Act of 2012 covers all private sector organizations engaged in data activities within Singapore. It regulates the management of personal data by businesses and imposes financial penalties. The rules for this policy are:

  - Singapore PDPA: DNA Sequence
  - Singapore PDPA: Identification Number (Wide)
  - Singapore PDPA: Identification Number (Default)
  - Singapore PDPA: Name and Address (Default)
  - Singapore PDPA: Name and Address (Narrow)
  - Singapore PDPA: Name and CCN
  - Singapore PDPA: Name and Identification Number (Default)
  - Singapore PDPA: Name and Identification Number (Narrow)
  - Singapore PDPA: Name and Password (Wide)
  - Singapore PDPA: Name and Password (Default)
  - Singapore PDPA: Name and Password (Narrow)
  - Singapore PDPA: Name and Phones Number (Wide)
  - Singapore PDPA: Name and Phones Number (Default)
  - Singapore PDPA: Name and Phones Number (Narrow)
  - Singapore PDPA: Name and Sensitive Health Information
  - Singapore PDPA: Phones Number (Wide)
  - Singapore PDPA: Phones Number (Default)
  - Singapore PDPA: Phones Number (Narrow)

South Africa

Policies for promoting compliance with South Africa Privacy regulations.

- South Africa ECT Act

  The Republic of South Africa Electronic Communication and Transaction Act defines a national e-strategy for the Republic and also prevents abuse of information systems. Chapter VIII of the act deals with protection of personal information. The policy detects combinations of valid South Africa ID number with credit card numbers. The rules for this policy is:

  - South Africa ECT Act: ID Number and CCN (Wide)
  - South Africa ECT Act: ID Number and CCN (Default)
- South Africa POPI

  The “Protection of Personal Information” (POPI) bill regulates the collection, dissemination, use and retention of private information.The rules for this policy are:

  - South Africa POPI: DNA Sequence
  - South Africa POPI: ID Number (Wide)

- South Africa POPI: ID Number (Default)
- South Africa POPI: ID Number and CCN (Wide)
- South Africa POPI: ID Number and CCN (Default)
- South Africa POPI: ID Number and Crime (Wide)
- South Africa POPI: ID Number and Crime (Default)
- South Africa POPI: ID Number and Date of Birth (Wide)
- South Africa POPI: ID Number and Date of Birth (Default)
- South Africa POPI: ID Number and Ethnicity or Religion (Wide)
- South Africa POPI: ID Number and Ethnicity or Religion (Default)
- South Africa POPI: ID Number and Health Information (Wide)
- South Africa POPI: ID Number and Health Information (Default)
- South Africa POPI: Name and Password (Wide)
- South Africa POPI: Name and Password (Default)
- South Africa POPI: Name and Password (Narrow)
- South Africa POPI: Name and Personal Finance Term
- South Africa POPI: ID Number and SWIFT Code (Wide)
- South Africa POPI: ID Number and Account Number (Default)
- South Africa POPI: Name and Sensitive Health Information

Switzerland

Policies for promoting compliance with Switzerland Privacy regulations.

- Swiss Confederation Federal Act of Data Protection

  The Federal Act of Data Protection of 1992 regulates personal information held by government and private bodies. The Act requires that information must be legally and fairly collected and places limits on its use and disclosure to third parties. Transfers to other nations must be registered and the recipient nation must have equivalent laws. The pre-defined policy comprises rules for detection of Swiss AHV numbers and DNA information. The rules for this policy are:

  - Swiss Federal Act of Data Protection: Old format AHV
  - Swiss Federal Act of Data Protection: new format AHV
  - Swiss Federal Act of Data Protection: DNA Sequence

Taiwan

Policies for promoting compliance with Taiwan Privacy regulations.

- Taiwan PIPA

  Taiwan - Personal Information Protection Act. The rules for this policy are:

  - Taiwan PIPA: ID Card Number (Wide)
  - Taiwan PIPA: ID Card Number (Default)
  - Taiwan PIPA: ID Card Number and Surname (Wide)
  - Taiwan PIPA: ID Card Number and Surname (Default)

- Taiwan PIPA: ID Card Number, Surname and Private Information (Wide)
- Taiwan PIPA: ID Card Number, Surname and Private Information (Default)

Thailand

Policies for promoting compliance with Thailand Privacy regulations.

- Thailand Official Information Act

  The Thailand Official Information Act, B.E. 2540 of 1997 sets a code of information practices for the processing of personal information by state agencies. The act mandates, among other things, not to disclose personal information to other state agencies or other persons without prior consent given in writing, except in limited circumstances. The pre-defined policy comprises rules for detecting validated Thai National ID Numbers and DNA sequences. The rules for this policy are:

  - Thailand Official Information Act: National ID (wide)
  - Thailand Official Information Act: National ID (default)
  - Thailand Official Information Act: DNA Sequence

Turkey

- Turkey Protection of Personal Data Draft Law

  A policy for protection of personal information, in accordance with Turkey's "Protection of Personal Data" Draft Law. The rules for this policy are:

  - Turkey Protection of Personal Data Draft Law: TC Kimlik
  - Turkey Protection of Personal Data Draft Law: TC Kimlik one support
  - Turkey Protection of Personal Data Draft Law: TC Kimlik and CCN
  - Turkey Protection of Personal Data Draft Law: Spreadsheets
  - Turkey Protection of Personal Data Draft Law: Confidential in Header Footer

United States of America - State Privacy Regulations

Policies for promoting compliance with various states' privacy regulations

Alabama Information Protection

Alabama standard 681S2-00 requires that executive branch agencies, boards, and commissions shall identify Personally Identifiable Information (PII), evaluate the risk and impact of loss or unauthorized disclosure of PII, and implement PII confidentiality safeguards. The policy detects combinations of PII like social security and credit card numbers. Additional rules detect passwords. The rules for this policy are:

- Alabama Information Protection: Account and Password
- Alabama Information Protection: Name and CCN
- Alabama Information Protection: Name and Password (Wide)
- Alabama Information Protection: Name and Password (Default)
- Alabama Information Protection: Name and Password (Narrow)
- Alabama Information Protection: Name and SSN
- Alabama Information Protection: Password Dissemination for HTTP Traffic (Wide)
- Alabama Information Protection: Password Dissemination for HTTP Traffic (Default)
- Alabama Information Protection: Password Dissemination for HTTP Traffic (Narrow)

Alaska Personal Information Protection Act

Alaska HB 65 of 2008 notifies consumers when a data breach concerning personal information has occurred. Personal information is defined to include unencrypted information on an individual, which consists of the individual's name and one or more of several other pieces of information, including social security number, driver's license number, account number, password, or other access codes. The policy detects combinations of full names with social security, driver's license, or credit card numbers. Additional rules detect passwords and account numbers. The rules for this policy are:

- Alaska Personal Information Protection Act: Name and SSN
- Alaska Personal Information Protection Act: Name and DL
- Alaska Personal Information Protection Act: Name and CCN
- Alaska Personal Information Protection Act: Name and Password (Wide)
- Alaska Personal Information Protection Act: Name and Password (Default)
- Alaska Personal Information Protection Act: Name and Password (Narrow)

- Alaska Personal Information Protection Act: Password Dissemination for HTTP Traffic (Wide)
- Alaska Personal Information Protection Act: Password Dissemination for HTTP Traffic (Default)
- Alaska Personal Information Protection Act: Password Dissemination for HTTP Traffic (Narrow)
- Alaska Personal Information Protection Act: Account and Password

Arizona Data Breach Notification Law

Arizona SB 1338 of 2006 requires businesses to provide consumer notification of data breaches. It is applicable to any person that conducts business in Arizona and owns or licenses computerized data that includes personal information or maintains such data. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and Arizona driver's license numbers. The rules for this policy are:

- Arizona Data Breach Notification Law: SSN with AZ driver license
- Arizona Data Breach Notification Law: SSN with CCN

Arkansas Personal Information Protection Act

Arkansas SB 1167 of 2005 requires organizations to protect personal information of Arkansas residents (including personal health information) and to inform Arkansas customers when their private information is disclosed during a security breach. The policy comprises rules that detect combinations of personally identifiable information with sensitive information such as protected health information, credit card numbers, or passwords. The rules for this policy are:

- Arkansas SB 1167: Arkansas Driver License with Sensitive Disease or Drug
- Arkansas Personal Information Protection Act: CCN with Arkansas Driver License
- Arkansas Personal Information Protection Act: Names with Sensitive Disease or Drug (Default)
- Arkansas Personal Information Protection Act: Names with Sensitive disease or drug (Narrow)
- Arkansas Personal Information Protection Act: Password Dissemination for HTTP Traffic (Wide)
- Arkansas Personal Information Protection Act: Password Dissemination for HTTP Traffic (Default)
- Arkansas Personal Information Protection Act: Password Dissemination for HTTP Traffic (Narrow)
- Arkansas Personal Information Protection Act: Password Dissemination for non-HTTP/S Traffic (Wide)
- Arkansas Personal Information Protection Act: Password Dissemination for non-HTTP/S Traffic (Default)

- Arkansas Personal Information Protection Act: Password Dissemination for non-HTTP/S Traffic (Narrow)
- Arkansas Personal Information Protection Act: SSN with CCN
- Arkansas Personal Information Protection Act: SSN with Sensitive Disease or Drug

California Personal Information Privacy Act

- California SB 1386 of 2003, amended by AB 1950 of 2004 and AB 1298, requires a person or business conducting business in California and any agency to notify Californians if their personal information is disclosed during a security breach. This law adds medical information to the information to be protected and extends the responsibility to organizations outside of the State, if they collect information about California residents. It does not apply to organizations that are subject to other privacy laws. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. Additional rules detect passwords. The rules for this policy are:
  - California Personal Information Privacy Act: 5-8 Digit Account Number
  - California Personal Information Privacy Act: 9 Digit Account Number
  - California Personal Information Privacy Act: 10 Digit Account Number
  - California Personal Information Privacy Act: California Driver License and Sensitive Disease or Drug
  - California Personal Information Privacy Act: CCN (Default)
  - California Personal Information Privacy Act: CCN (Narrow)
  - California Personal Information Privacy Act: CCN and California Driver License Number
  - California Personal Information Privacy Act: CCN and Sensitive Disease or Drug
  - California Personal Information Privacy Act: Celebrity Name and Sensitive Disease or Drug
  - California Personal Information Privacy Act: Celebrity Name and Common Medical Condition
  - California Personal Information Privacy Act: CCN and Common Medical Condition
  - California Personal Information Privacy Act: DNA Profile
  - California Personal Information Privacy Act: ICD9 Code and Name
  - California Personal Information Privacy Act: ICD9 Description and Name
  - California Personal Information Privacy Act: ICD10 Code and Name
  - California Personal Information Privacy Act: ICD10 Description and Name
  - California Personal Information Privacy Act: Name and Common Medical Condition (Default)
  - California Personal Information Privacy Act: Name and Common Medical Condition (Narrow)
  - California Personal Information Privacy Act: Name and HICN

- California Personal Information Privacy Act: Name and Sensitive Disease or Drug (Default)
- California Personal Information Privacy Act: Name and Sensitive Disease or Drug (Narrow)
- California Personal Information Privacy Act: Password Dissemination for HTTP Traffic (Wide)
- California Personal Information Privacy Act: Password Dissemination for HTTP Traffic (Default)
- California Personal Information Privacy Act: Password Dissemination for HTTP Traffic (Narrow)
- California Personal Information Privacy Act: Password Dissemination for non-HTTP/S Traffic (Wide)
- California Personal Information Privacy Act: Password Dissemination for non-HTTP/S Traffic (Default)
- California Personal Information Privacy Act: Password Dissemination for non-HTTP/S Traffic (Narrow)
- California Personal Information Privacy Act: SSN
- California Personal Information Privacy Act: SSN and Common Medical Condition
- California Personal Information Privacy Act: SSN and Sensitive Disease or Drug
- California Personal Information Privacy Act: SSN and California Driver License Number
- California Personal Information Privacy Act: SSN and CCN

Colorado Consumer Protection Act

Colorado HB 06-1119 of 2006 requires that an individual or commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The individual or the commercial entity shall give notice as soon as possible to the affected Colorado residents unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Colorado Consumer Protection Act: SSN: with Colorado driver license
- Colorado Consumer Protection Act: SSN with CCN
- Colorado Consumer Protection Act: Name with SSN
- Colorado Consumer Protection Act: Name with Colorado driver license
- Colorado Consumer Protection Act: Name with CCN
- Colorado Consumer Protection Act: SSN with DNA profile

Connecticut Data Breach Notification Act

Connecticut SB 650 of 2006 requires that any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security, following the discovery of the breach, to any resident of this state whose personal information was breached or is reasonably believed to have been breached. Such notice shall be made without unreasonable delay but not later than ninety days after the discovery of such breach. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Connecticut Data Breach Notification Act: Name and SSN
- Connecticut Data Breach Notification Act: Name and DL
- Connecticut Data Breach Notification Act: Name and CCN
- Connecticut Data Breach Notification Act: Name and Password (Wide)
- Connecticut Data Breach Notification Act: Name and Password (Default)
- Connecticut Data Breach Notification Act: Name and Password (Narrow)
- Connecticut Data Breach Notification Act: Password Dissemination for HTTP Traffic (Wide)
- Connecticut Data Breach Notification Act: Password Dissemination for HTTP Traffic (Default)
- Connecticut Data Breach Notification Act: Password Dissemination for HTTP Traffic (Narrow)
- Connecticut Data Breach Notification Act: Account and Password

Delaware Data Breach Notification

Delaware HB 116 of 2005 requires that any person who conducts business in this State and who owns, licenses, or maintains computerized data that includes personal information shall provide notice of any breach of security, following determination of the breach of security, to any resident of this state whose personal information was breached or is reasonably believed to have been breached; unless, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Delaware Data Breach Notification: Name and SSN
- Delaware Data Breach Notification: Name and CCN
- Delaware Data Breach Notification: Name and Password (Wide)
- Delaware Data Breach Notification: Name and Password (Default)
- Delaware Data Breach Notification: Name and Password (Narrow)
- Delaware Data Breach Notification: Password Dissemination for HTTP Traffic (Wide)

- Delaware Data Breach Notification: Password Dissemination for HTTP Traffic (Default)
- Delaware Data Breach Notification: Password Dissemination for HTTP Traffic (Narrow)
- Delaware Data Breach Notification: Account and Password
- Delaware Data Breach Notification: Credit cards and Sensitive Disease or drug
- Delaware Data Breach Notification: Credit Card and Common Medical Condition

District of Columbia Security Breach Notification Act

District of Columbia CB 16-810, signed into law as the Consumer Personal Information Security Breach Notification Act in 2007, requires any person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a breach of the security of the system, shall promptly notify any District of Columbia resident whose personal information was included in the breach. The notification shall be made n the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (d) of this section, and with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- District of Columbia Security Breach Notification Act: Name and SSN
- District of Columbia Security Breach Notification Act: Name and DL
- District of Columbia Security Breach Notification Act: Name and CCN
- District of Columbia Security Breach Notification Act: Name and Password (Wide)
- District of Columbia Security Breach Notification Act: Name and Password (Default)
- District of Columbia Security Breach Notification Act: Name and Password (Narrow)
- District of Columbia Security Breach Notification Act: Password Dissemination for HTTP Traffic (Wide)
- District of Columbia Security Breach Notification Act: Password Dissemination for HTTP Traffic (Default)
- District of Columbia Security Breach Notification Act: Password Dissemination for HTTP Traffic (Narrow)

Florida Information Protection Act

Florida SB 1524 of 2014 requires that a corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information shall provide notice to the department of any breach of security affecting 500 of more individuals in this state. Such notice must be provided to the department as expeditiously as practicable, but no later than 30 days after the

determination of the breach or reason to believe a breach occurred. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. Additional rules protect passwords. The rules for this policy are:

- Florida Information Protection Act: SSN with CCN
- Florida Information Protection Act: CCN with FL Driver License
- Florida Information Protection Act: Password Dissemination for non-HTTP/S Traffic (Wide)
- Florida Information Protection Act: Password Dissemination for non-HTTP/S Traffic (Default)
- Florida Information Protection Act: Password Dissemination for non-HTTP/S Traffic (Narrow)

Georgia Personal Data Security Act

Georgia SB 230 of 2005 requires that in the vent of a breach of the security of the system, which system is maintained by a third-party agent for a covered entity, the third-party agent shall notify the covered entity of such breach as expeditiously as practicable but no later than 72 hours after the determination of such breach or reason to believe such breach has occurred. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. Additional rules detect passwords. The rules for this policy are:

- Georgia Personal Data Security Act: SSN with CCN
- Georgia Personal Data Security Act: CCN with GA Driver License
- Georgia Personal Data Security Act: Password Dissemination for HTTP Traffic (Wide)
- Georgia Personal Data Security Act: Password Dissemination for HTTP Traffic (Default)
- Georgia Personal Data Security Act: Password Dissemination for HTTP Traffic (Narrow)
- Georgia Personal Data Security Act: Password Dissemination for non-HTTP/S Traffic (Wide)
- Georgia Personal Data Security Act: Password Dissemination for non-HTTP/S Traffic (Default)
- Georgia Personal Data Security Act: Password Dissemination for non-HTTP/S Traffic (Narrow)

Hawaii Security Breach of Personal Information

Hawaii SB 2290 of 2007 requires that any business that owns or licenses personal information of residents of Hawaii, any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), or any government agency that collects personal information for specific government purposes shall provide notice to the affected person that there has been a security breach, following discovery or notification of the breach. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit

card, and driver's license numbers. Additional rules detect passwords and account numbers. The rules for this policy are:

- Hawaii Security Breach of Personal Information: Name and SSN
- Hawaii Security Breach of Personal Information: Name and DL
- Hawaii Security Breach of Personal Information: Name and CCN
- Hawaii Security Breach of Personal Information: Name and Password (Wide)
- Hawaii Security Breach of Personal Information: Name and Password (Default)
- Hawaii Security Breach of Personal Information: Name and Password (Narrow)
- Hawaii Security Breach of Personal Information: Password Dissemination for HTTP Traffic (Wide)
- Hawaii Security Breach of Personal Information: Password Dissemination for HTTP Traffic (Default)
- Hawaii Security Breach of Personal Information: Password Dissemination for HTTP Traffic (Narrow)
- Hawaii Security Breach of Personal Information: Account and Password

Idaho Data Breach Notification

Idaho SB 1374 of 2006 requires a city, county, or stage agency, individual, or commercial entity that conducts business in Idaho and that owns or licenses computerized data that includes personal information about a resident of Idaho shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information about an Idaho resident has occurred or is reasonably likely to occur, the agency, individual, or commercial entity shall give notice as soon as possible to the affected Idaho resident. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. Additional rules detect passwords and account numbers. The rules for this policy are:

- Idaho Data Breach Notification: Name and SSN
- Idaho Data Breach Notification: Name and DL
- Idaho Data Breach Notification: Name and CCN
- Idaho Data Breach Notification: Name and Password (Wide)
- Idaho Data Breach Notification: Name and Password (Default)
- Idaho Data Breach Notification: Name and Password (Narrow)
- Idaho Data Breach Notification: Password Dissemination for HTTP Traffic (Wide)
- Idaho Data Breach Notification: Password Dissemination for HTTP Traffic (Default)
- Idaho Data Breach Notification: Password Dissemination for HTTP Traffic (Narrow)
- Idaho Data Breach Notification: Account and Password

Illinois Personal Information Protection Act

Illinois HB 1633 of 2006 requires data collectors to provide notification of a security breach after discovery, even if data has not been accessed by unauthorized persons. This state law affects all data collectors that own or license personal information (PI), or maintains computerized data that includes PI. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, state ID, and driver's license numbers. Additional rules detect passwords. The rules for this policy are:

- Illinois Personal Information Protection Act: SSN with CCN
- Illinois Personal Information Protection Act: CCN with Illinois Driver License
- Illinois Personal Information Protection Act: CCN with Illinois State ID
- Illinois Personal Information Protection Act: Password Dissemination for HTTP Traffic (Wide)
- Illinois Personal Information Protection Act: Password Dissemination for HTTP Traffic (Default)
- Illinois Personal Information Protection Act: Password Dissemination for HTTP Traffic (Narrow)
- Illinois Personal Information Protection Act: Password Dissemination for non-HTTP/S Traffic (Wide)
- Illinois Personal Information Protection Act: Password Dissemination for non-HTTP/S Traffic (Default)
- Illinois Personal Information Protection Act: Password Dissemination for non-HTTP/S Traffic (Narrow)

Indiana Disclosure of Security Breach law

Indiana SB 503 of 2006 requires that after discovering or being notified of a breach of the security of data, database owners shall disclose the breach to an Indiana resident whose: (1) unencrypted personal information was or may have been acquired by an unauthorized person; or (2) encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key; if the database owners know, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud affecting the Indiana resident. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Indiana Disclosure of Security Breach law: Name and SSN
- Indiana Disclosure of Security Breach law: Name and DL
- Indiana Disclosure of Security Breach law: Name and CCN
- Indiana Disclosure of Security Breach law: Name and Password (Wide)
- Indiana Disclosure of Security Breach law: Name and Password (Default)
- Indiana Disclosure of Security Breach law: Name and Password (Narrow)
- Indiana Disclosure of Security Breach law: Password Dissemination for HTTP Traffic (Wide)

- Indiana Disclosure of Security Breach law: Password Dissemination for HTTP Traffic (Default)
- Indiana Disclosure of Security Breach law: Password Dissemination for HTTP Traffic (Narrow)
- Indiana Disclosure of Security Breach law: Account and Password

Iowa Data Breach Notification Law

Iowa S.F. 2308 of 2008 requires that any person who owns or licenses computerized data that includes a consumer's personal information that is used in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security shall give notice of the breach of security, following discovery of such breach of security, to any consumer whose personal information was included in the information that was breached. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Iowa Data Breach Notification Law: Name and SSN
- Iowa Data Breach Notification Law: Name and DL
- Iowa Data Breach Notification Law: Name and CCN
- Iowa Data Breach Notification Law: Name and Password (Wide)
- Iowa Data Breach Notification Law: Name and Password (Default)
- Iowa Data Breach Notification Law: Name and Password (Narrow)
- Iowa Data Breach Notification Law: Password Dissemination for HTTP Traffic (Wide)
- Iowa Data Breach Notification Law: Password Dissemination for HTTP Traffic (Default)
- Iowa Data Breach Notification Law: Password Dissemination for HTTP Traffic (Narrow)
- Iowa Data Breach Notification Law: DNA profile

Kansas Protection of Consumer Information

Kansas SB 196 requires that a person that conducts business in this state, or a government, governmental subdivision, or agency that owns or licenses computerized data that includes personal information shall, when it becomes aware of any breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines that the misuse of information has occurred or is reasonably likely to occur, the person or government, governmental subdivision, or agency shall give notice as soon as possible to the affected Kansas resident. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Kansas Protection of Consumer Information: Name and SSN
- Kansas Protection of Consumer Information: Name and DL
- Kansas Protection of Consumer Information: Name and CCN

- Kansas Protection of Consumer Information: Name and Password (Wide)
- Kansas Protection of Consumer Information: Name and Password (Default)
- Kansas Protection of Consumer Information: Name and Password (Narrow)
- Kansas Protection of Consumer Information: Password Dissemination for HTTP Traffic (Wide)
- Kansas Protection of Consumer Information: Password Dissemination for HTTP Traffic (Default)
- Kansas Protection of Consumer Information: Password Dissemination for HTTP Traffic (Narrow)
- Kansas Protection of Consumer Information: Account and Password

Kentucky Data Breach Notification

Kentucky HB 232, signed into law in 2014, requires any person or business entity that conducts business in Kentucky to provide notification in case of an unauthorized acquisition of unencrypted, unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information (PII) maintained by the information holder as part of a database regarding multiple individuals that causes or leads the information holder to believe has caused or will cause identity theft or fraud against a Kentucky resident. Upon notification or discovery of a breach of the security of the system, an information holder must notify any resident of Kentucky whose unencrypted information was or is reasonably believed to have been acquired by an unauthorized person. It is applicable to any person that conducts business in the state and owns or licenses computerized data or maintains such data. The policy detects combinations of PII like social security, credit card, and driver's license numbers. The rules for this policy are:

- Kentucky Data Breach Notification: Account and Password
- Kentucky Data Breach Notification: Name and CCN
- Kentucky Data Breach Notification: Name and Password (Wide)
- Kentucky Data Breach Notification: Name and Password (Default)
- Kentucky Data Breach Notification: Name and Password (Narrow)
- Kentucky Data Breach Notification: Name and SSN
- Kentucky Data Breach Notification: Password Dissemination for HTTP Traffic (Wide)
- Kentucky Data Breach Notification: Password Dissemination for HTTP Traffic (Default)
- Kentucky Data Breach Notification: Password Dissemination for HTTP Traffic (Narrow)

Louisiana Data Breach Notification

Louisiana SB 205 of 2006 demands notification to any Louisiana resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person as a result of a security breach. The policy detects

combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Louisiana Data Breach Notification: Name and SSN
- Louisiana Data Breach Notification: Name and DL
- Louisiana Data Breach Notification: Name and CCN
- Louisiana Data Breach Notification: Name and Password (Wide)
- Louisiana Data Breach Notification: Name and Password (Default)
- Louisiana Data Breach Notification: Name and Password (Narrow)
- Louisiana Data Breach Notification: Password Dissemination for HTTP Traffic (Wide)
- Louisiana Data Breach Notification: Password Dissemination for HTTP Traffic (Default)
- Louisiana Data Breach Notification: Password Dissemination for HTTP Traffic (Narrow)
- Louisiana Data Breach Notification: Account and Password

Maine Data Breach Notification Law

Maine LD 1671 of 2006 requires that an information broker that maintains computerized data that includes personal information that becomes aware of a breach of the security of the system shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused, and shall give notice of a breach of the security of the system, following discovery or notification of the security breach, to a resident of this state whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Maine Data Breach Notification Law: Name and SSN
- Maine Data Breach Notification Law: Name and DL
- Maine Data Breach Notification Law: Name and CCN
- Maine Data Breach Notification Law: Name and Password (Wide)
- Maine Data Breach Notification Law: Name and Password (Default)
- Maine Data Breach Notification Law: (Narrow)
- Maine Data Breach Notification Law: Password Dissemination for HTTP Traffic (Wide)
- Maine Data Breach Notification Law: Password Dissemination for HTTP Traffic (Default)
- Maine Data Breach Notification Law: Password Dissemination for HTTP Traffic (Narrow)
- Maine Data Breach Notification Law: Account and Password

Maryland Personal Information Protection Act

Maryland HB 208 of 2008 requires that a business that owns or licenses computerized data that includes personal information of an individual residing in the state, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach. It is applicable to any person that conducts business in the state and owns or licenses computerized data or maintains such data. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Maryland Personal Information Protection Act: Name and SSN
- Maryland Personal Information Protection Act: Name and DL
- Maryland Personal Information Protection Act: Name and CCN
- Maryland Personal Information Protection Act: Name and Password (Wide)
- Maryland Personal Information Protection Act: Name and Password (Default)
- Maryland Personal Information Protection Act: Name and Password (Narrow)
- Maryland Personal Information Protection Act: Password Dissemination for HTTP Traffic (Wide)
- Maryland Personal Information Protection Act: Password Dissemination for HTTP Traffic (Default)
- Maryland Personal Information Protection Act: Password Dissemination for HTTP Traffic (Narrow)
- Maryland Personal Information Protection Act: Account and Password

Massachusetts Protection of Personal Information

Massachusetts 201 CMR 17 requires that every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to (a) the size, scope, and type of business of the person obligated to safeguard the personal information under such comprehensive information security program; (b) the amount of resources available to such person; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. The safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns or licenses such information may be regulated. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Massachusetts Protection of Personal Information: Name and SSN
- Massachusetts Protection of Personal Information: Name and SSN (Wide)
- Massachusetts Protection of Personal Information: Name and DL
- Massachusetts Protection of Personal Information: Name and DL (Wide)

- Massachusetts Protection of Personal Information: Name and CCN
- Massachusetts Protection of Personal Information: Name and CCN (Wide)
- Massachusetts Protection of Personal Information: Name and ID
- Massachusetts Protection of Personal Information: Name and Password (Wide)
- Massachusetts Protection of Personal Information: Name and Password (Default)
- Massachusetts Protection of Personal Information: Name and Password (Narrow)
- Massachusetts Protection of Personal Information: Name with Account and Password
- Massachusetts Protection of Personal Information: Account and Password
- Massachusetts Protection of Personal Information: Password Dissemination for HTTP Traffic (Wide)
- Massachusetts Protection of Personal Information: Password Dissemination for HTTP Traffic (Default)
- Massachusetts Protection of Personal Information: Password Dissemination for HTTP Traffic (Narrow)

Michigan Identity Theft Protection Act

Michigan HB 4658 of 2007 requires, unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, one ore more residents of this state, a person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach, shall provide a notice of the security breach to each resident of this state. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Michigan Identity Theft Protection Act: SSN
- Michigan Identity Theft Protection Act: SSN with CCN
- Michigan Identity Theft Protection Act: SSN with Michigan DL
- Michigan Identity Theft Protection Act: SSN with Account Number
- Michigan Identity Theft Protection Act: SSN with PIN Number
- Michigan Identity Theft Protection Act: SSN and Password (Wide)
- Michigan Identity Theft Protection Act: SSN and Password (Default)
- Michigan Identity Theft Protection Act: SSN and Password (Narrow)
- Michigan Identity Theft Protection Act: SSN with DNA profile

Minnesota Data Breach Notification

Minnesota HF 2121 of 2006 requires that any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the

most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in paragraph (c), or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Minnesota Data Breach Notification: Name with CCN
- Minnesota Data Breach Notification: Name with Minnesota driver license
- Minnesota Data Breach Notification: Name with SSN
- Minnesota Data Breach Notification: SSN with CCN
- Minnesota Data Breach Notification: SSN with DNA profile
- Minnesota Data Breach Notification: SSN with MN driver license

Mississippi Data Breach Notification

Mississippi HB 583 of 2010 requires that consumers are notified promptly if the security of their information has been compromised, and gives the public the right to freeze their credit files if they become a victim of identity theft. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Mississippi Data Breach Notification: Account and Password
- Mississippi Data Breach Notification: Name and CCN
- Mississippi Data Breach Notification: Name and Password (Wide)
- Mississippi Data Breach Notification: Name and Password (Default)
- Mississippi Data Breach Notification: Name and Password (Narrow)
- Mississippi Data Breach Notification: Name and SSN
- Mississippi Data Breach Notification: Password Dissemination for HTTP Traffic (Wide)
- Mississippi Data Breach Notification: Password Dissemination for HTTP Traffic (Default)
- Mississippi Data Breach Notification: Password Dissemination for HTTP Traffic (Narrow)

Missouri Breach Notification Law

Missouri HB 62 of 2009 requires that any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri shall provide notice to the affected consumer that there has been a breach of security, following discovery or notification of the breach. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Missouri Breach Notification Law: Name and SSN
- Missouri Breach Notification Law: Name and DL

- Missouri Breach Notification Law: Name and CCN
- Missouri Breach Notification Law: Name and Password (Wide)
- Missouri Breach Notification Law: Name and Password (Default)
- Missouri Breach Notification Law: Name and Password (Narrow)
- Missouri Breach Notification Law: Password Dissemination for HTTP Traffic (Wide)
- Missouri Breach Notification Law: Password Dissemination for HTTP Traffic (Default)
- Missouri Breach Notification Law: Password Dissemination for HTTP Traffic (Narrow)
- Missouri Breach Notification Law: Account and Password
- Missouri Breach Notification Law: ICD10 Descriptions and US full names
- Missouri Breach Notification Law: Name and Sensitive Disease or drug

Montana Data Breach Notification Statute

Montana HB 732 of 2005 requires that any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system, following discovery or notification of the breach, to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Montana Data Breach Notification Statute: Name and SSN
- Montana Data Breach Notification Statute: Name and DL
- Montana Data Breach Notification Statute: Name and CCN
- Montana Data Breach Notification Statute: Name and Password (Wide)
- Montana Data Breach Notification Statute: Name and Password (Default)
- Montana Data Breach Notification Statute: Name and Password (Narrow)
- Montana Data Breach Notification Statute: Password Dissemination for HTTP Traffic (Wide)
- Montana Data Breach Notification Statute: Password Dissemination for HTTP Traffic (Default)
- Montana Data Breach Notification Statute: Password Dissemination for HTTP Traffic (Narrow)
- Montana Data Breach Notification Statute: Account and Password

Nebraska Notification of Data Security Breach Act

Nebraska LB 876, which was signed into law on April 13, 2006, requires that an individual or a commercial entity that conducts business in Nebraska and that owns or licenses computerized data that includes personal information about a resident of Nebraska shall, when it becomes aware of a breach of the security of the system,

conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose. If the investigation determines that the use of information about a Nebraska resident for an unauthorized purpose has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident. Notice shall be made as soon as possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Nebraska Notification of Data Security Breach Act: Account and Password
- Nebraska Notification of Data Security Breach Act: Name and CCN
- Nebraska Notification of Data Security Breach Act: Name and Password (Wide)
- Nebraska Notification of Data Security Breach Act: Name and Password (Default)
- Nebraska Notification of Data Security Breach Act: Name and Password (Narrow)
- Nebraska Notification of Data Security Breach Act: Name and SSN
- Nebraska Notification of Data Security Breach Act: Password Dissemination for HTTP Traffic (Wide)
- Nebraska Notification of Data Security Breach Act: Password Dissemination for HTTP Traffic (Default)
- Nebraska Notification of Data Security Breach Act: Password Dissemination for HTTP Traffic (Narrow)

Nevada Security of Personal Information

Nevada SB SB 347 of 2006 requires that data collectors that maintain records that contain personal information of a resident of this state shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Nevada Security of Personal Information: Name and SSN
- Nevada Security of Personal Information: Name and SSN (Wide)
- Nevada Security of Personal Information: Name and DL
- Nevada Security of Personal Information: Name and DL (Wide)
- Nevada Security of Personal Information: Name and CCN
- Nevada Security of Personal Information: Name and CCN (Wide)
- Nevada Security of Personal Information: Name and ID
- Nevada Security of Personal Information: Name and Password (Wide)
- Nevada Security of Personal Information: Name and Password (Default)

- Nevada Security of Personal Information: Name and Password (Narrow)
- Nevada Security of Personal Information: Name with Account and Password
- Nevada Security of Personal Information: Account and Password
- Nevada Security of Personal Information: Password Dissemination for HTTP Traffic (Wide)
- Nevada Security of Personal Information: Password Dissemination for HTTP Traffic (Default)
- Nevada Security of Personal Information: Password Dissemination for HTTP Traffic (Narrow)

New Hampshire Notice of Security Breach

New Hampshire HB 1660 of 2007 requires businesses who own or license computerized data that includes personal information shall, when they become aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, businesses shall notify the affected individuals as soon as possible. Personal information is considered the customer's full name in combination with any of the following: social security number, driver's license number, or financial account information. The policy detects a combination of full names with social security, driver's license, or credit card numbers. Additional rules detect passwords and account numbers. The rules for this policy are:

- New Hampshire Notice of Security Breach: Name and SSN
- New Hampshire Notice of Security Breach: Name and DL
- New Hampshire Notice of Security Breach: Name and CCN
- New Hampshire Notice of Security Breach: Name and Password (Wide)
- New Hampshire Notice of Security Breach: Name and Password (Default)
- New Hampshire Notice of Security Breach: Name and Password (Narrow)
- New Hampshire Notice of Security Breach: Password Dissemination for HTTP Traffic (Wide)
- New Hampshire Notice of Security Breach: Password Dissemination for HTTP Traffic (Default)
- New Hampshire Notice of Security Breach: Password Dissemination for HTTP Traffic (Narrow)
- New Hampshire Notice of Security Breach: Account and Password

New Jersey Personal Information and Privacy Protection Act

New Jersey A 4001 requires that any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities. The policy

detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- New Jersey Personal Information and Privacy Protection Act: SSN with CCN
- New Jersey Personal Information and Privacy Protection Act: CCN with NJ Driver License
- New Jersey Personal Information and Privacy Protection Act: Password Dissemination for HTTP Traffic (Wide)
- New Jersey Personal Information and Privacy Protection Act: Password Dissemination for HTTP Traffic (Default)
- New Jersey Personal Information and Privacy Protection Act: Password Dissemination for HTTP Traffic (Narrow)
- New Jersey Personal Information and Privacy Protection Act: Password Dissemination for non-HTTP/S Traffic (Wide)
- New Jersey Personal Information and Privacy Protection Act: Password Dissemination for non-HTTP/S Traffic (Default)
- New Jersey Personal Information and Privacy Protection Act: Password Dissemination for non-HTTP/S Traffic (Narrow)

New Mexico Data Breach Notification Act

New Mexico HB 15 of 2017 requires that any person that is licensed to maintain or possess computerized data containing personal identifying information of a New Mexico resident that the person does not own or license shall notify the owner or licensee of the information of any security breach in the most expedient time possible. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- New Mexico Data Breach Notification Act: Account and Password
- New Mexico Data Breach Notification Act: DNA profile
- New Mexico Data Breach Notification Act: Name and CCN
- New Mexico Data Breach Notification Act: Name and Password (Wide)
- New Mexico Data Breach Notification Act: Name and Password (Default)
- New Mexico Data Breach Notification Act: Name and Password (Narrow)
- New Mexico Data Breach Notification Act: Name and SSN
- New Mexico Data Breach Notification Act: Password Dissemination for HTTP Traffic (Wide)
- New Mexico Data Breach Notification Act: Password Dissemination for HTTP Traffic (Default)
- New Mexico Data Breach Notification Act: Password Dissemination for HTTP Traffic (Narrow)

New York Data Security Act

New York A 4254 of 2005 provides that in the event of unauthorized access to "private information," defined as personal information in combination with a social

security number, driver's license, or an account or credit card number, the business or state entity is required to notify affected customers and inform appropriate authorities. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- New York Data Security Act: SSN: with NY driver license
- New York Data Security Act: SSN with CCN
- New York Data Security Act: Name with SSN
- New York Data Security Act: Name with New-York driver license
- New York Data Security Act: Name with CCN
- New York Data Security Act: SSN with DNA profile

North Carolina Identity Theft Protection Act

North Carolina SB 1048 of 2005 requires that any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form (whether computerized, paper, or otherwise) shall provide notice to the affected person that there has been a security breach, following discovery or notification of the breach. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- North Carolina Identity Theft Protection Act: Name and SSN
- North Carolina Identity Theft Protection Act: Name and DL
- North Carolina Identity Theft Protection Act: Name and CCN

North Dakota Data Breach Notification

North Dakota Data Breach Notification, amended in 2017 by HB 1088, requires any person that owns or licenses computerized data that includes personal information, to disclose any breach of the security system, following discovery or notification of the breach in the security of the data, to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- North Dakota Data Breach Notification: Account and Password
- North Dakota Data Breach Notification: Name and CCN
- North Dakota Data Breach Notification: Name and Password (Wide)
- North Dakota Data Breach Notification: Name and Password (Default)
- North Dakota Data Breach Notification: Name and Password (Narrow)
- North Dakota Data Breach Notification: Name and SSN
- North Dakota Data Breach Notification: Password Dissemination for HTTP Traffic (Wide)

- North Dakota Data Breach Notification: Password Dissemination for HTTP Traffic (Default)
- North Dakota Data Breach Notification: Password Dissemination for HTTP Traffic (Narrow)

Ohio Data Security Breach Notification Law

Ohio HB 104 of 2005 requires that any person that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system, following its discovery or notification of the breach of the security of the system, to any resident of this state whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes, or is reasonably believed will cause, a material risk of identity theft or other fraud to the resident. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Ohio Data Security Breach Notification Law: Name and SSN
- Ohio Data Security Breach Notification Law: Name and DL
- Ohio Data Security Breach Notification Law: Name and CCN
- Ohio Data Security Breach Notification Law: Name and Password (Wide)
- Ohio Data Security Breach Notification Law: Name and Password (Default)
- Ohio Data Security Breach Notification Law: Name and Password (Narrow)
- Ohio Data Security Breach Notification Law: Password Dissemination for HTTP Traffic (Wide)
- Ohio Data Security Breach Notification Law: Password Dissemination for HTTP Traffic (Default)
- Ohio Data Security Breach Notification Law: Password Dissemination for HTTP Traffic (Narrow)

Oklahoma Security Breach Notification Act

Oklahoma HB 2357 of 2006 requires that if you maintain, as part of a database, a consumer's name and other personal identification numbers (i.e., SSN, driver's license, credit card, or financial information with a personal security code) that such information must be encrypted or redacted so that in the event of a breach, such information cannot be obtained and used by a third party. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Oklahoma Security Breach Notification Act: Name and SSN
- Oklahoma Security Breach Notification Act: Name and DL
- Oklahoma Security Breach Notification Act: Name and CCN
- Oklahoma Security Breach Notification Act: Name and Password (Wide)
- Oklahoma Security Breach Notification Act: Name and Password (Default)
- Oklahoma Security Breach Notification Act: Name and Password (Narrow)

- Oklahoma Security Breach Notification Act: Password Dissemination for HTTP Traffic (Wide)
- Oklahoma Security Breach Notification Act: Password Dissemination for HTTP Traffic (Default)
- Oklahoma Security Breach Notification Act: Password Dissemination for HTTP Traffic (Narrow)
- Oklahoma Security Breach Notification Act: Account and Password

Oregon Consumer Identity Theft Protection Act

Oregon SB 583 of 2007 requires that a person that owns or licenses personal information that the person uses in the course of the person's business, vocation, occupation, or volunteer activities and that was subject to a breach of security shall give notice of the breach of security to a) the consumer to whom the personal information pertains; b) the Attorney General, either in writing or electronically, if the number of consumers to whom the person must send the notice exceeds 250. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. Additional rules detect passwords and account numbers.The rules for this policy are:

- Oregon Consumer Identity Theft Protection Act: Name and SSN
- Oregon Consumer Identity Theft Protection Act: Name and DL
- Oregon Consumer Identity Theft Protection Act: Name and CCN
- Oregon Consumer Identity Theft Protection Act: Name and Password (Wide)
- Oregon Consumer Identity Theft Protection Act: Name and Password (Default)
- Oregon Consumer Identity Theft Protection Act: Name and Password (Narrow)
- Oregon Consumer Identity Theft Protection Act: Password Dissemination for HTTP Traffic (Wide)
- Oregon Consumer Identity Theft Protection Act: Password Dissemination for HTTP Traffic (Default)
- Oregon Consumer Identity Theft Protection Act: Password Dissemination for HTTP Traffic (Narrow)
- Oregon Consumer Identity Theft Protection Act: Account and Password

Pennsylvania Breach of Personal Information Notification Act

Pennsylvania SBG 712 of 2006 requires that an entity that maintains, stores, or manages computerized data that includes personal information shall provide notice of any breach of the security of the system, following discovery of the breach of the security of the system, to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Pennsylvania Breach of Personal Information Act: Name and SSN
- Pennsylvania Breach of Personal Information Act: Name and DL

- Pennsylvania Breach of Personal Information Act: Name and CCN
- Pennsylvania Breach of Personal Information Act: Name and Password (Wide)
- Pennsylvania Breach of Personal Information Act: Name and Password (Default)
- Pennsylvania Breach of Personal Information Act: Name and Password (Narrow)
- Pennsylvania Breach of Personal Information Act: Account and Password
- Pennsylvania Breach of Personal Information Act: Password Dissemination for HTTP Traffic (Wide)
- Pennsylvania Breach of Personal Information Act: Password Dissemination for HTTP Traffic (Default)
- Pennsylvania Breach of Personal Information Act: Password Dissemination for HTTP Traffic (Narrow)

Puerto Rico Data Breach Notification

The Puerto Rico Citizen Information of Data Banks Security Act, originally HB 1184, signed into law in 2005, requires that any entity that is the proprietor or custodian of a data bank for commercial use that includes personal information of citizens who reside in Puerto Rico must notify said citizens of any violation of the system's security when the data bank whose security has been violated contains all or part of the personal information file and the same is not protected by a cryptographic code, but only by a password. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Puerto Rico Data Breach Notification: Account and Password
- Puerto Rico Data Breach Notification: Name and CCN
- Puerto Rico Data Breach Notification: Name and Password (Wide)
- Puerto Rico Data Breach Notification: Name and Password (Default)
- Puerto Rico Data Breach Notification: Name and Password (Narrow)
- Puerto Rico Data Breach Notification: Name and SSN
- Puerto Rico Data Breach Notification: Password Dissemination for HTTP Traffic (Wide)
- Puerto Rico Data Breach Notification: Password Dissemination for HTTP Traffic (Default)
- Puerto Rico Data Breach Notification: Password Dissemination for HTTP Traffic (Narrow)

Rhode Island Identity Theft Protection Act

Rhode Island HB 6191 of 2006 requires that any municipal agency, state agency, or person that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes personal information shall provide notification as set forth in this section of any disclosure of personal information, or any breach of the security of the system, that poses a significant risk of identity theft to any resident of Rhode Island whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person or entity. The policy detects combinations of Personally

Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Rhode Island Identity Theft Protection Act: Name and SSN
- Rhode Island Identity Theft Protection Act: Name and DL
- Rhode Island Identity Theft Protection Act: Name and CCN
- Rhode Island Identity Theft Protection Act: Name and Password (Wide)
- Rhode Island Identity Theft Protection Act: Name and Password (Default)
- Rhode Island Identity Theft Protection Act: Name and Password (Narrow)
- Rhode Island Identity Theft Protection Act: Password Dissemination for HTTP Traffic (Wide)
- Rhode Island Identity Theft Protection Act: Password Dissemination for HTTP Traffic (Default)
- Rhode Island Identity Theft Protection Act: Password Dissemination for HTTP Traffic (Narrow)
- Rhode Island Identity Theft Protection Act: Account and Password

South Carolina Data Breach Notification

South Carolina SB 453 of 2008 requires that a person conducting business in this state, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system, following discovery or notification of the breach in the security of the data, to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur, or use of the information creates a material risk of harm to the resident. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (C), or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- South Carolina Data Breach Notification: Account and Password
- South Carolina Data Breach Notification: Name and CCN
- South Carolina Data Breach Notification: Name and Password (Wide)
- South Carolina Data Breach Notification: Name and Password (Default)
- South Carolina Data Breach Notification: Name and Password (Narrow)
- South Carolina Data Breach Notification: Name and SSN
- South Carolina Data Breach Notification: Password Dissemination for HTTP Traffic (Wide)
- South Carolina Data Breach Notification: Password Dissemination for HTTP Traffic (Default)

- South Carolina Data Breach Notification: Password Dissemination for HTTP Traffic (Narrow)

South Dakota Medical Records Law

Section 44:73:09:03 of the Administrative Rules of South Dakota requires there shall be written policies and procedures to govern the administration and activities of the medical record service. They shall include policies and procedures pertaining to the confidentiality and safeguarding of medical records, the record content, continuity of a resident's medical records during subsequent admissions, requirements for completion of the record, and the entries to be made by various authorized personnel. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- South Dakota Medical Records Law: ICD9 Code and Name
- South Dakota Medical Records Law: ICD9 Description and Name
- South Dakota Medical Records Law: ICD10 Code and Name
- South Dakota Medical Records Law: ICD10 Description and Name
- South Dakota Medical Records Law: Name and Common Medical Condition
- South Dakota Medical Records Law: Name and HICN
- South Dakota Medical Records Law: Name and Sensitive Disease or Drug
- South Dakota Medical Records Law: Name and SSN

Tennessee Data Breach Notification

Tennessee HB 2170 of 2005 requires that any information holder shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of Tennessee whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (d), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Tennessee Data Breach Notification: Name and SSN
- Tennessee Data Breach Notification: Name and DL
- Tennessee Data Breach Notification: Name and CCN
- Tennessee Data Breach Notification: Name and Password (Wide)
- Tennessee Data Breach Notification: (Default)
- Tennessee Data Breach Notification: (Narrow)
- Tennessee Data Breach Notification: Password Dissemination for HTTP Traffic (Wide)
- Tennessee Data Breach Notification: Password Dissemination for HTTP Traffic (Default)

- Tennessee Data Breach Notification: Password Dissemination for HTTP Traffic (Narrow)
- Tennessee Data Breach Notification: Account and Password

Texas Identity Theft Enforcement and Protection Act

Texas SB 122 of 2005 requires businesses to implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure of any sensitive personal information collected or maintained by the business in the regular course of business. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Texas Identity Theft Enforcement and Protection Act: SSN: with Texas driver license
- Texas Identity Theft Enforcement and Protection Act: SSN with CCN
- Texas Identity Theft Enforcement and Protection Act: Name with SSN
- Texas Identity Theft Enforcement and Protection Act: Name with Texas driver license
- Texas Identity Theft Enforcement and Protection Act: Name with CCN
- Texas Identity Theft Enforcement and Protection Act: SSN with DNA profile

Utah Protection of Personal Information Act

Utah SB 69 of 2007 requires that 1) any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business. 2) a person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Utah Protection of Personal Information Act: SSN with CCN
- Utah Protection of Personal Information Act: CCN with Utah Driver License
- Utah Protection of Personal Information Act: SSN and Account number and Password
- Utah Protection of Personal Information Act: Password Dissemination for HTTP Traffic (Wide)
- Utah Protection of Personal Information Act: Password Dissemination for HTTP Traffic (Default)
- Utah Protection of Personal Information Act: Password Dissemination for HTTP Traffic (Narrow
- Utah Protection of Personal Information Act: Password Dissemination for non-HTTP/S Traffic (Wide)

- Utah Protection of Personal Information Act: Password Dissemination for non-HTTP/S Traffic (Default)
- Utah Protection of Personal Information Act: Password Dissemination for non-HTTP/S Traffic (Narrow)

Vermont Security Breach Notice Act

Vermont S 284 of 2007 requires any data collector that owns or licenses computerized personally identifiable information that includes personal information concerning a consumer shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Vermont Security Breach Notice Act: Account and Password
- Vermont Security Breach Notice Act: Name and CCN
- Vermont Security Breach Notice Act: Name and Password (Wide)
- Vermont Security Breach Notice Act: Name and Password (Default)
- Vermont Security Breach Notice Act: Name and Password (Narrow)
- Vermont Security Breach Notice Act: Name and SSN
- Vermont Security Breach Notice Act: Password Dissemination for HTTP Traffic (Wide)
- Vermont Security Breach Notice Act: Password Dissemination for HTTP Traffic (Default)
- Vermont Security Breach Notice Act: Password Dissemination for HTTP Traffic (Narrow)

Virginia Data Breach Notification

Virginia SB 307 of 2008 requires that an individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee with information about any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the personal information was accessed and acquired by an unauthorized person or the individual or entity reasonable believes the personal information was accessed and acquired by an unauthorized person. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Virginia Data Breach Notification: Name and SSN
- Virginia Data Breach Notification: Name and DL
- Virginia Data Breach Notification: Name and CCN

Washington Data Breach Notification

Washington SB 6043 requires any person or entity who conducts business in the state, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information, and who discovers a breach of the

security of the system, shall promptly notify any resident whose personal information was included in the breach. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Washington Data Breach Notification: SSN: with WA driver license
- Washington Data Breach Notification: SSN with CCN
- Washington Data Breach Notification: Name with SSN
- Washington Data Breach Notification: Name with Washington driver license
- Washington Data Breach Notification: Name with CCN
- Washington Data Breach Notification: SSN with DNA profile

West Virginia Consumer Credit and Protection Act

West Virginia SB 340 of 2008 requires that an individual or entity that owns or licenses computerized data that includes personal information shall give notice of any breach of the security of the system, following discovery or notification of the breach of the security of the system, to any resident of this state whose unencrypted and unredacted personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any resident of this state. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- West Virginia Consumer Credit and Protection Act: Account and Password
- West Virginia Consumer Credit and Protection Act: Name and CCN
- West Virginia Consumer Credit and Protection Act: Name and Password (Wide)
- West Virginia Consumer Credit and Protection Act: Name and Password (Default)
- West Virginia Consumer Credit and Protection Act: Name and Password (Narrow)
- West Virginia Consumer Credit and Protection Act: Name and SSN
- West Virginia Consumer Credit and Protection Act: Password Dissemination for HTTP Traffic (Wide)
- West Virginia Consumer Credit and Protection Act: Password Dissemination for HTTP Traffic (Default)
- West Virginia Consumer Credit and Protection Act: Password Dissemination for HTTP Traffic (Narrow)

Wisconsin Data Breach Notification

Wisconsin SB 164, signed into law in 2006 as Wisconsin Notice of Unauthorized Acquisition of Personal Information, states that if an entity whose principal place of business is located in this state or an entity that maintains or licenses personal information in this state knows that personal information in the entity's possession has been acquired by a person whom the entity knows has not been authorized to acquire

the personal information, the entity shall make reasonable efforts to notify each subject of the personal information. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Wisconsin Data Breach Notification: SSN with CCN
- Wisconsin Data Breach Notification: SSN with Wisconsin DL
- Wisconsin Data Breach Notification: SSN with Account Number
- Wisconsin Data Breach Notification: SSN with PIN Number
- Wisconsin Data Breach Notification: SSN and Password (Wide)
- Wisconsin Data Breach Notification: SSN and Password (Default)
- Wisconsin Data Breach Notification: SSN and Password (Narrow)
- Wisconsin Data Breach Notification: SSN with DNA profile

Wyoming Data Breach Notification

Wyoming Computer Security Breach related act, amended by SF 35 and 36 in 2015, requires that any person or business that conducts business in Wyoming and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system, following discovery or notification of the breach, to any resident of Wyoming whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver's license numbers. The rules for this policy are:

- Wyoming Data Breach Notification: Account and Password
- Wyoming Data Breach Notification: Name and CCN
- Wyoming Data Breach Notification: Name and Password (Wide)
- Wyoming Data Breach Notification: Name and Password (Default)
- Wyoming Data Breach Notification: Name and Password (Narrow)
- Wyoming Data Breach Notification: Name and SSN
- Wyoming Data Breach Notification: Password Dissemination for HTTP Traffic (Wide)
- Wyoming Data Breach Notification: Password Dissemination for HTTP Traffic (Default)
- Wyoming Data Breach Notification: Password Dissemination for HTTP Traffic (Narrow)

US and Canada Federal Regulations

The following regulations apply to both the United States and Canada:

- *Check 21 Act*
- *Children's Online Privacy Act (COPPA)*, page 94

- *Controlled Unclassified Information (CUI)*
- *DIACAP*
- *Export Administration Regulations (EAR)*
- *FCRA*
- *FDA - 21 CFR*
- *FERC and NERC*
- *FERPA*
- *FFIEC*
- *FISMA*
- *GLBA*
- *HIPAA*
- *ITAR*
- *MITS*
- *Risk Management Framework (RMF) for DoD Information Technology (IT)*
- *Sarbanes-Oxley Act (SOX)*

Check 21 Act

The Check Clearing for the 21st Century Act (Check 21) is a Federal law designed to foster innovation in the payments system and to enhance its efficiency by reducing some of the legal impediments to check truncation. The policy detects TIFF files, widely used for scanned checks. The rule for this policy is:

- Check 21: TIFF Format

Children's Online Privacy Act (COPPA)

The Children's Online Privacy Protection Act of 1998 (COPPA) is a United States federal law applied to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. The policy detects combinations of personal information with age information that indicates that the person's age is less than 13, based on explicit age or date of birth. The rules for this policy are:

- COPPA: PII of Children (Wide)
- COPPA: PII of Children (Default)

Controlled Unclassified Information (CUI)

Policy for detecting files that contain controlled unclassified information, based on CUI markings. Some US regulations, for example, the Department of Defense's "Defense Federal Acquisition Regulation Supplement" (DFARS) to the American Federal Acquisition Regulation (FAR), require contractors and subcontractors to safeguard covered information, marked by Controlled Unclassified Information (CUI). The rules for this policy are:

- Controlled Unclassified Information: Banner Marking (Wide)

- Controlled Unclassified Information: Banner Marking (Default)
- Controlled Unclassified Information: Banner Marking (Narrow)
- Controlled Unclassified Information: Portion Marking (Wide)
- Controlled Unclassified Information: Portion Marking (Default)
- Controlled Unclassified Information: Portion Marking (Narrow)

DIACAP

The DoD Information Assurance Certification and Accreditation Process (DIACAP) is the US Department of Defense process to ensure the management of risks on Information Systems (IS). The policy is applied to information systems of DoD-related units and contractors. The DLP aspect of the policy applies to combinations of Personally Identifiable Information (like social security number or credit card number) with sensitive private information, such as health conditions, names of crimes, and ethnicities, to promote compliance with DoD Privacy Program (DoD 5400.11-R) and Privacy of Health Information in DoD Health Care (DoD 6025.18). Additional rules detect confidential information about the corporate network, and confidential documents, according to DoD 8520.1 - Protection of Sensitive Compartmented Information (SCI). This regulation was deprecated in 2014 and replaced by "Risk Management Framework for DoD Information Technology". The transition to the new regulation must be done before the end of 2016. The rules for this policy are:

- DIACAP: DoD 5400.11-R - Name and Crime
- DIACAP: DoD 5400.11-R - Name and Ethnicity
- DIACAP: DoD 5400.11-R - Name and SSN
- DIACAP: DoD 5400.11-R - SSN and Crime
- DIACAP: DoD 5400.11-R - SSN and Ethnicity
- DIACAP: DoD 6025.18 - CCN and Sensitive Disease or drug
- DIACAP: DoD 6025.18 - Name and Common Medical Condition (Default)
- DIACAP: DoD 6025.18 - Name and Common Medical Condition (Narrow)
- DIACAP: DoD 6025.18 - Name and Sensitive Disease (Default)
- DIACAP: DoD 6025.18 - Name and Sensitive Disease (Narrow)
- DIACAP: DoD 6025.18 - SSN and Sensitive Disease or Drug
- DIACAP: DoD 8520.1 - Confidential Document
- DIACAP: DoD 8520.1 - Proprietary in Header or Footer
- DIACAP: DoD 8520.1 - Password Dissemination for HTTP Traffic (Wide)
- DIACAP: DoD 8520.1 - Password Dissemination for HTTP Traffic (Default)
- DIACAP: DoD 8520.1 - Password Dissemination for HTTP Traffic (Narrow)
- DIACAP: DoD 8520.1 - Password Dissemination for non-HTTP/S Traffic (Wide)
- DIACAP: DoD 8520.1 - Password Dissemination for non-HTTP/S Traffic (Default)
- DIACAP: DoD 8520.1 - Password Dissemination for non-HTTP/S Traffic (Narrow)

- DIACAP: Network Information and Security (Pattern and IP)
- DIACAP: Network Information and Security (Textual Pattern)

Export Administration Regulations (EAR)

The Export Administration Regulations (EAR) are issued by the United States Department of Commerce, and control also the usage of "dual purpose" items (i.e., commercial products that can also be used for military purposes.) The definition of "Export" includes disclosing or transferring technical data to a foreign person whether in the U.S. or abroad. The policy comprises rules for detection of probable EAR-regulated information, such as chemical formulas, information pertaining encryption technology and confidential documents. The rules for this policy are:

- EAR: CAD Files: Abaqus ODB File
-
- EAR: CAD Files: Autodesk Design Web File
- EAR: CAD Files: Autodesk Maya Binary File
- EAR: CAD Files: Autodesk Maya Textual File
- EAR: CAD Files: Catia File
- EAR: CAD Files: Corel Draw File
- EAR: CAD Files: DWG File
- EAR: CAD Files: DXF Binary File
- EAR: CAD Files: DXF Textual File
- EAR: CAD Files: IGS Textual File
- EAR: CAD Files: JT File
- EAR: CAD Files: Nastran OP2 File
- EAR: CAD Files: PTC Creo ASM File
- EAR: CAD Files: PTC Creo DRW File
- EAR: CAD Files: PTC Creo FRM File
- EAR: CAD Files: PTC Creo PRT File
- EAR: CAD Files: Siemens NX PRT File
- EAR: CAD Files: SolidWorks File
- EAR: CAD Files: STL Binary File
- EAR: CAD Files: STL Textual File
- EAR: CAD Files: STP File
- EAR: CAD Files: WHIP File
- EAR: CAD Files: X_T Textual File
- EAR: Chemicals and Materials (Default)
- EAR: Chemicals and Materials (Narrow)
- EAR: Chemicals and Materials (Wide)
- EAR: Confidential Document

- EAR: Encryption Technologies (Default)
- EAR: Encryption Technologies (Narrow)
- EAR: Encryption Technologies (Wide)
- EAR: Laser and Microelectronics (Default)
- EAR: Laser and Microelectronics (Narrow)
- EAR: Laser and Microelectronics (Wide)
- EAR: Microorganisms and Toxins (Default)
- EAR: Microorganisms and Toxins (Narrow)
- EAR: Microorganisms and Toxins (Wide)
- EAR: Microsoft Visio File
- EAR: Military Technologies (Default)
- EAR: Military Technologies (Narrow)
- EAR: Military Technologies (Wide)
- EAR: Nuclear Technologies (Default)
- EAR: Nuclear Technologies (Narrow)
- EAR: Nuclear Technologies (Wide)
- EAR: Proprietary in Document
- EAR: Python (Default)
- EAR: Python (Wide)
- EAR: Space Technologies (Default)
- EAR: Space Technologies (Narrow)
- EAR: Space Technologies (Wide)
- EAR: C Family or Java (Default)
- EAR: C Family or Java (Wide)

FCRA

The Fair Credit Reporting Act (“FCRA”) is a United States federal law. The Act is designed to help ensure that consumer reporting agencies act fairly, impartially, and with respect for the consumer's right to privacy when preparing consumer reports on individuals. The policy comprises rules for detection of personal financial information. The rules for this policy are:

- FCRA: SSN and Personal Finance Terms
- FCRA: DL and Personal Finance Terms
- FCRA: SSN and Account
- FCRA: DL and Account
- FCRA: CCN: All Credit Cards
- FCRA: Credit Card Magnetic Strips
- FCRA: Name and Personal Finance Terms

FDA - 21 CFR

Title 21 Part 11 of the Code of Federal Regulations (CFR) deals with the FDA guidelines on electronic records and electronic signatures in the United States. Part 11 requires drug makers, medical device manufacturers, biotech companies, biologics developers, and other FDA-regulated industries, with some specific exceptions, to implement controls, including audits, system validations, audit trails, electronic signatures, and documentation for software and systems involved in processing electronic data that are (a) required to be maintained by the FDA predicate rules or (b) used to demonstrate compliance to a predicate rule. The rules for this policy are:

- FDA 21 CFR: Clinical Trials
- FDA 21 CFR: Controlled Drugs
- FDA 21 CFR: DICOM
- FDA 21 CFR: DNA Sequence
- FDA 21 CFR: Name and Common Medical Condition (Default)
- FDA 21 CFR: Name and Common Medical Condition (Narrow)
- FDA 21 CFR: Password Dissemination for HTTP Traffic (Wide)
- FDA 21 CFR: Password Dissemination for HTTP Traffic (Default)
- FDA 21 CFR: Password Dissemination for HTTP Traffic (Narrow)
- FDA 21 CFR: Protein Sequence (Default)
- FDA 21 CFR: Protein Sequence (Narrow)

FERC and NERC

Policy to promote compliance with the requirements imposed by the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Council (NERC) to protects Critical Energy Infrastructure Information (CEII). The policy detects sensitive Energy Infrastructure Information, such as natural gas pipeline flow diagrams, various drawing and schemes files and FERC forms 567 and 715. The rules for this policy are:

- FERC and NERC: CAD Files: DWG File
- FERC and NERC: CAD Files: DXF Binary File
- FERC and NERC: CAD Files: DXF Textual File
- FERC and NERC: CAD Files: IGS Textual File
- FERC and NERC: CAD Files: JT File
- FERC and NERC: CAD Files: PTC Creo ASM File
- FERC and NERC: CAD Files: PTC Creo DRW File
- FERC and NERC: CAD Files: PTC Creo FRM File
- FERC and NERC: CAD Files: PTC Creo PRT File
- FERC and NERC: CAD Files: SolidWorks File
- FERC and NERC: CAD Files: STL Binary File
- FERC and NERC: CAD Files: STL Textual File

- FERC and NERC: CAD Files: STP File
- FERC and NERC: CAD Files: WHIP File
- FERC and NERC: CAD Files: X_T Textual File
- FERC and NERC: Disclaimer
- FERC and NERC: Form 567
- FERC and NERC: Form 715
- FERC and NERC: Microsoft Visio
- FERC and NERC: Pipeline Flow Diagram

FERPA

The Family Educational Rights and Privacy is a US Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. The policy detects combinations of Personally Identifiable Information (PII) like social security number or driver license number, and sensitive private information such as grades, health conditions, and names of crimes and ethnicities. The rules for this policy are:

- FERPA: Driver License and Common Medical Condition
- FERPA: Driver License and Ethnicities
- FERPA: Driver License and Grades
- FERPA: Driver License and Sensitive Disease or drug
- FERPA: Name and Common Medical Condition (Default)
- FERPA: Name and Common Medical Condition (Narrow)
- FERPA: Name and Sensitive Disease or drug (Default)
- FERPA: Name and Sensitive Disease or drug (Narrow)
- FERPA: SSN and Common Medical Condition
- FERPA: SSN and Ethnicities
- FERPA: SSN and Grades
- FERPA: SSN and Sensitive Disease or drug

FFIEC

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the Federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions

The rules for this policy are:

- FFIEC: 5-8 Digit Account Number

- FFIEC: 9 Digit Account Number
- FFIEC: 10 Digit Account Number
- FFIEC: Credit Card Magnetic Strip
- FFIEC: Credit Card Number
- FFIEC: Driver License
- FFIEC: Password Dissemination for HTTP Traffic (Wide)
- FFIEC: Password Dissemination for HTTP Traffic (Default)
- FFIEC: Password Dissemination for HTTP Traffic (Narrow)
- FFIEC: Password Dissemination for non-HTTP/S Traffic (Wide)
- FFIEC: Password Dissemination for non-HTTP/S Traffic (Default)
- FFIEC: Password Dissemination for non-HTTP/S Traffic (Narrow)
- FFIEC: PIN
- FFIEC: Social Security Number
- FFIEC: TIFF File
- FFIEC: Zip Code and Financial Term

FISMA

The Federal Information Security Management Act of 2002 ("FISMA") imposes a mandatory set of processes that must be followed for all information systems used or operated by a US federal agency or by a contractor or other organization on behalf of a US Government agency. The policy detects combinations of Personally Identifiable Information (PII) like social security number or credit card number, with sensitive private information, such as health conditions, names of crimes, and ethnicities. Additional rules detect confidential information about the corporate network, and confidential documents. The rules for this policy are:

- FISMA: CCN and Crime
- FISMA: CCN and Ethnicity
- FISMA: CCN and Sensitive Disease or Drug
- FISMA: Confidential in Document
- FISMA: Proprietary in Document
- FISMA: Network Information and Security (Pattern and IP)
- FISMA: Network Information and Security (Textual Pattern)
- FISMA: Password Dissemination for HTTP Traffic (Wide)
- FISMA: Password Dissemination for HTTP Traffic (Default)
- FISMA: Password Dissemination for HTTP Traffic (Narrow)
- FISMA: Password Dissemination for non-HTTP/S Traffic (Wide)
- FISMA: Password Dissemination for non-HTTP/S Traffic (Default)
- FISMA: Password Dissemination for non-HTTP/S Traffic (Narrow)
- FISMA: SSN and Crime
- FISMA: SSN and Ethnicity

- FISMA: SSN and Sensitive Disease or Drug

GLBA

The Financial Modernization Act of 1999, also known as the “Gramm-Leach-Bliley Act” or GLB Act, is a U.S. Federal regulation that includes provisions to protect consumers' personal financial information held by financial institutions. The policy contains rules to detect accounts, credit cards, and social security numbers. The policy comprises rules for detection of personal financial information and other personal information. The rules for this policy are:

- GLBA: CCN (Default)
- GLBA: CCN (Narrow)
- GLBA: Name and 5-8 Digit Account Numbers
- GLBA: Name and 9-Digit Account Numbers
- GLBA: Name and 10-Digit Account Numbers
- GLBA: Name and Contact Information
- GLBA: Name and Personal Finance Terms
- GLBA: Name and Sensitive Disease or Drug (Default)
- GLBA: Name and Sensitive Disease or Drug (Narrow)
- GLBA: Name and SSN
- GLBA: RTN/ABA (Wide)
- GLBA: RTN/ABA (Default)
- GLBA: RTN/ABA (Narrow)
- GLBA: SSN and Account
- GLBA: SSN and Personal Finance Terms

HIPAA

The Health Insurance Portability and Accountability Act is a US Federal law that specifies a series of administrative, technical, and physical safeguards, organizational and documentation requirements for covered entities to use to assure the availability, confidentiality, and integrity of electronically protected health information. The policy detects combinations of Personally Identifiable Information (PII) like name, social security or credit card number, and protected health information (PHI). The rules for this policy are:

- HIPAA: Credit Card Number and Common Medical Condition
- HIPAA: Credit Card Number and Sensitive Disease or Drug
- HIPAA: DICOM
- HIPAA: DNA Profile (Default)
- HIPAA: DNA Profile (Narrow)
- HIPAA: DOB and Name (Wide)
- HIPAA: DOB and Name (Default)
- HIPAA: ICD9 Code and Description

- HIPAA: ICD9 Code and Name
- HIPAA: ICD9 Description and Name
- HIPAA: ICD10 Code and Description
- HIPAA: ICD10 Code and Name
- HIPAA: ICD10 Description and Name
- HIPAA: Medical Form (Wide)
- HIPAA: Medical Form (Default)
- HIPAA: Medical Form (Narrow)
- HIPAA: Name and Common Medical Condition (Default)
- HIPAA: Name and Common Medical Condition (Narrow)
- HIPAA: Name and Contact Information
- HIPAA: Name and HICN
- HIPAA: Name and Sensitive Disease or Drug (Default)
- HIPAA: Name and Sensitive Disease or Drug (Narrow)
- HIPAA: NDC Number (Wide)
- HIPAA: NDC Number (Default)
- HIPAA: NDC Number (Narrow)
- HIPAA: SPSS Text File
- HIPAA: SSN and Common Medical Condition
- HIPAA: SSN and Sensitive Disease or Drug

ITAR

The ITAR regulation for industry and government regulates dissemination of encryption, space, military and nuclear technology, along with source code. The rules for this policy are:

- ITAR: C family or Java Source Code
- ITAR: Confidential in Header or Footer
- ITAR: Encryption Technologies (Default)
- ITAR: Encryption Technologies (Narrow)
- ITAR: Encryption Technologies (Wide)
- ITAR: Military Technologies (Default)
- ITAR: Military Technologies (Narrow)
- ITAR: Military Technologies (Wide)
- ITAR: Nuclear Technologies (Default)
- ITAR: Nuclear Technologies (Narrow)
- ITAR: Nuclear Technologies (Wide)
- ITAR: Proprietary in Header or Footer
- ITAR: Python (Default)

- ITAR: Python (Wide)
- ITAR: Space Technologies (Default)
- ITAR: Space Technologies (Narrow)
- ITAR: Space Technologies (Wide)
- ITAR: SPICE Source code
- ITAR: Technical Drawing files
- ITAR: Verilog Source code
- ITAR: VHDL Source Code
- ITAR:SPICE Source code (Berkeley version)

MITS

The Management of Information Technology Security (MITS) standard defines baseline security requirements that Canadian federal departments must fulfill to ensure the security of information and information technology (IT) assets under their control. The DLP aspect of the policy applies to combinations of Personally Identifiable Information (like social insurance number or credit card number) with sensitive private information, such as health conditions, to promote compliance with the Canadian Privacy Impact Assessment mandated by MITS. Additional rules detect confidential information about the corporate network, and confidential documents, to promote compliance with the Canadian Government Security Policy. The rules for this policy are:

- MITS: Confidential Document
- MITS: Proprietary in Document
- MITS: Network Information and Security (Pattern and IP)
- MITS: Network Information and Security (Textual Pattern)
- MITS: Password Dissemination for HTTP Traffic (Wide)
- MITS: Password Dissemination for HTTP Traffic (Default)
- MITS: Password Dissemination for HTTP Traffic (Narrow)
- MITS: Password Dissemination for non-HTTP/S Traffic (Wide)
- MITS: Password Dissemination for non-HTTP/S Traffic (Default)
- MITS: Password Dissemination for non-HTTP/S Traffic (Narrow)
- MITS: SIN and CCN
- MITS: SIN and Common Medical Condition
- MITS: SIN and Sensitive Disease or Drug
- MITS: Social Insurance Number

Risk Management Framework (RMF) for DoD Information Technology (IT)

The Risk Management Framework is a United States federal government policy and standards to help secure information systems developed by National Institute of Standards and Technology (NIST). The two main publications that cover the details of RMF are NIST Special Publication 800-37, "Guide for Applying the Risk

Management Framework to Federal Information Systems", and NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations". DoD instruction 8510.01 defines the Risk Management Framework for DoD Information Technology. The rules for this policy are:

- RMF for DoD IT: CCN and Sensitive Disease or Drug
- RMF for DoD IT: Confidential Document
- RMF for DoD IT: Name and Common Medical Condition (Default)
- RMF for DoD IT: Name and Common Medical Condition (Narrow)
- RMF for DoD IT: Name and Crime
- RMF for DoD IT: Name and Ethnicity
- RMF for DoD IT: Name and Sensitive Disease (Default)
- RMF for DoD IT: Name and Sensitive Disease (Narrow)
- RMF for DoD IT: Name and SSN
- RMF for DoD IT: Network Information and Security (Pattern and IP)
- RMF for DoD IT: Network Information and Security (Textual Pattern)
- RMF for DoD IT: Password Dissemination for HTTP Traffic (Wide)
- RMF for DoD IT: Password Dissemination for HTTP Traffic (Default)
- RMF for DoD IT: Password Dissemination for HTTP Traffic (Narrow)
- RMF for DoD IT: Password Dissemination for non-HTTP/S Traffic (Wide)
- RMF for DoD IT: Password Dissemination for non-HTTP/S Traffic (Default)
- RMF for DoD IT: Password Dissemination for non-HTTP/S Traffic (Narrow)
- RMF for DoD IT: Proprietary in Header or Footer
- RMF for DoD IT: SSN and Crime
- RMF for DoD IT: SSN and Ethnicity
- RMF for DoD IT: SSN and Sensitive Disease or Drug

Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act (SOX) mandates public companies to comply with its requirements. This act provides strict guidelines for ensuring corporate governance and control policies for information within publicly traded companies. The Forcepoint SOX-related policy promotes compliance with the data protection aspects of SOX by detecting audit terms and SEC 10-K and 10-Q reports. The rules for this policy are:

- SOX: Form 10-K (Non-Standard Fiscal Year)
- SOX: Form 10-K (Standard Fiscal Year)
- SOX: Form 10-Q (Non-Standard Fiscal Year)
- SOX: Form 10-Q (Standard Fiscal Year)
- SOX: SOX-Related Term

Data Theft Risk Indicators

Forcepoint DLP includes the following types of Data Theft Risk Indicator policies:

- *Employee Discontent*, page 109
- *Indicators of Compromise*, page 107
- *Suspicious User Activity*, page 105

Suspicious User Activity

- Data Sent During Unusual Hours

  Detects data that is sent at an unusual time. You define what is considered an unusual time in the script classifier, Unusual Hours. Each rule in this policy target a different type of data, such as Office or archive files.

  Example: If you define working days in the classifier as Monday-Friday and unusual hours as 9pm-5am, then data sent on Saturday, Sunday, or during the working week between 9 p.m. and 5 a.m. triggers this policy.

  - Source Code C family or Java Sent During Unusual Hours
  - Confidential in Header/Footer Sent During Unusual Hours
  - Office Files Sent Over Time During Unusual Hours
  - Archive Files Sent Over Time During Unusual Hours
  - Python Source Code Sent During Unusual Hours
- Deep Web URLs

  Policy for detecting deep web URLs that appear in analyzed content such as textual documents or email messages and end with the pseudo-top-level domains .onion and .i2p. The deep web is a portion of World Wide Web content that is not indexed by standard search engines and that is intentionally hidden from the regular Internet, accessible only with special software, such as Tor. Such URLs are used for anonymous defamation, unauthorized leaks of sensitive information and copyright infringement, distribution of illegal sexual content, selling controlled substances, money laundering, bank fraud, credit card fraud and identity theft, among other things. The rules for this policy are:

  - Deep Web URLs: .i2p (Wide)
  - Deep Web URLs: .i2p (Default)
  - Deep Web URLs: .onion
- Email to Competitors

  A policy for detecting email messages that are being sent from one's corporate email address to his or her personal email address. The rules for this policy are:

  - Email to Competitors
  - Contact Information to Competitors
  - Encrypted Attachment to Competitors

- Malicious Concealment

  Policy for detection of content suspected to be manipulated to avoid detection.This may cause false positives. The rules for this policy are:

  - Manipulated Content - L33T
  - Manipulated Content - Reversed Text
  - Manipulated Content - ROT13
  - Manipulated Content - Upside Down Text
  - Manipulated Content (Default)
  - Manipulated Content (Narrow)
  - Manipulated Content (Wide)
- Password Dissemination

  Detects content suspected to be a password in clear text. The rules for this policy are:

  - Password Dissemination: Email Address and Password (Wide)
  - Password Dissemination: Email Address and Password (Default)
  - Password Dissemination for HTTP Traffic (Wide)
  - Password Dissemination for HTTP Traffic (Default)
  - Password Dissemination for HTTP Traffic (Narrow)
  - Password Dissemination for non-HTTP/S Traffic (Wide)
  - Password Dissemination for non-HTTP/S Traffic (Default)
  - Password Dissemination for non-HTTP/S Traffic (Narrow)
- Problem Gambling

  Detects expressions that are indicative of problem gambling; for example, “I am addicted to gambling”, “My gambling is out of control”. The rule for this policy is:

  - Problem Gambling
- Suspected Mail to Self

  Policy for detecting email messages that are being sent from one’s corporate email address to his or her personal email address. The rules for this policy are:

  - Self CV/Resume Distribution: English (Wide)
  - Self CV/Resume Distribution: English (Default)
  - Archive Files Sent Over Time in Suspected Mail to Self
  - Confidential in Header/Footer in Suspected Mail to Self
  - Database Files in Suspected Mail to Self
  - Encrypted Files of Known Format in Suspected Mail to Self
  - Encrypted Files of Unknown Format in Suspected Mail to Self
  - Office Files Sent Over Time in Suspected Mail to Self
  - C Family or Java Source Code in Suspected Mail to Self
  - Python Source Code in Suspected Mail to Self
  - Suspected Mail to Self

- Unknown File Formats Over Time

  Detects when unencrypted binary files of unknown formats are being sent repeatedly over a period of time. For example, if 50 unencrypted files of an unknown format are sent during 1 hour, this policy is triggered. The rules for this policy are:

  - Unknown file formats over time (Wide)
  - Unknown file formats over time (Default)
  - Unknown file formats over time (Narrow)
  - Unknown file formats over time to uncategorized sites
- User Traffic Over Time

  Policy for detection of suspicious behavior of users by measuring the rate and type of transactions over time. This may cause false positives. The rules for this policy are:

  - User Traffic Over Time: CV and Resume
  - User Traffic Over Time: Source Code
  - User Traffic Over Time: Specific Attachment

Indicators of Compromise

- .REG Files

  Policy for detecting .REG files (Windows Registry files). The rule for this policy is:

  - .REG File
- Database Dumps/Backup Files

  Policy for detecting records of SQL table data extracted from a database. The rules for this policy are:

  - Database Dumps/Backup Files: MySQL-Format Database Dump (Wide)
  - Database Dumps/Backup Files: MySQL-Format Database Dump (Default)
  - Database Dumps/Backup Files: Microsoft Tape Format
- Encrypted Files

  Policy for detection of encrypted PGP files, password-protected files of known formats, like Microsoft Word and ZIP, and unknown encrypted files. The rules for this policy are:

  - Encrypted Files: B1 File
  - Encrypted Files: RAR File
  - Encrypted Files: RAR5 File
  - Encrypted Files: ZIP File
  - Encrypted Files: Microsoft Access Database File (Legacy)
  - Encrypted Files: Microsoft Excel Binary File (Legacy)
  - Encrypted Files: Microsoft Office Encrypted File (OOXML)

- Encrypted Files: Microsoft OneNote Encrypted File
- Encrypted Files: Microsoft PowerPoint Binary File (Legacy)
- Encrypted Files: Microsoft Word Binary File (Legacy)
- Encrypted Files: PDF File
- Encrypted Files: PGP Encrypted File
- Encrypted Files: PGP Signed and Encrypted File
- Encrypted Files: Unknown Encrypted Format

- Password Files

  Searches for outbound password files, such as SAM database and UNIX/Linux password files. The rules for this policy are:

  - Password Files: .htpasswd File (Wide)
  - Password Files: .htpasswd File (Default)
  - Password Files: .htpasswd File (Narrow)
  - Password Files: General File
  - Password Files: Password File (Wide)
  - Password Files: Password File (Default)
  - Password Files: SAM File (Wide)
  - Password Files: SAM File (Default)
  - Password Files: SAM File (Narrow)
  - Password Files: Shadow File (Wide)
  - Password Files: Shadow File (Default)

- Private Keys

  Policy for detecting private keys or file formats that contain them. The rule for this policy is:

  - Private Keys: DSA Private Key
  - Private Keys: Elliptic Curve Private Key
  - Private Keys: JSON Keystore File Private Key
  - Private Keys: OpenSSH Private Key
  - Private Keys: PGP Private Key
  - Private Keys: PKCS #1 Private Key
  - Private Keys: Encrypted PKCS #8 Private Key
  - Private Keys: Unencrypted PKCS #8 Private Key
  - Private Keys: PKCS #12 File
  - Private Keys: SSH2 Private Key
  - Private Keys: Textual PPK Private Key

- Suspected Malware Communication

  Identifies traffic that is thought to be malware “phoning home” or attempting to steal information. Detection is based on the analysis of traffic patterns from

known infected machines. Applies only when Forcepoint Web Security is installed. Rules in this policy include:

- Suspected Malware Communication (Wide)
- Suspected Malware Communication (Default)

- Suspected Malicious Dissemination

  Policy for the detection of a suspected malicious content dissemination such as: encrypted or manipulated information, passwords files, credit card tracks, suspected applications and dubious content such as information about the network, software license keys, and database files. The rules for this policy are:

  - Suspected Malicious Dissemination: Encrypted File (Known Format)
  - Suspected Malicious Dissemination: Email Address and Password (Wide)
  - Suspected Malicious Dissemination: Email Address and Password (Default)
  - Suspected Malicious Dissemination: Generic Encryption Detection (Wide)
  - Suspected Malicious Dissemination: Generic Encryption Detection (Default)
  - Suspected Malicious Dissemination: IT Asset Information
  - Suspected Malicious Dissemination: Malicious Concealment
  - Suspected Malicious Dissemination: Password Dissemination for non-HTTP/S Traffic (Wide)
  - Suspected Malicious Dissemination: Password Dissemination for non-HTTP/S Traffic (Default)
  - Suspected Malicious Dissemination: Password Dissemination for non-HTTP/S Traffic (Narrow)
  - Suspected Malicious Dissemination: Password Dissemination for HTTP Traffic (Wide)
  - Suspected Malicious Dissemination: Password Dissemination for HTTP Traffic (Default)
  - Suspected Malicious Dissemination: Password Dissemination for HTTP Traffic (Narrow)
  - Counter Malicious: Password File
  - Suspected Malicious Dissemination: Suspected Application (Steganography and Encryption)

Employee Discontent

Predefined Policies and Classifiers | Forcepoint DLP | v8.6.x

- CV and Resume in English

  Policy for detection of documents comprising resumes and CVs in English.

  The rule for this policy is:

  - CV and Resume in English

- CV and Resume in French

  Policy for detection of resumes and CVs in French.

The rules for this policy are:

- CV and Resume in French (Wide)
- CV and Resume in French (Default)
- CV and Resume in French (Narrow)

- CV and Resume in German

  Policy for detection of resumes and CVs in German.

  The rules for this policy are:

  - CV and Resume in German (Wide)
  - CV and Resume in German (Default)
  - CV and Resume in German (Narrow)

- CV and Resume in Spanish

  Policy for detection of resumes and CVs in Spanish.

  The rules for this policy are:

  - CV and Resume in Spanish (Wide)
  - CV and Resume in Spanish (Default)
  - CV and Resume in Spanish (Narrow)

- Disgruntled Employee

  Detects expressions that are indicative of disgruntled employees. For example: “I hate my boss”, “I hate my job”.

  - Disgruntled Employee (Default)
  - Disgruntled Employee (Narrow)

- Israel CV and Resume

  Policy for detection of documents comprising resumes and CVs in Hebrew and English. The rules for this policy are:

  - Israel CV and Resume: English
  - Israel CV and Resume: Hebrew

- Russia CV and Resume

  Policy for detection of documents comprising resumes and CVs in Russian, Ukrainian, and English. The rules for this policy are:

  - Russia CV and Resume: English
  - Russia CV and Resume: Russian or Ukrainian

- Self CV/Resume Distribution

  Policy for detecting employees who distribute their resume or Curriculum Vitae, indicating they may be searching for a new job. The rules for this policy include:

  - Self CV Distribution: English (Wide)
  - Self CV Distribution: English (Default)

- Ukraine CV and Resume

  Policy for detection of documents comprising resumes and CVs in Ukrainian, Russian, and English. The rules for this policy are:

- Ukraine CV and Resume: English
- Ukraine CV and Resume: Russian or Ukrainian

Quick Policies

Forcepoint DLP includes the following types of quick policies:

- *Web DLP policy*, page 111
- *Email DLP policy*, page 112
- *Mobile DLP policy*, page 113

Web DLP policy

The Web DLP "quick policy" includes the PCI policy, PHI policies, and PII policies listed in this document (including financial policies). In addition, the Web DLP policy includes several policies for the data theft attribute:

- Common password information

  Searches for outbound passwords in plain text. The rules for this policy are:

  - Common password information
  - Common password information (Wide)
  - Common password information (Narrow)
- Encrypted files - known format

  Searches for outbound transactions comprising common encrypted file formats. The rules for this policy are:

  - Encrypted files (known format)
- Encrypted files - unknown format

  Searches for outbound files that were encrypted using unknown encryption formats. The rules for this policy are:

  - Encrypted files - unknown format
  - Encrypted files - unknown format (Wide)
- IT asset information

  Searches for suspicious outbound transactions, such as those containing information about the network, credit card magnetic tracks, and database files. Rules in this policy include:

  - IT asset information (Default)
  - IT asset information (Narrow)
  - IT asset information (Wide)
- Suspected Malware Communication

- Identifies traffic that is thought to be malware “phoning home” or attempting to steal information. Detection is based on the analysis of traffic patterns from known infected machines. Applies only when Forcepoint Web Security is installed. Rules in this policy include:
  - Suspected Malware Communication
- Password files

  Searches for outbound password files, such as a SAM database and UNIX / Linux passwords files. Rules in this policy include:
  - Password Files: Shadow Files
  - Password Files: Shadow Files (Wide)
  - Password Files: Password Files
  - Password Files: Password Files (Wide)
  - Password Files: SAM files
  - Password Files: General files
- Suspicious Behavior Over Time

  Accumulates transaction data such as number of HTTP/S posts, post size, and encryption information over a period of time to search for suspicious behavior that could be indicative of malicious activity. Some rules apply only when Forcepoint Web Security is installed. Rules in this policy include:
  - Number of HTTP/S Posts per Time
  - Cumulative Post Size per Time
  - Cumulative Generic Encryption per Time

Email DLP policy

Predefined Policies and Classifiers | Forcepoint DLP | v8.6.x

The Email DLP “quick policy” includes the PCI policy, PHI policies, and PII policies listed in this document (including financial policies).In addition, the Email DLP policy includes:

- Questionable images

  Detects images that may be objectionable or pose a liability to your organization. There is one rule in this policy:
  - Questionable images
- Acceptable use

  Detects dictionary terms that may be unacceptable in the work place, including adult, drugs, gambling, hate speech, job search, and violent terms. There is one rule in this policy:
  - Acceptable use

  This policy includes terms in 12 languages:
  - English
  - French

- Spanish
- Italian
- German
- Dutch
- Portuguese
- Chinese
- Taiwanese
- Turkish
- Japanese
- Russian

Mobile DLP policy

The Mobile DLP "quick policy" includes the PCI policy, PHI policies, and PII policies listed in this document (including financial policies). In addition, the Mobile DLP policy includes:

- Questionable images

  Detects images that may be objectionable or pose a liability to your organization. There is one rule in this policy:

  - Questionable images
- Acceptable use

  Detects dictionary terms that may be unacceptable in the work place, including adult, drugs, gambling, hate speech, job search, and violent terms. There is one rule in this policy:

  - Acceptable use

  This policy includes terms in 12 languages:

  - English
  - French
  - Spanish
  - Italian
  - German
  - Dutch
  - Portuguese
  - Chinese
  - Taiwanese
  - Turkish
  - Japanese
  - Russian

Discovery policies

The predefined discovery policies are categorized as follows:

Acceptable Use

- Acceptable Use- Indecent Images for Discovery

  Policy for detection of indecent images using image analysis.This may cause false positives. The rule for this policy is:

  - Non Acceptable Use - Indecent Images
- Acceptable Use- Obscenities & Racism for Discovery

  Policy for detection of offensive or inappropriate terms (non-editable). The rules for this policy are:

  - Non Acceptable Use In file names - inappropriate
  - Non Acceptable Use In file names - medium
  - Non Acceptable Use In file names - offensive

Company Confidential and Intellectual Property

- Bids and Tenders for Discovery

  Policy for detecting bids, proposals, and tenders, such as responses to request for proposal (RFP) and invitation for bids (IFB) documents.

  - Bids and Tenders (Wide)
  - Bids and Tenders (Default)
  - Bids and Tenders (Narrow)

- Call Detail Records for Discovery

  Policy for detection of Call Detail Record (CDR) files. The rules for this policy are:

  - CDR: Call details rows
  - CDR: Call details headers
- Database Files

  Policy for the detection of database files. The rules for this policy are:

  - Database File: Ability Office File
  - Database File: Borland Reflex 2 File
  - Database File: dBase File
  - Database File: Filemaker File
  - Database File: Lotus Notes NSF File
  - Database File: Microsoft Access File
  - Database File: Microsoft Exchange Server File
  - Database Files: Microsoft Program Database File
  - Database File: Microsoft Works for DOS File
  - Database File: Microsoft Works for Mac File
  - Database File: Microsoft Works for Windows File
  - Database File: MORE File
  - Database Files: MySQL Table Definition File
  - Database File: Paradox File
  - Database Files: SAS7BDAT Database Storage File
  - Database File: SmartWare II File
  - Database Files: SQLite Database File
- Digitally Signed PDF Files for Discovery

  Policy for detection of digitally signed PDF files. The rule for this policy is:

  - Digitally Signed PDF File (Native)
- Financial information for Discovery

  Policy for detection of files containing general, personal, and investment financial information.The rules for this policy are:

  - Financial Information - Personal
  - Financial Information - Investment
  - Financial Information - General
- Hardware Source code for Discovery

  Policy for detection of source code for various hardware languages: SPICE and its flavors, VHDL and Verilog. This policy is comprised of several rules for each language, each covering a different aspect of the detected texts.

  The rules for this policy are:

  - SPICE Source code (Berkeley version)

- SPICE Source code
- Verilog Source code PreciseID NLP
- VHDL Source Code

- IMEI for Discovery

  Policy for detection of serial (IMEI) numbers of cell phones. The International Mobile Equipment Identity (IMEI) is a number unique to every GSM and UMTS and iDEN mobile phone as well as some satellite phones. It is usually found printed on the phone underneath the battery.

  The rules for this policy are:

  - IMEI: with proximity

- Location Coordinates for Discovery

  Policy for detection of location coordinates. The rules for this policy are:

  - Location Coordinates: Latitude-Longitude
  - Location Coordinates: UTM

- Movie Manuscripts for Discovery

  Policy for detection of movie and TV script files.

  The rule for this policy is:

  - Movie and TV Manuscripts

- Network Security Information for Discovery

  Policy for detection of network security documents and network diagrams. This policy detects Network diagrams by searching for IP addresses, MAC addresses and various terms common to such documents. In order to achieve complete coverage, first 2 rules and one of the MAC address rules must be selected.

  The rules for this policy are:

  - Network Information and Security (patterns and IP)
  - Network Information and Security (textual patterns)
  - MAC Addresses (default)

- Patents for Discovery

  Policy for detection of patents and patent applications

  The rule for this policy is:

  - Patents detection

- Petroleum and Gas-Sensitive information for Discovery

  Detect leakage of sensitive data in the Oil and Gas industry and, in particular, information pertaining to oil prospecting and drilling.

  The rules for this policy are:

  - Petroleum and Gas-Sensitive Information: Latitude-Longitude Location Coordinates
  - Petroleum and Gas-Sensitive Information: Logs and Survey Reports
  - Petroleum and Gas-Sensitive Information: Petroleum-Related File Extensions
  - Petroleum and Gas-Sensitive Information: Prospecting Related Terms

- Petroleum and Gas-Sensitive Information: UTM Location Coordinates

- Security Software Files for Discovery

  Policy for detection of security software files.

  The rule for this policy is:

  - Security Software Files: Splunk Enterprise Security Event Log

- Software Design Documents for Discovery

  Policy for detection of software design documents.

  The rule for this policy is:

  - Software Design Documents

- Software Source Code for Discovery

  Policy for detection of computer source code. The rules for this policy are:

  - Software Source Code: C family or Java
  - Software Source Code: C family or Java Extensions
  - Software Source Code: Python (Default)
  - Software Source Code: Python (Wide)

- Strategic Planning Documents for Discovery

  Policy for detection of documents of prime strategic value, such as business and marketing plans. The rule for this policy is:

  - Strategic Planning Documents

- License Keys for Discovery

  Policy to identify Microsoft license keys. This helps mitigate software piracy and unauthorized usage of corporate assets. The rule for this policy is:

  - Microsoft license keys

Employee Discontent

- CV and Resume in English for Discovery

  Policy for detection of documents comprising resumes and CVs in English. The rule for this policy is:

  - CV and Resume in English

- CV and Resume in French for Discovery

  Policy for detection of documents comprising resumes and CVs in French. The rules for this policy are:

  - CV and Resume in French (Wide)
  - CV and Resume in French (Default)
  - CV and Resume in French (Narrow)

- CV and Resume in German for Discovery

  Policy for detection of documents comprising resumes and CVs in German. The rules for this policy are:

- CV and Resume in German (Wide)
- CV and Resume in German (Default)
- CV and Resume in German (Narrow)

- CV and Resume in Spanish for Discovery

  Policy for detection of documents comprising resumes and CVs in Spanish. The rules for this policy are:
  - CV and Resume in Spanish (Wide)
  - CV and Resume in Spanish (Default)
  - CV and Resume in Spanish (Narrow)
- Israel CV and Resume for Discovery

  Policy for detection of documents comprising resumes and CVs in Hebrew and English. The rule for this policy is:
  - Israel CV and Resume: Hebrew
- Russia CV and Resume for Discovery

  Policy for detection of documents comprising resumes and CVs in Russian, Ukrainian, and English. The rule for this policy is:
  - Russia CV and Resume: Russian or Ukrainian
- Ukraine CV and Resume for Discovery

  Policy for detection of documents comprising resumes and CVs in Ukrainian, Russian, and English. The rule for this policy is:
  - Ukraine CV and Resume: Russian or Ukrainian

Financial Information

- 401(k) and 403(b) forms for Discovery

  Policy for detection of 401(k) and 403(b) form that contain private information of employees. The rules for this policy are:
  - 401(k) form (Default)
  - 403(b) form (Default)
- Mergers and Acquisitions for Discovery

  Policy for detection of Information suspected to be related to mergers and acquisitions. The rule for this policy is:
  - Mergers and Acquisitions information
- Austria Finance for Discovery

  Policy for detection of Austrian financial information.
  - Austria Finance: Austrian IBAN (Default)
  - Austria Finance: Austrian IBAN (Wide)
- Belgium Finance for Discovery

  Policy for detection of Belgian financial information.

- Belgium Finance: Belgian IBAN (Default)
- Belgium Finance: Belgian IBAN (Wide)

- Bulgaria Finance for Discovery

  Policy for detection of Bulgarian financial information.
  - Bulgaria Finance: Bulgarian IBAN (Default)
  - Bulgaria Finance: Bulgarian IBAN (Wide)
- Croatia Finance for Discovery

  Policy for detection of Croatian financial information. The rules for this policy are:
  - Croatia Finance: Croatian IBAN (Default)
  - Croatia Finance: Croatian IBAN (Wide)
- Cyprus Finance for Discovery

  Policy for detection of Cypriot financial information. The rules for this policy are:
  - Cyprus Finance: Cypriot IBAN (Default)
  - Cyprus Finance: Cypriot IBAN (Wide)
- Czech Republic Finance for Discovery.

  Policy for detection of Czech financial information. The rules for this policy are:
  - Czech Republic Finance: Czech IBAN (Default)
  - Czech Republic Finance: Czech IBAN (Wide)
- Denmark Finance for Discovery

  Policy for detection of Danish financial information. This may cause false positives. The rule for this policy is:
  - Denmark Finance: Danish IBAN
- Estonia Finance for Discovery

  Policy for detection of Estonian financial information. The rules for this policy are:
  - Estonia Finance: Estonian IBAN (Default)
  - Estonia Finance: Estonian IBAN (Wide)
- Financial Information for Discovery

  Policy for detection of files containing general, personal, and investment financial information. The rules for this policy are:
  - Financial Information - Personal Rule for detecting combinations of terms related to financial transactions, credit history, financial status and other personal financial data.
  - Financial Information - Investment
  - Financial Information - General
- Finland Finance for Discovery

  Policy for detection of Finnish financial information. This may cause false positives. The rule for this policy is:
  - Finland Finance: Finnish IBAN (default)

- France Finance for Discovery

  Policy for detection of French financial information. This may cause false positives. The rule for this policy is:

  - France Finance: French IBAN (default)
- Germany Finance for Discovery

  Policy for detection of German financial information. This may cause false positives. The rule for this policy is:

  - Germany Finance: German IBAN (default)
- Greece Finance for Discovery

  Policy for detection of Greek financial information. This may cause false positives. The rule for this policy is:

  - Greece Finance: Greece IBAN (default)
- Hungary Finance for Discovery

  Policy for detection of Hungarian financial information. The rules for this policy are:

  - Hungary Finance: Hungarian IBAN (Default)
  - Hungary Finance: Hungarian IBAN (Wide)
- Iceland Finance for Discovery

  Policy for detection of Icelandic financial information.This may cause false positives. The rule for this policy is:

  - Iceland Finance: Icelandic IBAN (default)
- Ireland Finance for Discovery

  Policy for detection of Irish financial information. This may cause false positives. The rules for this policy are:

  - Ireland Finance: Irish IBAN (default)
  - Ireland Finance: Irish Bank Account
- ISIN and CUSIP for Discovery

  Policy for detection of International Securities Identification Number (ISIN), which uniquely identifies a security. The ISIN code is a 12-character alphanumerical code that serves as uniform identification of a security at trading and settlement. This may cause false positives. The rules for this policy are:

  - ISIN number - with proximity
  - CUSIP Numbers (default)
- Italy Finance for Discovery

  Policy for detection of Italian financial information. This may cause false positives. The rule for this policy is:

  - Italy Finance: Italian IBAN (default)
- Latvia Finance for Discovery

  Policy for detection of Latvian financial information. The rules for this policy are:

  - Latvia Finance: Latvian IBAN (Default)
  - Latvia Finance: Latvian IBAN (Wide)

- Lithuania Finance for Discovery

  Policy for detection of Lithuanian financial information. The rules for this policy are:

  - Lithuania Finance: Lithuanian IBAN (Default)
  - Lithuania Finance: Lithuanian IBAN (Wide)
- Luxembourg Finance for Discovery

  Policy for detection of Luxembourgian financial information. The rules for this policy are:

  - Luxembourg Finance: Luxembourgian IBAN (Default)
  - Luxembourg Finance: Luxembourgian IBAN (Wide)
- Malta Finance for Discovery

  Policy for detection of Maltese financial information. The rules for this policy are:

  - Malta Finance: Maltese IBAN (Default)
  - Malta Finance: Maltese IBAN (Wide)
- Mexico Finance for Discovery

  Policy for detection of Mexican financial information. The rules for this policy are:

  - Mexico Finance: Standardized Bank Code (CLABE) (Wide)
  - Mexico Finance: Standardized Bank Code (CLABE) (Default)
- Netherlands Finance for Discovery

  Policy for detection of Dutch financial information. This may cause false positives. The rule for this policy is:

  - Netherlands Finance: Netherlands IBAN (default)
- Norway Finance for Discovery

  Policy for detection of Norwegian financial information. This may cause false positives. The rule for this policy is:

  - Norway Finance: Norwegian IBAN (default)
- People’s Republic of China for Discovery

  Policy for detection of PRC financial information. The rules for this policy are:

  - People’s Republic of China Finance: Business Registration Number - 15 digits
  - People’s Republic of China Finance: Credit Card
  - People’s Republic of China Finance: Financial cards Track1
  - People’s Republic of China Finance: Financial cards Track2
  - People’s Republic of China Finance: Financial cards Track3
  - People’s Republic of China Finance: Union Pay Credit Card
- Poland Finance Information for Discovery:

  Policy for detection of Polish financial information. This may cause false positives. The rule for this policy is:

  - Poland Finance: Polish IBAN (default)

- Portugal Finance for Discovery

  Policy for detection of Portuguese financial information. The rules for this policy are:

  - Portugal Finance: Portuguese IBAN (Default)
  - Portugal Finance: Portuguese IBAN (Wide)
- Pricing Information for Discovery

  Policy for detection of files containing pricing information and pricelists.

  The rules for this policy are:

  - Pricing Information predefined 1
  - Pricing Information predefined 2
- Romania Finance for Discovery

  Policy for detection of Romanian financial information. The rules for this policy are:

  - Romania Finance: Romanian IBAN (Default)
  - Romania Finance: Romanian IBAN (Wide)
- RTN/ABA Numbers for Discovery

  Policy for detection of Routing Transit Numbers (RTN), also known as American Bankers Association (ABA) numbers. RTN numbers are nine digit bank codes, used in the United States to identify, for example, which financial institution checks and banknotes are drawn upon.This may cause false positives. The rules for this policy are:

  - RTN/ABA: Default
  - RTN/ABA: Narrow
- Saudi Arabia Finance for Discovery

  Policy for detection of Saudi Arabia financial information. The rule for this policy is:

  - Saudi Arabia Finance: Saudi Arabia IBAN (default)
- Slovakia Finance for Discovery

  Policy for detection of Slovak financial information. The rules for this policy are:

  - Slovakia Finance: Slovak IBAN (Default)
  - Slovakia Finance: Slovak IBAN (Wide)
- Slovenia Finance for Discovery

  Policy for detection of Slovenian financial information. The rules for this policy are:

  - Slovenia Finance: Slovene IBAN (Default)
  - Slovenia Finance: Slovene IBAN (Wide)
- Spain Finance Information for Discovery:

  Policy for detection of Spanish financial information. This may cause false positives. The rule for this policy is:

  - Spain Finance: Spanish IBAN (default)

- Sweden Finance Information for Discovery:

  Policy for detection of Swedish financial information. This may cause false positives. The rule for this policy is:

  - Sweden Finance: Swedish IBAN (default)
- Switzerland Finance Information for Discovery:

  Policy for detection of Swiss financial information. This may cause false positives. The rule for this policy is:

  - Switzerland Finance: Swiss IBAN (default)
- Turkey Finance for Discovery:

  Policy for detection of Turkish financial information. This may cause false positives. The rules for this policy are:

  - Turkey Finance: Tax ID Number
  - Turkey Finance: Turkish IBAN
- UK Finance Information for Discovery:

  Policy for detection of UK financial information. This may cause false positives. The rule for this policy is:

  - UK Finance: UK IBAN (default)
- IRS Tax Forms for Discovery

  Policy for the detection of IRS Tax Forms; for example, Form W-2, Form W-4, and Form 1040. The rules for this policy are:

  - IRS Tax Forms: Form 1040 and Form 1040A (Wide)
  - IRS Tax Forms: Form 1040 and Form 1040A (Default)
  - IRS Tax Forms: Form 1040 and Form 1040A (Narrow)
  - IRS Tax Forms: Form 1040EZ (Wide)
  - IRS Tax Forms: Form 1040EZ (Default)
  - IRS Tax Forms: Form 1040EZ (Narrow)
  - IRS Tax Forms: Form W-2
  - IRS Tax Forms: Form W-4 (Wide)
  - IRS Tax Forms: Form W-4 (Default)
  - IRS Tax Forms: Form W-4 (Narrow)
  - IRS Tax Forms: Form W-4P (Wide)
  - IRS Tax Forms: Form W-4P (Default)
  - IRS Tax Forms: Form W-4P (Narrow)
  - IRS Tax Forms: Form W-4V (Wide)
  - IRS Tax Forms: Form W-4V (Default)
  - IRS Tax Forms: Form W-4V (Narrow)
  - IRS Tax Forms: Form W-9 (Wide)
  - IRS Tax Forms: Form W-9 (Default)
  - IRS Tax Forms: Form W-9 (Narrow)

- IRS Tax Forms: Form W-9S (Wide)
- IRS Tax Forms: Form W-9S (Default)
- IRS Tax Forms: Form W-9S (Narrow)

EU General Data Protection Regulation (GDPR)

The description and list of rules for each policy in this category can be found in other sections of this document.

- Austria PII for Discovery
- Belgium Finance for Discovery
- Belgium PII for Discovery
- Biometric Files for Discovery
- Bulgaria Finance for Discovery
- Bulgaria PII for Discovery
- Croatia Finance for Discovery
- Croatia PII for Discovery
- CV and Resume in English for Discovery
- CV and Resume in French for Discovery
- CV and Resume in German for Discovery
- CV and Resume in Spanish for Discovery
- Cyprus Finance for Discovery
- Cyprus PII for Discovery
- Czech Republic Finance for Discovery
- Czech Republic PII for Discovery
- Denmark Finance For Discovery
- Denmark PII for Discovery
- Estonia Finance for Discovery
- Estonia PII for Discovery
- Finland Finance For Discovery
- Finland PII for Discovery
- France Finance For Discovery
- France PII for Discovery
- Germany Finance For Discovery
- Germany PII for Discovery
- Greece Finance For Discovery
- Greece PII for Discovery
- Hungary Finance for Discovery

- Hungary PII for Discovery
- IMEI for Discovery
- Ireland Finance For Discovery
- Ireland PII for Discovery
- Italy Finance For Discovery
- Italy PHI For Discovery
- Italy Private Information for Discovery
- Latvia Finance for Discovery
- Latvia PII for Discovery
- Lithuania Finance for Discovery
- Lithuania PII for Discovery
- Luxembourg Finance for Discovery
- Luxembourg PII for Discovery
- Malta Finance for Discovery
- Malta PII for Discovery
- Netherlands Finance For Discovery
- Netherlands PII for Discovery
- PCI for discovery
- Poland Finance For Discovery
- Poland PII for Discovery
- Portugal Finance for Discovery
- Portugal PII for Discovery
- Romania Finance for Discovery
- Romania PII for Discovery
- Slovakia Finance for Discovery
- Slovakia PII for Discovery
- Slovenia Finance for Discovery
- Slovenia PII for Discovery
- Spain Finance For Discovery
- Spain PII for Discovery
- Sweden Finance For Discovery
- Sweden PHI For Discovery
- Sweden PII for Discovery
- UK Finance For Discovery
- UK PHI For Discovery
- UK PII For Discovery

Indicators of Compromise

- Database Dumps/Backup Files for Discovery

  Policy for detecting records of SQL table data extracted from a database. The rules for this policy are:

  - Database Dumps/Backup Files: MySQL-Format Database Dump (Wide)
  - Database Dumps/Backup Files: MySQL-Format Database Dump (Default)
  - Database Dumps/Backup Files: Microsoft Tape Format
- Private Keys for Discovery

  Policy for detecting private keys or file formats that contain them. The rules for this policy are:

  - Private Keys: DSA Private Key
  - Private Keys: Elliptic Curve Private Key
  - Private Keys: JSON Keystore File Private Key
  - Private Keys: OpenSSH Private Key
  - Private Keys: PGP Private Key
  - Private Keys: PKCS #1 Private Key
  - Private Keys: Encrypted PKCS #8 Private Key
  - Private Keys: Unencrypted PKCS #8 Private Key
  - Private Keys: PKCS #12 File
  - Private Keys: SSH2 Private Key
  - Private Keys: Textual PPK Private Key
- .REG Files for Discovery

  Policy for detecting .REG files (Windows Registry files). The rule for this policy is:

  - .REG File
- Suspected Malicious Dissemination for Discovery

  Policy for the detection of a suspected malicious content dissemination such as: encrypted or manipulated information, passwords files, credit card tracks, suspected applications and dubious content such as information about the network, software license keys, and database files. The rules for this policy are:

  - Suspected Malicious Dissemination: Email Address and Password (Wide)
  - Suspected Malicious Dissemination: Email Address and Password (Default)
  - Suspected Malicious Dissemination: Encrypted File (Known Format)
  - Suspected Malicious Dissemination: Generic Encryption Detection
  - Suspected Malicious Dissemination: IT Asset Information
  - Suspected Malicious Dissemination: Malicious Concealment
  - Suspected Malicious Dissemination: Password (Wide)
  - Suspected Malicious Dissemination: Password (Default)

- Suspected Malicious Dissemination: Password (Narrow)
- Suspected Malicious Dissemination: Password File
- Suspected Malicious Dissemination: Suspected Application (Steganography and Encryption)

- Suspicious Data Concealment Applications

  Policy for detection of data concealment applications. The rule for this policy is:

  - Suspicious data concealment applications: Steganography applications

Payment Card Information (PCI)

- PCI Audit for discovery

  A permissive policy for detecting potential credit-card-numbers. The policy contains several rules to address corner cases, such as numbers that appear as part of a long sequence, with user-defined delimiters etc. Most of the rules in the policy may cause high rate of false positives and are not recommended for usage in production mode. The rules for this policy are:

  - PCI Audit: No Word Boundaries
  - PCI Audit: Non-Delimited
  - PCI Audit: User-Defined Delimiter
  - PCI Audit: CCN and Expiration Date
  - PCI Audit: CCN and CVV
  - PCI Audit: CCN Without Validation
  - PCI Audit: Credit Card Number (Extra Wide)
  - PCI Audit: Credit Card Number (Default)
  - PCI Audit: Credit Card Magnetic Strip
  - PCI Audit: Masked Credit Card Number
  - PCI Audit: CCN in Non-English Characters
  - PCI Audit: User-Defined IIN (Wide)
  - PCI Audit: User-Defined IIN (Default)
  - PCI Audit: User-Defined IIN (Narrow)

- PCI Policy for discovery

  The Payment Card Industry Data Security Standard (PCI DSS) is an industry standard, accepted internationally by all major credit card issuers. The standard is enforced on companies and organization that accept credit card payments or process, store, or transmit cardholder data. The standard mandates, among others, that credit card numbers and cardholder data should be highly secured and that transactions comprising data should be encrypted. The rules for this policy are:

  - PCI : Credit Cards - Wide
  - PCI : Credit Cards - Default
  - PCI : Credit Cards - Narrow

- PCI: Credit Card Magnetic Strips

Protected Health Information (PHI)

- Australia PHI for Discovery

  Policy for detection of protected health information for Australian citizens. The rules for this policy are:

  - Australia PHI: DICOM
  - Australia PHI: Medicare Number and Sensitive Disease or Drug
  - Australia PHI: Medicare Number and Common Medical Condition
  - Australia PHI: SPSS Text File
- Health data For Discovery

  Policy for detection of data types pertaining to medical conditions, drugs etc

  The rules for this policy are:

  - Health Data: DNA Profile (Default)
  - Health Data: DNA Profile (Narrow)
  - Health Data: DICOM
  - Health Data: DOB and Name
  - Health Data: ICD9 Code
  - Health Data: ICD9 Code and Description
  - Health Data: ICD9 Code and Name
  - Health Data: ICD9 Description and Name
  - Health Data: ICD10 Code
  - Health Data: ICD10 Code and Description
  - Health Data: ICD10 Code and Name
  - Health Data: ICD10 Description and Name
  - Health Data: Medical Form (Wide)
  - Health Data: Medical Form (Default)
  - Health Data: Medical Form (Narrow)
  - Health Data: Name and Common Medical Condition
  - Health Data: Name and Sensitive Disease or Drug
  - Health Data: NDC Number (Default)
  - Health Data: NDC Number (Narrow)
  - Health Data: SPSS Text File
- Israel PHI For Discovery

  Policy for detection of protected health information for Israeli citizens, to promote compliance with Israeli privacy rules and Israeli patients rights law of 1996. The rules for this policy are:

- Israel PHI: DICOM
- Israel PHI: Identity Number and General Medical Information
- Israel PHI: Identity Number and Sensitive Medical Information
- Israel PHI: Name and Sensitive Medical Information
- Israel PHI: Name and General Medical Information
- Israel PHI: SPSS Text File

- Italy PHI For Discovery

  Policy for detection of protected health information for Italy citizens. The rules for this policy are:

  - Italy PHI: Codice Fiscale and Health Information
  - Italy PHI: DICOM
  - Italy PHI: Name and Health Information
  - Italy PHI: SPSS Text File

- Norway PHI For Discovery

  Policy for detection of protected health information for Norwegian citizens. The rules for this policy are:

  - Norway PHI: DICOM
  - Norway PHI: ICD10 Code
  - Norway PHI: ICD10 Code and Description
  - Norway PHI: ICD10 Code and First Name
  - Norway PHI: ICD10 Code and Full Name
  - Norway PHI: ICD10 Code and Last Name
  - Norway PHI: ICD10 Code and PIN
  - Norway PHI: ICD10 Description
  - Norway PHI: Name and Health Information
  - Norway PHI: Name and Personal Number
  - Norway PHI: Personal Number
  - Norway PHI: Personal Number and Health Information
  - Norway PHI: SPSS Text File

- Sweden PHI For Discovery

  A policy for discovery of protected health information (PHI) of Swedish citizens and residents. The policy comprises rules for detection of Health information and Medical Conditions (in Swedish or English), in proximity to personally identifiable information such as personal number (personnummer), or name. The rules for this policy are:

  - Sweden PHI: DICOM
  - Sweden PHI: DNA Profile
  - Sweden PHI: ICD10 Code
  - Sweden PHI: ICD10 Code and Description

- Sweden PHI: ICD10 Code and Name (Wide)
- Sweden PHI: ICD10 Code and Name (Default)
- Sweden PHI: ICD10 Code and Name (Narrow)
- Sweden PHI: ICD10 Code and Personal Number
- Sweden PHI: ICD10 Description
- Sweden PHI: Name and Health Information
- Sweden PHI: Name and Sensitive Disease or Drug
- Sweden PHI: Personal Number and Health Information
- Sweden PHI: Personal Number and Sensitive Disease or Drug
- Sweden PHI: SPSS Text File

- UK PHI For Discovery

  Policy for detection of UK NHS numbers.The rules for this policy are:

  - UK PHI: DICOM
  - UK PHI: NHS Number (Default)
  - UK PHI: NHS Number (Narrow)
  - UK PHI: SPSS Text File

- US PHI For Discovery

  A policy for detection of protected health information of US citizens. The rules for this policy are:

  - US PHI: DICOM
  - US PHI: Medical Form (Wide)
  - US PHI: Medical Form (Default)
  - US PHI: Medical Form (Narrow)
  - US PHI: Name and Common Medical Condition (Default)
  - US PHI: Name and Common Medical Condition (Narrow)
  - US PHI: Name and HICN
  - US PHI: Name and Sensitive Disease or Drug (Default)
  - US PHI: Name and Sensitive Disease or Drug (Narrow)
  - US PHI: SPSS Text File
  - US PHI: SSN and Common Medical Condition
  - US PHI: SSN and Sensitive Disease or Drug

Personally Identifiable Information (PII)

- Australia PII for Discovery

  Policy to detect files containing personally identifiable information for residents of Australia. The rules for this policy are:

  - Australia PII: Credit File (Wide)

- Australia PII: Credit File (Default)
- Australia PII: Credit File (Narrow)
- Australia PII: Driver License Number
- Australia PII: Email Address and Password (Wide)
- Australia PII: Email Address and Password (Default)
- Australia PII: Tax File Number (Wide)
- Australia PII: Tax File Number (Default)

- Austria PII for Discovery

  Policy for detection of Austrian private information. The rules for this policy are:

  - Austria PII: CCN and Name
  - Austria PII: Crime and Name
  - Austria PII: Email Address and Password (Wide)
  - Austria PII: Email Address and Password (Default)
  - Austria PII: Ethnicity and Name
  - Austria PII: Sensitive Disease and Name
  - Austria PII: Social Security Number (Wide)
  - Austria PII: Social Security Number (Default)
  - Austria PII: Social Security Number and Name (Wide)
  - Austria PII: Social Security Number and Name (Default)

- Belgium PII for Discovery

  Policy for detection of Belgian private information. The rules for this policy are:

  - Belgium PII: Email Address and Password (Wide)
  - Belgium PII: Email Address and Password (Default)
  - Belgium PII: Name and ID Card Number (Wide)
  - Belgium PII: Name and ID Card Number (Default)
  - Belgium PII: Name and Passport Number (Wide)
  - Belgium PII: Name and Passport Number (Default)
  - Belgium PII: ID Card Number
  - Belgium PII: Passport Number

- Biometric Files for Discovery

  Policy for detection of biometric files. The rules for this policy are:

  - Biometric Files for Discovery: NIEM-Conformant XML
  - Biometric Files for Discovery: OASIS XML Common Biometric Format (XCBF)

- Brazil PII for Discovery

  Policy for detection of combinations of Brazilian PII like Brazilian full names, CPF numbers, and health conditions. The rules for this policy are:

  - Brazil PII: Email Address and Password (Wide)

- Brazil PII: Email Address and Password (Default)
- Brazil PII: Name and CPF
- Brazil PII: Name and Sensitive Disease
- Brazil PII: CPF and Sensitive Disease
- Brazil PII: Identity Card Number
- Brazil PII: National Register of Legal Entities Number (Wide)
- Brazil PII: National Register of Legal Entities Number (Default)

- Bulgaria PII for Discovery

  Policy for detection of Bulgarian private information. The rules for this policy are:
  - Bulgaria PII: Unified Civil Number (Wide)
  - Bulgaria PII: Unified Civil Number (Default)
- Canada PII for Discovery

  Policy for detection of Canadian private information. The rules for this policy are:
  - Canada PII: Credit File (Wide)
  - Canada PII: Credit File (Default)
  - Canada PII: Credit File (Narrow)
  - Canada PII: Email Address and Password (Wide)
  - Canada PII: Email Address and Password (Default)
  - Canada PII: SIN and Name
  - Canada PII: Name and Canadian Driver's License Number
- Chile PII for Discovery

  Policy for detection of Chilean private information. The rules for this policy are:
  - Chile PII: Email Address and Password (Wide)
  - Chile PII: Email Address and Password (Default)
  - Chile PII: National Identity Number (RUN/RUT) (Wide)
  - Chile PII: National Identity Number (RUN/RUT) (Default)
- Colombia PII for Discovery

  Policy for detection of Colombian private information. The rules for this policy are:
  - Colombia PII: Email Address and Password (Wide)
  - Colombia PII: Email Address and Password (Default)
  - Colombia PII: Identification Number (Wide)
  - Colombia PII: Identification Number (Default)
- Costa Rica PII for Discovery

  Policy for detection of Costa Rican private information. The rules for the policy are:
  - Costa Rica PII: Email Address and Password (Wide)
  - Costa Rica PII: Email Address and Password (Default)

- Costa Rica PII: Identification Number (Default)
- Costa Rica PII: Identification Number (Narrow)
- Costa Rica PII: Legal Identification Number (Default)
- Costa Rica PII: Legal Identification Number (Narrow)

- Credit Card Numbers for Discovery

  Policy for detection of credit card numbers. The rules for this policy are:

  - Credit Card Numbers: Credit Cards (Wide)
  - Credit Card Numbers: Credit Cards (Default)
  - Credit Card Numbers: Credit Cards (Narrow)
  - Japanese Credit Cards: All Credit Cards

- Croatia PII for Discovery

  Policy for detection of Unique Master Citizen Numbers and Personal identification numbers. The rules for this policy are:

  - Croatia PII: Unique Master Citizen Number (Wide)
  - Croatia PII: Unique Master Citizen Number (Default)
  - Croatia PII: Personal identification number (Wide)
  - Croatia PII: Personal identification number (Default)

- Cyprus PII for Discovery

  Policy for detection of Cypriot private information. The rules for this policy are:

  - Cyprus PII: Tax Identification Code (Wide)
  - Cyprus PII: Tax Identification Code (Default)

- Czech Republic PII for Discovery

  Policy for detection of Czech Republic private information. The rules for this policy are:

  - Czech Republic PII: Email Address and Password (Wide)
  - Czech Republic PII: Email Address and Password (Default)
  - Czech Republic PII: Rodne Cislo (Wide)
  - Czech Republic PII: Rodne Cislo (Default)

- Denmark PII for Discovery

  Policy for detection of Danish personally identifiable information. The rule for this policy is:

  - Denmark PII: CPR Number
  - Denmark PII: Email Address and Password (Wide)
  - Denmark PII: Email Address and Password (Default)

- EIN for Discovery

  Policy for detection of Employer Identification Numbers (EIN). This may cause false positives. The rule for this policy is:

  - EIN: Default

- Email Address for Discovery

Policy for detection of files containing a large number of email addresses. The rules for this policy are:

- Email: Multiple Email addresses
- Email: Multiple Email addresses with different domains

- Estonia PII for Discovery

  Policy for detection of Estonian private information. The rules for this policy are:

  - Estonia PII: Personal Identification Code (Wide)
  - Estonia PII: Personal Identification Code (Default)

- Finland PII for Discovery

  Policy for detection of Finnish personally identifiable information. The rule for this policy is:

  - Finland PII: Email Address and Password (Wide)
  - Finland PII: Email Address and Password (Default)
  - Finland PII: Social Security Number

- France PII for Discovery

  Policy for detection of French personally identifiable information. The rule for this policy is:

  - France PII: Email Address and Password (Wide)
  - France PII: Email Address and Password (Default)
  - France PII: INSEE numbers

- General Sensitive Information for Discovery

  Policy for detection of sensitive private information, whose loss may damage the privacy or the reputation of the pertained person or expose the person to potential fraud. The policy comprises rules for detection of various kinds of sensitive private information, such as protected health information, account numbers and passwords. The rules for this policy are:

  - General Sensitive Information: Credit Card Magnetic Strip
  - General Sensitive Information: US Credit Card Number
  - General Sensitive Information: EU Credit Card Number
  - General Sensitive Information: DNA Profile
  - General Sensitive Information: Name and Account Number
  - General Sensitive Information: Name and Crime
  - General Sensitive Information: Name and Ethnicity
  - General Sensitive Information: Name and Grade
  - General Sensitive Information: Name and Sensitive Disease
  - General Sensitive Information: Password (Wide)
  - General Sensitive Information: Password (Default)
  - General Sensitive Information: Password (Narrow)
  - Sensitive Private: PIN

- Germany PII for Discovery

Policy to detect private and sensitive information in German, for German-speaking countries. The rules for this policy are:

- Germany PII: Credit Card Number and Name
- Germany PII: Email Address and Password (Wide)
- Germany PII: Email Address and Password (Default)
- Germany PII: Ethnicity and Name
- Germany PII: Sensitive Disease and Name
- Germany PII: Crime and Name

- Greece PII for Discovery

  Policy for detection of Greek personally identifiable information. The rules for this policy are:

  - Greece PII: AFM Number
  - Greece PII: AFM number (Wide)
  - Greece PII: AFM Number and Name
  - Greece PII: AFM number and Name (Wide)
  - Greece PII: Email Address and Password (Wide)
  - Greece PII: Email Address and Password (Default)
  - Greece PII: ID Number
  - Greece PII: ID Number and Name
  - Greece PII: ID and Name (Wide)
  - Greece PII: Sensitive Medical Information and Name
  - Greece PII: Sensitive Medical Information and Name (Wide)

- Hong Kong PII for Discovery

  Policy to detect files containing personally identifiable information for residents of Hong Kong. The rules for this policy are:

  - Hong Kong PII: Email Address and Password (Wide)
  - Hong Kong PII: Email Address and Password (Default)
  - Hong Kong PII: ID Number (Wide)
  - Hong Kong PII: ID Number (Default)
  - Hong Kong PII: ID Number (Narrow)
  - Hong Kong PII: ID Number and Address (Wide)
  - Hong Kong PII: ID Number and Address (Default)
  - Hong Kong PII: ID Number and Address (Narrow)
  - Hong Kong PII: ID Number and Surname (Wide)
  - Hong Kong PII: ID Number and Surname (Default)
  - Hong Kong PII: ID Number and Surname (Narrow)
  - Hong Kong PII: ID Number, Surname and Address (Wide)
  - Hong Kong PII: ID Number, Surname and Address (Default)
  - Hong Kong PII: ID Number, Surname and Address (Narrow)

- Hong Kong PII: Surname and Address (Default)
- Hong Kong PII: Surname and Address (Narrow)
- Hong Kong PII: Surname and Address (Wide)

- Hungary PII for Discovery

  Policy for detection of Hungarian private information. The rules for this policy are:

  - Hungary PII: Hungarian Szemelyi Azonosito Szam (Wide)
  - Hungary PII: Hungarian Szemelyi Azonosito Szam (Default)
  - Hungary PII: Hungarian TAJ szam (Wide)
  - Hungary PII: Hungarian TAJ szam (Default)
  - Hungary PII: Hungarian Adoazonosito jel (Wide)
  - Hungary PII: Hungarian Adoazonosito jel (Default)

- Iceland Private Information for Discovery

  Policy for detection of Icelandic personally identifiable information. The rule for this policy is:

  - Iceland PII: Kennitala of Individuals

- India PII for Discovery

  Policy for detection of Indian personally identifiable information. The rules for this policy are:

  - India PII: Email Address and Password (Wide)
  - India PII: Email Address and Password (Default)
  - India PII: Form 16
  - India PII: PAN

- Indonesia PII for Discovery

  Policy for detection of Indonesian private information. The rules for this policy are:

  - Indonesia PII: Email Address and Password (Wide)
  - Indonesia PII: Email Address and Password (Default)
  - Indonesia PII: Single Identity Number (Wide)
  - Indonesia PII: Single Identity Number (Default)

- Ireland PII for Discovery

  Policy for detection of Irish personally identifiable information. The rules for this policy are:

  - Ireland PII: Email Address and Password (Wide)
  - Ireland PII: Email Address and Password (Default)
  - Ireland PII: Personal Public Service Number (PRSI/PPS) and Name
  - Ireland PII: Driver Number
  - Ireland PII: Passport Number

- Israel PII for Discovery

  Policy to identify files containing Israeli confidential and private information. The rules for this policy are:

  - Israel PII: CV and Resume in Hebrew
  - Israel PII: Email Address and Password (Wide)
  - Israel PII: Email Address and Password (Default)
  - Israel PII: Identity Number
  - Israel PII: Identity Number and General Medical Information
  - Israel PII: Identity Number and Sensitive Medical Information
  - Israel PII: Isracard Credit Card Number
  - Israel PII: Name and General Medical Information
  - Israel PII: Name and Sensitive Medical Information
  - Israel PII: Name and Identity Number
- Italy Private Information for Discovery

  Policy to detect private and sensitive information in Italy, including health information. The rules for this policy are:

  - Italy PII: Codice Fiscale
  - Italy PII: Name and Codice Fiscale
  - Italy PII: Name and health information
  - Italy PII: Codice Fiscale and health information
- Japan PII for Discovery

  Policy to detect private and sensitive information in Japan. The rules for this policy are:

  - Japan PII: Credit Cards Number
  - Japan PII: Corporate Number
  - Japan PII: Email Address and Password (Wide)
  - Japan PII: Email Address and Password (Default)
  - Japan PII: Individual Number
- Kazakhstan PII for Discovery

  Policy for detection of Kazakh private information. The rules for this policy are:

  - Kazakhstan PII: Taxpayer Registration Numbers (Wide)
  - Kazakhstan PII: Taxpayer Registration Numbers (Default)
  - Kazakhstan PII: Individual Identification Numbers (Wide)
  - Kazakhstan PII: Individual Identification Numbers (Default)
  - Kazakhstan PII: Business Identification Numbers (Wide)
  - Kazakhstan PII: Business Identification Numbers (Default)
- Latvia PII for Discovery

  Policy for detection of Latvian private information. The rules for this policy are:

  - Latvia PII: Personal Identity Number (Wide)

- Latvia PII: Personal Identity Number (Default)

- Lithuania PII for Discovery

  Policy for detection of Lithuanian private information. The rules for this policy are:

  - Lithuania PII: Personal Code (Wide)
  - Lithuania PII: Personal Code (Default)

- Luxembourg PII for Discovery

  Policy for detection of Luxembourgian private information. The rules for this policy are:

  - Luxembourg PII: National Identification Number - 11 Digits (Wide)
  - Luxembourg PII: National Identification Number - 11 Digits (Default)
  - Luxembourg PII: National Identification Number - 13 Digits (Wide)
  - Luxembourg PII: National Identification Number - 13 Digits (Default)

- Macau PII for Discovery

  Policy to detect files containing personally identifiable information for residents of Macau. The rules for this policy are:

  - Macau PII: Email Address and Password (Wide)
  - Macau PII: Email Address and Password (Default)
  - Macau PII: ID Number (Wide)
  - Macau PII: ID Number (Default)
  - Macau PII: ID Number (Narrow)

- Malaysia Private Information for Discovery

  Policy to detect files containing personally identifiable information for residents of Malaysia. The rule for this policy is:

  - Malaysia PII: Malaysia ID formal form with BP w proximity

- Malta PII for Discovery

  Policy for detection of Maltese private information. The rules for this policy are:

  - Malta PII: Identity Card Number (Wide)
  - Malta PII: Identity Card Number (Default)

- Mexico PII for Discovery

  Policy for detection of Mexican Personal Information. The rules for this policy are:

  - Mexico PII: Email Address and Password (Wide)
  - Mexico PII: Email Address and Password (Default)
  - Mexico PII: RFC Number
  - Mexico PII: CURP (Default)
  - Mexico PII: CURP (Narrow)
  - Mexico PII: CPISP (Default)
  - Mexico PII: CPISP (Narrow)

- Mexico PII: Passport Number (Wide)
- Mexico PII: Passport Number (Default)
- Mexico PII: Social Security Number (NSS) (Wide)
- Mexico PII: Social Security Number (NSS) (Default)
- Mexico PII: SSP Contratos Internos Detection

- Netherlands PII for Discovery

  Policy to detect private and sensitive information in Dutch, for Dutch-speaking countries. The rules for this policy are:

  - Netherlands PII: Citizen Service Number and Ethnicity
  - Netherlands PII: Citizen Service Number and Password (Wide)
  - Netherlands PII: Citizen Service Number and Password (Default)
  - Netherlands PII: Citizen Service Number and Password (Narrow)
  - Netherlands PII: Citizen Service Number and CCN
  - Netherlands PII: Citizen Service Number and Crime
  - Netherlands PII: Citizen Service Number and Disease
  - Netherlands PII: Driver License Number
  - Netherlands PII: Email Address and Password (Wide)
  - Netherlands PII: Email Address and Password (Default)
  - Netherlands PII: Passport Number
  - Netherlands PII: Bank Account Number (Wide)
  - Netherlands PII: Bank Account Number (Default)

- New Zealand PII for Discovery

  Policy to detect files containing personally identifiable information for residents of New Zealand. The rule for this policy is:

  - New Zealand PII: Email Address and Password (Wide)
  - New Zealand PII: Email Address and Password (Default)
  - New Zealand PII: NHI number

- Norway PII for Discovery

  Policy to detect private and sensitive information in Norway, including health information. The rules for this policy are:

  - Norway PII: Personal Number
  - Norway PII: Name and Personal Number
  - Norway PII: Name and Sensitive Disease
  - Norway PII: Personal Number and Sensitive Disease

- People’s Republic of China PII for Discovery

  Policy for detection of People's Republic of China private information. The rules for this policy are:

  - People’s Republic of China PII: CV and Resume in Chinese
  - People's Republic of China PII: Email Address and Password (Wide)

- People's Republic of China PII: Email Address and Password (Default)
- People’s Republic of China PII: Identification Number
- People's Republic of China PII: Passport Number (Default)
- People's Republic of China PII: Passport Number (Narrow)

- Peru PII for Discovery

  Policy for detection of Peruvian private information. The rules for this policy are:

  - Peru PII: Email Address and Password (Wide)
  - Peru PII: Email Address and Password (Default)
  - Peru PII: Unique Identification Code (CUI) (Wide)
  - Peru PII: Unique Identification Code (CUI) (Default)
  - Peru PII: Unique Identification Code (CUI) (Narrow)
  - Peru PII: Unique Taxpayer Registration Number (RUC) of Individuals (Wide)
  - Peru PII: Unique Taxpayer Registration Number (RUC) of Individuals (Default)
  - Peru PII: Unique Taxpayer Registration Number (RUC) of Non-Individuals (Wide)
  - Peru PII: Unique Taxpayer Registration Number (RUC) of Non-Individuals (Default)

- Philippines PII for Discovery

  Policy for detection of Philippines private information. The rules for this policy are:

  - Philippines PII: DNA Profile
  - Philippines PII: Name and Address (Wide)
  - Philippines PII: Name and Address (Default)
  - Philippines PII: Name and Address (Narrow)
  - Philippines PII: Name and CCN (Wide)
  - Philippines PII: Name and CCN (Default)
  - Philippines PII: Name and CCN (Narrow)
  - Philippines PII: Name and Common Medical Condition (Wide)
  - Philippines PII: Name and Common Medical Condition (Default)
  - Philippines PII: Name and Crime (Wide)
  - Philippines PII: Name and Crime (Default)
  - Philippines PII: Name and Date of Birth (Wide)
  - Philippines PII: Name and Date of Birth (Default)
  - Philippines PII: Name and Password (Wide)
  - Philippines PII: Name and Password (Default)
  - Philippines PII: Name and Password (Narrow)
  - Philippines PII: Name and PhilHealth Identification Number (Wide)

- Philippines PII: Name and PhilHealth Identification Number (Default)
- Philippines PII: Name and Physical Information (Wide)
- Philippines PII: Name and Physical Information (Default)
- Philippines PII: Name and Sensitive Disease or Drug (Wide)
- Philippines PII: Name and Sensitive Disease or Drug (Default)
- Philippines PII: Name and SSS Number (Wide)
- Philippines PII: Name and SSS Number (Default)
- Philippines PII: Name and TIN (Wide)
- Philippines PII: Name and TIN (Default)
- Philippines PII: PhilHealth Identification Number (Wide)
- Philippines PII: PhilHealth Identification Number (Default)
- Philippines PII: SSS Number (Wide)
- Philippines PII: SSS Number (Default)
- Philippines PII: TIN Number (Wide)
- Philippines PII: TIN Number (Default)

- Poland PII for Discovery

  Policy for detection of personal information for residents of Poland. The rules for this policy are:

  - Poland PII: IBAN and Name
  - Poland PII: NIP and Name
  - Poland PII: NIP with proximity
  - Poland PII: PESEL and Name
  - Poland PII: PESEL with proximity
  - Poland PII: Polish ID and Name
  - Poland PII: Polish ID with proximity
  - Poland PII: REGON and Name
  - Poland PII: REGON with proximity

- Portugal PII for Discovery

  Policy for detection of Portuguese private information. The rules for this policy are:

  - Portugal PII: Document Number (Wide)
  - Portugal PII: Document Number (Default)
  - Portugal PII: Email Address and Password (Wide)
  - Portugal PII: Email Address and Password (Default)
  - Portugal PII: Social Security Number (Wide)
  - Portugal PII: Social Security Number (Default)
  - Portugal PII: Tax Identification Number of Individuals (Wide)
  - Portugal PII: Tax Identification Number of Individuals (Default)

- Romania PII for Discovery

  Policy for detection of Romanian private information. The rule for this policy is:

  - Romania PII: Personal numeric code
- Russia PII for Discovery

  Policy for detection of Russian personally identifiable information. The rules for this policy are:

  - Russia PII: Email Address and Password (Wide)
  - Russia PII: Email Address and Password (Default)
  - Russia PII: Passport Number
  - Russia PII: Passport Number and Name
- Singapore PII for Discovery

  Policy to detect files containing personally identifiable information for residents of Singapore. The rules for this policy are:

  - Singapore PII: Email Address and Password (Wide)
  - Singapore PII: Email Address and Password (Default)
  - Singapore PII: Identification Numbers
- Slovakia Private Information for Discovery

  Policy for detection of Slovak private information. The rules for this policy are:

  - Slovakia PII: Email Address and Password (Wide)
  - Slovakia PII: Email Address and Password (Default)
  - Slovakia PII: Rodne Cislo (Wide)
  - Slovakia PII: Rodne Cislo (Default)
- Slovenia PII for Discovery

  Policy for detection of Unique Master Citizen Numbers. The rules for this policy are:

  - Slovenia PII: Unique Master Citizen Number (Wide)
  - Slovenia PII: Unique Master Citizen Number (Default)
- Social Security Numbers Private Information for Discovery

  Policy for detection of validated social security numbers policy. The rules for this policy are:

  - US SSN - Wide
  - US SSN - Default
  - US SSN - Narrow
  - US SSN - not masked
- South Africa PII for Discovery

  Policy for detection of personal information of South African citizens. The rules for this policy are:

  - South Africa PII: Email Address and Password (Wide)
  - South Africa PII: Email Address and Password (Default)

- South Africa PII: ID Number (Wide)
- South Africa PII: ID Number (Default)

- South Korea PII for Discovery

  Policy to detect files containing personally identifiable information for residents of South Korea. The rules for this policy are:

  - South Korea PII: Email Address and Password (Wide)
  - South Korea PII: Email Address and Password (Default)
  - South Korea PII: ID Number
  - South Korea PII: Phone Number

- Spain PII for Discovery

  Policy for private and sensitive information in Spanish. The policy contains rules to detect combinations of Spain National Identity Document and sensitive private information like account number, ethnicity and health conditions. The rules for this policy are:

  - Spain PII: DNI, Account and Password
  - Spain PII: DNI and Credit Card Number
  - Spain PII: DNI and Crime
  - Spain PII: DNI and Diseases
  - Spain PII: DNI and Ethnicity
  - Spain PII: DNI Number
  - Spain PII: Email Address and Password (Wide)
  - Spain PII: Email Address and Password (Default)
  - Spain PII: Name and Address (Default)
  - Spain PII: Name and Address (Narrow)
  - Spain PII: Name and Credit Card Number
  - Spain PII: Name and DNI
  - Spain PII: Name and IBAN
  - Spain PII: Name and Passport Number
  - Spain PII: Name and Email Address
  - Spain PII: Name and Phone Number
  - Spain PII: Name and Social Security Number (Wide)
  - Spain PII: Name and Social Security Number (Default)
  - Spain PII: Social Security Number (Wide)
  - Spain PII: Social Security Number (Default)

- Sweden PII for Discovery

  Policy for detection of Swedish personally identifiable information. The rules for this policy are:

  - Sweden PII: Email Address and Password (Wide)
  - Sweden PII: Email Address and Password (Default)

- Sweden PII: ID Number

- Switzerland PII for Discovery

  Policy for detection of Swiss personally identifiable information. The rules for this policy are:

  - Switzerland PII: Email Address and Password (Wide)
  - Switzerland PII: Email Address and Password (Default)
  - Switzerland PII: New Format AHV Number

- Taiwan PII for Discovery

  Policy to detect files containing personally identifiable information for residents of Taiwan. The rules for this policy are:

  - Taiwan PII: Email Address and Password (Wide)
  - Taiwan PII: Email Address and Password (Default)
  - Taiwan PII: ID Card Number (Wide)
  - Taiwan PII: ID Card Number (Default)

- Thailand PII for Discovery

  Policy for detection of Thai personally identifiable information. The rule for this policy is:

  - Thailand PII: Email Address and Password (Wide)
  - Thailand PII: Email Address and Password (Default)
  - Thailand: National ID Number

- Turkey PII for Discovery

  Policy for detection of personal information of Turkish citizens. The rules for this policy are:

  - Turkey PII: Email Address and Password (Wide)
  - Turkey PII: Email Address and Password (Default)
  - Turkey PII: TC Kimlik
  - Turkey PII: PII Spreadsheets

- UK PII for Discovery

  Policy for detection of personal information of UK citizens. The rules for this policy are:

  - UK PII: Bank Account Number
  - UK PII: Bank Account Number and Sort Code
  - UK PII: Credit File (Wide)
  - UK PII: Credit File (Default)
  - UK PII: Credit File (Narrow)
  - UK PII: Driver Number
  - UK PII: Email Address and Password (Wide)
  - UK PII: Email Address and Password (Default)
  - UK PII: National Insurance Number

- UK PII: Passport Number
- UK PII: Postal Code
- UK PII: Sort Code
- UK PII: Tax ID Number

- US PII for Discovery

  Policy to detect personally identifiable information (PII) for residents of the United States. The rules for this policy are:

  - US PII: Credit card Number and Social Security Number
  - US PII: Credit File (Wide)
  - US PII: Credit File (Default)
  - US PII: Credit File (Narrow)
  - US PII: Email Address and Password (Wide)
  - US PII: Email Address and Password (Default)
  - US PII: Name and Address (Wide)
  - US PII: Name and Address (Default)
  - US PII: Name and Driver License Number
  - US PII: Name and Passport Number (Wide)
  - US PII: Name and Passport Number (Default)
  - US PII: Name and Passport Number (Narrow)
  - US PII: Name and Social Security Number
  - US PII: Passport Number (Wide)
  - US PII: Passport Number (Default)
  - US PII: Name and ITIN
  - US PII: Social Security Number

- Vietnam PII for Discovery

  Policy for detection of Vietnamese private information. The rules for this policy are:

  - Vietnam PII: CMND Number (Wide)
  - Vietnam PII: CMND Number (Default)
  - Vietnam PII: Email Address and Password (Wide)
  - Vietnam PII: Email Address and Password (Default)

Regulations

- FERC and NERC for Discovery

  Policy to promote compliance with the requirements imposed by the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Council (NERC) to protects Critical Energy Infrastructure Information (CEII). The policy detects sensitive Energy Infrastructure Information, such as

natural gas pipeline flow diagrams, various drawing and schemes files and FERC forms 567 and 715. The rules for this policy are:

- FERC and NERC: disclaimer
- FERC and NERC: pipeline flow diagrams
- FERC and NERC: form 567
- FERC and NERC: form 715

- SEC and SOX for Discovery

  The Sarbanes-Oxley Act (SOX) mandates public companies to comply with its requirements. This act provides strict guidelines for ensuring corporate governance and control policies for information within publicly traded companies. This policy promotes compliance with the data protection aspects of SOX by detecting audit terms and SEC 10-K and 10-Q reports. The rules for this policy are:

  - SOX: Form 10-K (Standard Fiscal Year)
  - SOX: Form 10-Q (Standard Fiscal Year)
  - SOX: SOX-Related Term

- Swedish Patient Data Act (SFS 2008:355, Patientdatalagen) - For Discovery

  A policy to promote compliance with the Swedish Patient Data Act (Patientdatalag , SFS 2008:355) that mandates protection of protected health information (PHI) and Personally Identifiable Information (PII) of Swedish citizens and residents . The policy comprises rules for discovery of health information or medical conditions (in Swedish or English), in proximity to personally identifiable information such as personnummer or name, and for detection of SPSS files and Database files. The rules for this policy are:

  - SFS 2008:355: Database File
  - SFS 2008:355: DICOM
  - SFS 2008:355: DNA Profile
  - SFS 2008:355: ICD10 Code
  - SFS 2008:355: ICD10 Code and Description
  - SFS 2008:355: ICD10 Code and Name (Wide)
  - SFS 2008:355: ICD10 Code and Name (Default)
  - SFS 2008:355: ICD10 Code and Name (Narrow)
  - SFS 2008:355: ICD10 Code and Personal Number
  - SFS 2008:355: ICD10 Description
  - SFS 2008:355: Name and Health Information
  - SFS 2008:355: Name and Personal Number
  - SFS 2008:355: Name and Sensitive Disease or Drug
  - SFS 2008:355: Personal Number
  - SFS 2008:355: Personal Number and Health Information
  - SFS 2008:355: Personal Number and Sensitive Disease or Drug
  - SFS 2008:355: SPSS Text File

- US-ITAR for Discovery

  International Traffic in Arms Regulations (ITAR) is a set of United States government regulations that control the export and import of defense-related articles and services. The policy detects information about sensitive technologies being disseminated, as well as source code and confidential documents. For source code in the SPICE and VHDL languages, please select all relevant rules to achieve complete coverage. The rules for this policy are:

  - ITAR: Encryption
  - ITAR: Nuclear
  - ITAR: Space
  - ITAR: Military
  - ITAR: Technical Drawing files

Suspicious User Activity

- Database Files for Discovery

  Policy for the detection of database files. The rules for this policy are:

  - Database File: Ability Office format
  - Database File: Borland Reflex 2
  - Database File: dBase format
  - Database File: Filemaker format
  - Database File: Lotus Notes NSF format
  - Database File: MORE format
  - Database File: Microsoft Access format
  - Database File: Microsoft Exchange Server format
  - Database File: Microsoft Works for DOS format
  - Database File: Microsoft Works for Mac format
  - Database File: Microsoft Works for Windows format
  - Database File: Paradox format
  - Database File: SmartWare II format

- Deep Web URLs for Discovery

  Policy for detecting deep web URLs that appear in analyzed content such as textual documents or email messages and end with the pseudo-top-level domains .onion and .i2p. The deep web is a portion of World Wide Web content that is not indexed by standard search engines and that is intentionally hidden from the regular Internet, accessible only with special software, such as Tor. Such URLs are used for anonymous defamation, unauthorized leaks of sensitive information and copyright infringement, distribution of illegal sexual content, selling controlled substances, money laundering, bank fraud, credit card fraud and identity theft, among other things. The rules for this policy are:

- Deep Web URLs: .i2p (Wide)
- Deep Web URLs: .i2p (Default)
- Deep Web URLs: .onion

File-type classifiers

This section contains the full list of file-type classifiers provided by Forcepoint. You can also create new classifiers. For information, see Adding a file-type classifier.

Classifier	Description
7-Zip File	Detection of 7zip files according to internal properties.
Abaqus ODB Format	Detection of Abaqus ODB files.
Ability Database File	Detection of Ability Office Database file format according to internal file properties.
AutoCAD DFX Binary File	Detection of Autodesk DXF binary file format according to internal file properties.
AutoCAD DFX Text File	Detection of Autodesk DXF textual file format according to internal file properties.
Autodesk Design Web Format	Detection of Autodesk Design Web (DWF) files.
Autodesk DWG File	Detection of Autodesk DWG CAD file format according to internal file properties.
Autodesk Maya Binary Format	Detection of Autodesk Maya binary (MB) files.
Autodesk Maya Textual Format	Detection of Autodesk Maya textual (MA) files.
Autodesk WHIP File	Detection of Autodesk Whip file format according to internal file properties.
Base64 file	Detection of files in Base64 format according to internal file properties.
Borland Reflex 2 File	Detection of the Borland Reflex 2 database file format according to internal file properties.
CATIA File	Detection of CATIA file format according to internal file properties.
CDXA/MPEG-PS files	Detection of video files in the CDXA/MPEG-PS format.
Corel Draw File	Detection of CorelDRAW file format according to internal file properties.
dBase File	Detection of dBase database file format according to internal file properties.

Classifier	Description
DICOM	Detection of Digital Imaging and Communications in Medicine (DICOM) medical imaging files.
Digitally Signed PDF File (Native)	Detection of PDF files containing digital signatures created by using Adobe Acrobat.
Encrypted 7-Zip File	Detection of encrypted 7zip files according to internal properties.
Encrypted Access Database File (Legacy)	Detection of password protected Microsoft Access Database files (.mdb) that were created before Office 2007 according to internal file properties.
Solid Works File	Detection of SolidWorks files.
Encrypted B1 File	Detection of encrypted B1 files according to internal file properties.
Encrypted Files of Known Formats	Detection of encrypted PGP files or password-protected Nero files, archive files (ZIP, RAR, RAR5, B1, and 7-Zip), or office suite files (PDF; Microsoft Access, Excel, OneNote, PowerPoint, and Word).
Encrypted PDF File	Detection of encrypted PDF documents according to internal file properties.
Encrypted PowerPoint Binary File (Legacy)	Detection of password protected Microsoft PowerPoint Binary files (.ppt) that were created before Office 2007 according to internal file properties.
Encrypted RAR File	Detection of encrypted RAR archives according to internal file properties.
Encrypted RAR5 File	Detection of encrypted RAR5 files according to internal file properties.
Encrypted Word Binary File (Legacy)	Detection of password protected Microsoft Word Binary files (.doc) that were created before Office 2007 according to internal file properties.
Encrypted ZIP File	Detection of encrypted ZIP archives according to internal file properties.
FileMaker File	Detection of Filemaker database files for Macintosh according to internal file properties.
Incomplete ZIP	Detection of non-encrypted ZIP files that can't be opened by the system.
Java Class Files	Detection of .class files that can be executed on the Java Virtual Machine (JVM).
Jupiter Tesselation (JT) File	Detection of Jupiter Tesselation (JT) files.
Link Library Format	Detection of Link Libraries files (.dll).
Lotus Notes NSF File	Detection of IBM Lotus Notes database NSF/NTF files according to internal file properties.
MATLAB Figures and Binary Files	Detection of matrix laboratory .fig and binary files.

Classifier	Description
Microsoft Access File - All Versions	Detection of Microsoft Access database files (all versions) according to internal file properties.
Microsoft Encrypted OneNote File	Detection of password-protected Microsoft OneNote files.
Microsoft Excel File	Detection of Microsoft Excel files (all versions) that are not protected by Windows Rights Management Services (RMS) according to internal file properties.
Microsoft Exchange Server Database Files	Detection of Microsoft Exchange Server database file format according to internal file properties.
Microsoft Office Excel 2003 XML Files (Legacy)	Detection of Microsoft Office Excel 2003 XML files that were created before Office 2007 according to internal file properties.
Microsoft Office Encrypted Files (OOXML)	Detection of password protected Office Open XML files according to internal file properties. Open XML files include Word, Excel, PowerPoint and other Office documents created in Office 2007 or later.
Microsoft Office File	Detection of Office Open XML files that are not protected by Windows Rights Management Services (RMS) according to internal file properties. Open XML files include Word, Excel, PowerPoint and other Office documents created in Office 2007 or later.
Microsoft Office File - All Versions	Detection of Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Access, Microsoft Project and Microsoft Visio files (all versions) according to internal file properties.
Microsoft Office Files - Non-RMS-Protected	Detection of Microsoft Office documents that are not protected by Windows Rights Management Services (RMS). Office documents include Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Access, Microsoft Project and Microsoft Visio. Detection is based on internal file properties.
Microsoft Office Word 2003 XML Files (Legacy)	Detection of Microsoft Office Word 2003 XML files that were created before Office 2007 according to internal file properties.
Microsoft Outlook 2011 for Mac Files	Detection of Microsoft Outlook 2011 for Mac files.
Microsoft PowerPoint Binary File (Legacy)	Detection of PowerPoint Binary files that are not protected by Windows Rights Management Services (RMS) according to internal file properties.
Microsoft PowerPoint File	Detection of Microsoft PowerPoint files (all versions) that are not protected by Windows Rights Management Services (RMS) according to internal file properties.
Microsoft Program Database File	Detection of Microsoft Program database files.
Microsoft Project File - All Versions	Detection of Microsoft Project files (all versions) according to internal file properties.

Classifier	Description
Microsoft Tape Format	Detection of Microsoft Tape Format (MTF) backup files used by the backup utilities included in Microsoft SQL Server, and by other Microsoft Windows software, such as NTBackup and Backup Exec.
Microsoft Visio File	Detection of Microsoft Visio files (all versions) according to internal file properties.
Microsoft Word File	Detection of Microsoft Word files (all versions) that are not protected by Windows Rights Management Services (RMS) according to internal file properties.
MORE Database File	Detection of MORE database files for Macintosh according to internal file properties.
Microsoft Works Database File (for DOS)	Detection of Microsoft Works database files for DOS according to internal file properties.
Microsoft Works Database File (for Macintosh)	Detection of Microsoft Works database files for Macintosh according to internal file properties.
Microsoft Works Database File (for Windows)	Detection of Microsoft Works database files for Windows according to internal file properties.
MySQL Table Definition File	Detection of MySQL table definition files.
Nastran OP2 format	Detection of Nastran OP2 files.
Nero Encrypted File	Detection of encrypted nero files according to internal properties.
NIEM-Conformant XML	Detection of NIEM-Conformant XML files, part of the ANSI/ NIST-ITL standard “Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information.” XML formats based on the ANSI/NIST-ITL standard, such as FBI EBTS XML files, are also detected.
OASIS XML Common Biometric Format (XCBF)	Detection of OASIS XML Common Biometric Format (XCBF) files, which are based on the binary biometric file format CBEFF.
Outlook Restricted-Permission Message	Detection of Outlook Restricted-Permission Message (RPMSG) files
Paradox Database File	Detection of Paradox database files according to internal file properties.
PGP Encrypted File	Detection of encrypted PGP file format according to internal file properties.
PGP Signed and Encrypted File	Detection of signed and encrypted PGP file format according to internal file properties.
PKCS #12 Files	Detection of PKCS #12 files (.p12, .pfx)
Portable Document Format (PDF) - All Versions	Detection of PDF files according to internal properties.
PTC Creo ASM Format	Detection of PTC Creo ASM files.

Classifier	Description
PTC Creo DRW Format	Detection of PTC Creo DRW files.
PTC Creo FRM Format	Detection of PTC Creo FRM files.
PTC Creo PRT Format	Detection of PTC Creo PRT files.
Raster Graphics Formats	Detection of raster graphics formats. For example: Microsoft Windows Bitmap Image (BMP), Graphics Interchange Format (GIF), Tagged Image File (TIF), and JPEG Interchange Format.
RMS-Protected Microsoft Office Files	Detection of Outlook Restricted-Permission Message (RPMSG) files and Microsoft Office files that are protected by Windows Rights Management Services (RMS). Microsoft Office files include Word, Excel, PowerPoint and other Office documents.
SAS7BDAT Database Storage File	Detection of SAS7BDAT database storage files.
Siemens NX PRT Format	Detection of Siemens NX PRT files.
SmartWare II Database File	Detection of SmartWare II database files according to internal file properties.
Solid Works File	Detection of SolidWorks files.
Splunk Enterprise Security Event Log File	Detection of Splunk Enterprise Security Event log files.
SQLite Database File	Detection of SQLite database files.
STL Binary Format	Detection of 3D Systems STL binary CAD files.
STP Format	Detection of ISO 10303-21 STEP files.
Tagged Image File Format (TIFF) File	Detection of TIFF (Tagged Image File Format) files according to internal properties.
Unencrypted Portable Document Format (PDF)	Detection of unencrypted PDF files according to internal properties.
Unknown Format	Detects files of an unknown format, i.e., those that are not supported.
Various Archive Formats	Detection of BinHex, GZIP, Legato EMailXtender Archive, Microsoft CAB, ZIP archive format, RAR format, UNIX TAR encapsulation.
Various Computer Aided Design Formats	Detection of AutoCAD DXF graphics, AutoCAD Drawing, CATIA formats, Microsoft Visio, MicroStation.
Various Database Files	Detection of Microsoft Access and Microsoft Project.
Various Executables Formats	Detection of Windows Executable files and Link Libraries.

Classifier	Description
Various Graphics Formats	Detection of Computer Graphics Metafile, CorelDRAW, DCX Fax System, Encapsulated PostScript, Enhanced Metafile, GIF, JPEG, Lotus AMIDraw Graphics, Lotus Pic, MacPaint, Microsoft Office Drawing, PC PaintBrush, Portable Network Graphics, SGI RGB Image, Sun Raster Image, Tagged Image File, Truevision Targa, Windows Animated Cursor, Windows Bitmap, Windows Icon Cursor, Windows Metafile, Word Perfect Graphics.
Various Mail Formats	Detection of Domino XML, Legato Extender, Lotus Notes DB, Microsoft Outlook, Microsoft Outlook Express, Microsoft Outlook Personal Folder, Text Mail (MIME), Transport Neutral Encapsulation Format.
Various Multimedia Formats	Detection of Advanced Streaming Format (ASF), Audio Interchage File Format (AIFF), Microsoft Wave Sound (WAV), MIDI, MP3, Mpeg-1 Video, Mpeg-2 Audio, NeXT/Sun Audio, Quick Time Movie, Windows Video (AVI).
Various Presentation Formats	Detection of Microsoft PowerPoint, Apple iWork Keynote (Legacy), Corel Presentations, Lotus Freelance Graphics 2, Macromedia Flash, Applix Graphics and Star Office Impress files that are not protected by Windows Rights Management Services (RMS).
Various Project Planning Formats	Detection of Microsoft Project Files.
Various Spreadsheet Formats	Detection of Microsoft Excel, Apple iWork Numbers (Legacy), Applix Spreadsheets, Comma Separated Values (CSV), Data Interchange Format, Lotus 1-2-3, Microsoft Works Spreadsheet and Star Office Spreadsheet files that are not protected by Windows Rights Management Services (RMS).
Various Text and Markup Formats	Detection of ASCII, HTML, Microsoft Excel Windows XML, Microsoft Word Windows XML, Microsoft Visio XML, MIME HTML, Rich Text Format (RTF), Unicode Text, XHTML, XML.
Various Word Processing Formats	Detection of Microsoft Word, Adobe FrameMaker Interchange, Apple iWork Pages (Legacy), Applix Words, Corel WordPerfect, Display Write, Folio Flat File, Founder Chinese E-Paper Basic, Oasys, Haansoft Hangul, IBM DCA/RFT, Just Systems Ichitaro, Lotus AMI, Lotus Word, Microsoft Works, Star Office Writer, WordPad, XML Paper Specification, XyWrite and Yahoo Instant Messenger files that are not protected by Windows Rights Management Services (RMS).
Vector Graphics Formats	Detection of vector graphics formats. For example: Simple Vector Format (SVF) and Microsoft Office Drawing (MSO).
Web Archive Files	Detection of WEBARCHIVE files containing HTML, images, sound, and video from web pages previously visited.
Windows Event Viewer log files (Windows 2000 and XP)	Detection of Windows event logs in Windows 2000 and Windows XP Event Viewer format.
Windows Event Viewer log files (Windows Vista 7 and 8)	Detection of Windows event logs in Windows Vista, Windows 7, and Windows 8 format.

Classifier	Description
XML Format	Detection of XML files according to internal file properties.
ZIP File	Detection of all unencrypted ZIP files

Script classifiers

This section contains the full list of predefined script classifiers. Edit the classifiers as needed. For information, see Editing a predefined script.

Classifier	Description
.htpasswd file that uses bcrypt, MD5, or SHA-1 hash function (Default).	Detection of .htpasswd file that use the bcrypt, MD5, SHA-1, or salted SHA-1 hash functions. All lines in the file should be valid hash lines. Characters statistical analysis is used in order to prevent unintended matches. An example for a bcrypt line is “admin:$2y$14$mhtB34wX83QuzRhTu.4fqu.75XpELvXXaC.bCbYzbugMw2H/RyTcu”.
.htpasswd file that uses bcrypt, MD5, or SHA-1 hash function (Narrow)	Detection of .htpasswd file that use the bcrypt, MD5, SHA-1, or salted SHA-1 hash functions. All lines in the file should be valid hash lines. At least 4 lines are needed in order to have a match. Characters statistical analysis is used in order to prevent unintended matches. An example for a bcrypt line is “admin:$2y$14$mhtB34wX83QuzRhTu.4fqu.75XpELvXXaC.bCbYzbugMw2H/RyTcu”.
.htpasswd file that uses bcrypt, MD5, or SHA-1 hash function (Wide)	Detection of .htpasswd file that use the bcrypt, MD5, SHA-1, or salted SHA-1 hash functions (e.g., “admin:$2y$14$mhtB34wX83QuzRhTu.4fqu.75XpELvXXaC.bCbYzbugMw2H/RyTcu”).
.htpasswd file that uses the crypt hash function (Default)	Detection of .htpasswd file that use the crypt hash function. All lines in the file should be valid hash lines. At least 4 lines are needed in order to have a match. Characters statistical analysis is used in order to prevent unintended matches. An example for a crypt line is “admin:uBbBQTqv1Kx9M”.
.htpasswd file that uses the crypt hash function (Narrow)	Detection of .htpasswd file that use the bcrypt, MD5, SHA-1 or salted SHA-1 hash functions. All lines in the file should be valid hash lines. At least 8 lines are needed in order to have a match. Characters statistical analysis is used in order to prevent unintended matches. An example for a crypt line is “admin:uBbBQTqv1Kx9M”.
.htpasswd file that uses the crypt hash function (Wide)	Detection of .htpasswd file that use the crypt hash function. At least 3 lines are needed in order to have a match. An example for a crypt line is “admin:uBbBQTqv1Kx9M”.
1st Magnetic Track	Detection of the string encoded on the 1st magnetic track of a credit card, containing the card number, and personal information of the card holder.

Classifier	Description
1st Magnetic Track (Chinese cards)	Detection of the string encoded on the 1st magnetic track of a Chinese credit card, containing the card number, and personal information of the card holder.
2nd Magnetic Track	Detection of the string encoded on the 2nd magnetic track of a credit card, containing the CCN, PIN, expiration date, and other card issuer data.
2nd Magnetic Track (Chinese cards)	Detection of the string encoded on the 2nd magnetic track of a chinese credit card, containing the CCN, PIN, expiration date, and other card issuer data.
3rd Magnetic Track	Detection of the string encoded on the 3rd magnetic track of a credit card, containing the CCN, PIN, and other card issuer data.
3rd Magnetic Track (Chinese cards)	Detection of the string encoded on the 3rd magnetic track of a Chinese credit card, containing the CCN, PIN, and other card issuer data.
9-Digit Slovak and Czech Birth Numbers	Detects valid 9-digit delimited or un-delimited Slovak and Czech birth numbers (Rodne Cislo). At least half of all 9-digit numbers need to be valid. For example “450819001”.
10-Digit Slovak and Czech Birth Numbers	Detects valid 10-digit delimited or un-delimited Slovak and Czech birth numbers (Rodne Cislo). At least half of all 10-digit numbers need to be valid. For example “8501306605”.
Aadhaar Number	Detection of Aadhaar 12 digit individual identification numbers.
ActionScript source code	Detection of source code content written in ActionScript, employing context-sensitive lexical analysis, patterns, and structures.
Australian Address	Detects Australian addresses. Uses several address formats such as number followed by a word and then a term that relates to a street (e.g., St., Rd., Ave.) For example: 12 Brigadoon St.
Australian Business Number (Default)	Detects Australian Business Numbers (ABN). Looks for 11-digit numbers that follow the ABN rules. If more than 3 valid ABNs are found, the classifier determines the percentage of valid ABNs to 11-digit numbers. If fewer than 4 valid ABNs are found, the classifier looks for ABN-related terms, such as ‘ABN’ or ‘Australian Business Number’, in proximity to the numbers found. For example: ABN: 12345678900
Australian Business Number (Wide)	Detects Australian Business Numbers (ABNs). Looks for 11-digit numbers that follow the ABN rules. For example: 12345678900. If one or more ABNs are found, the rule is triggered.

Classifier	Description
Australian Names (Default)	Detects full Australian names. Uses first-name and last-name dictionaries as well as internal dictionaries to identify valid full names. Weights case (John Smith vs. john smith) and honorifics (Dr., Mr., Mrs.). Uses a moderate threshold to signify a match. For example, using the default classifier, 'John Smith', 'john Smith', and 'dr. john smith' trigger the rule, but 'john smith' does not. Use the 'Default' classifier to balance between false positives and false negatives.
Australian Names (Narrow)	Detects full Australian names. Uses first-name and last-name dictionaries as well as internal dictionaries to identify valid full names. Weights case (John Smith vs. john smith) and honorifics (Dr., Mr., Mrs.). Uses a high threshold to signify a match. For example, using the narrow classifier, only 'John Smith' triggers the rule. 'john Smith', 'dr. john smith', and 'john smith' do not. Use the 'Narrow' classifier to reduce the false positives.
Australian Names (Wide)	Detects full Australian names. Uses first-name and last-name dictionaries as well as internal dictionaries to identify valid full names. Weights case (John Smith vs. john smith) and honorifics (Dr., Mr., Mrs.). Uses a low threshold to signify a match. For example, using the wide classifier, all permutations of 'John Smith' trigger the rule, including 'john Smith', 'dr. john smith', and 'john smith'. Use the 'Wide' classifier to reduce the false negatives.
Australian Tax File Number (Default)	Detects valid nine-digit Australian Tax File Numbers (TFN). At least 40% of the nine-digit numbers in the text must be valid; for example, "565051611".
Australian Tax File Number (Wide)	Detects valid nine-digit Australian Tax File Numbers (TFN); for example, "565051611".
Australian Tax File Number Near Term	Detects valid nine-digit Australian Tax File Numbers (TFN) near a support term; for example, "TFN: 565051611".
Austrian Social Security Number (Wide)	Detects valid 10-digit Austrian social security numbers (Sozialversicherungsnummern). For example: "1237 010180".
Austrian Social Security Number (Default)	Detects valid 10-digit Austrian social security numbers (Sozialversicherungsnummern). At least 30% of the 10-digit numbers in the text must be valid. For example: "1237 010180".
Austrian Social Security Number Near Term	Detects valid 10-digit Austrian social security numbers (Sozialversicherungsnummern) near a support term in English or German. For example: "Sozialversicherungsnummer 1237010180".
Belgium: ID Card Number	Detection of validated Belgium ID Card numbers
Brazil: RG Numbers (Default)	Detection of RG (Registro Geral) numbers.
Brazil: RG Numbers (Narrow)	Detection of RG (Registro Geral) numbers when appearing with support terms.

Classifier	Description
Brazilian CPF Number	Detection of validated Brazil CPF numbers.
Brazilian Name	Detection of Brazilian full names.
Bulgarian Unified Civil Number (Wide)	Detects valid 10-digit Bulgarian unified civil numbers. For example: “6909088552”.
Bulgarian Unified Civil Number (Default)	Detects valid 10-digit Bulgarian unified civil numbers. At least 50% of the 10-digit numbers in the text must be valid. For example: “6909088552”.
Bulgarian Unified Civil Number Near Term	Detects valid 10-digit Bulgarian unified civil numbers near a support term in Bulgarian or English. For example: “Unified Civil Number 6909088552”.
CAD x_t text format	Detection of CAD x_t text files
Canadian Names (Default)	Detection of Canadian full names.
Canadian Names (Wide)	Detection of Canadian full names.
CCN - for printer agent	Detection of valid credit card numbers, employing context sensitive lexical analysis and statistical analysis of patterns, taking into account possible errors that may be induced by the OCR software.
CDR	Detection of Call Detail Records with information like source phone number, destination phone number, call date, duration, etc.
CDR: headers	Detection of Call Detail Records by looking for column headers related to information such as source phone number, destination phone number, call date, duration, etc.
Chilean National Identity Number (RUN/RUT) (Wide)	Detects valid case-insensitive 9-character Chilean National Identity Numbers (RUN) and Tax Identification Numbers (RUT) that consist of 8 digits followed by a digit or the letter "K". For example: "15414638-5".
Chilean National Identity Number (RUN/RUT) (Default)	Detects valid case-sensitive 9-character Chilean National Identity Numbers (RUN) and Tax Identification Numbers (RUT) that consist of 8 digits followed by a digit or the letter "K". At least 30% of the similar 9-character numbers in the text must be valid. For example: "15414638-5".
Chilean National Identity Number (RUN/RUT) Near Term	Detects valid 9-character Chilean National Identity Numbers (RUN) and Tax Identification Numbers (RUT) that consist of 8 digits followed by a digit or the letter "K", near a support term in Spanish or English. For example: "Rol Unico Nacional 15414638-5".
Chinese Credit Cards (Default)	Detection of credit card numbers used in the People's Republic of China employing various heuristics involving credit card-related terms and use of delimiters. By default, only the first 4 digits and the last 4 digits are shown in the reports.
Chinese Credit Cards (Narrow)	Detection of credit card numbers used in the People's Republic of China. Requires additional evidence, such as credit card related terms in proximity, in order to qualify number as a credit card number. By default, only the first 4 digits and the last 4 digits are shown in the reports.

Classifier	Description
Chinese Credit Cards (Wide)	Detection of potential credit card numbers used in the People's Republic of China, based only on format and validation. This classifier may cause false-positives. By default, only the first 4 digits and the last 4 digits are shown in the reports.
Chinese Surnames	Detection of common Hong Kong surnames.
Colombian ID Number Near Term (Default)	Detects 7- or 8-digit Citizenship Card ID Numbers (Cedula de Ciudadania) or 10-digit Unique Personal Identification Number (NUIP) near a support term in Spanish or English. For example: "Cedula: 1129572839".
Colombian ID Number Near Term (Wide)	Detects 7- or 8-digit Citizenship Card ID Numbers (Cedula de Ciudadania) or 10-digit Unique Personal Identification Number (NUIP) near a support term in Spanish or English. Possible short support terms include "CC" and "ID". For example: "CC: 1129572839".
Confidential Header/ Footer with Expiration Date	Detection of documents with confidential data in the header or footer that includes an American-formatted date (MM-DD-YYYY).
Contract Reference of Secretaria de Seguridad Publica (SSP)	Detection of Contract Nomenclature of Secretaria de Seguridad Publica (SSP).
Costa Rican ID Number Near Term (Default)	Detects of 9-digit Identification Numbers (Numero de Cedula Identidad) that may be preceded by the digit "0", near a permissive support term in Spanish or English. For example: "Cedula: 9-0071-5946".
Costa Rican ID Number Near Term (Narrow)	Detects of 9-digit Identification Numbers (Numero de Cedula Identidad) that may be preceded by the digit "0", near a support term in Spanish or English. For example: "Cedula de Identidad: 9-0071-5946".
Costa Rican Legal ID Number Near Term (Default)	Detects of 10- or 12-digit Legal Identification Numbers (Numero de Cedula Juridica) that may be preceded by the digit "0", near a permissive support term in Spanish or English. For example: "Cedula: 3 101 981567".
Costa Rican Legal ID Number Near Term (Narrow)	Detects of 10- or 12-digit Legal Identification Numbers (Numero de Cedula Juridica) that may be preceded by the digit "0", near a support term in Spanish or English. For example: "Cedula Juridica: 3-101-981567".
Count attachments	Used to count the number of attachments and/or recipients.
Credit Card Magnetic Tracks	Detection of the strings encoded on 1st. 2nd and 3rd magnetic tracks of a credit card.
Credit Cards - Wide Minus Default	Detection of potential credit card numbers, based only on format and validation, may cause false-positives. Detects all CCNs that belong to ‘wide’ sensitivity and not to ‘default’. By default, only the first 4 digits and the last 4 digits are shown in the reports.
Credit Cards (Default)	Detection of credit card numbers employing various heuristics involving credit card related terms and use of delimiters. By default, only the first 4 digits and the last 4 digits are shown in the reports.

Classifier	Description
Credit Cards (Extra-Wide)	Detection of potential credit-card-numbers, based only on format and validation.
Credit Cards (Narrow)	Detection of credit card numbers. Requires additional evidence, such as credit card related terms in proximity, in order to qualify number as a credit card number. By default, only the first 4 digits and the last 4 digits are shown in the reports.
Credit Cards (Wide)	Detection of potential credit card numbers, based only on format and validation, may cause false-positives. By default, only the first 4 digits and the last 4 digits are shown in the reports.
Credit Cards Pattern	Detection of potential credit card number patterns based only on format (without validation).
Credit Cards: American Express	Detection of valid American Express credit card numbers employing various heuristics involving credit card related terms and use of delimiters.
Credit Cards: Bankcard	Detection of valid Bankcard credit card numbers employing various heuristics involving credit card related terms and use of delimiters.
Credit Cards: Diners	Detection of valid Diners credit card numbers employing various heuristics involving credit card related terms and use of delimiters.
Credit Cards: Discover	Detection of valid Discover credit card numbers employing various heuristics involving credit card related terms and use of delimiters.
Credit Cards: Enroute	Detection of valid Enroute credit card numbers employing various heuristics involving credit card related terms and use of delimiters.
Credit Cards: Isracard	Detection of valid Isracard credit card numbers, when appearing together with an Isracard related term in English or Hebrew. By default, only the last 4 digits are shown in the reports.
Credit Cards: JCB 1sr	Detection of valid JCB credit card numbers employing various heuristics involving credit card related terms and use of delimiters.
Credit Cards: JCB 2nd	Detection of valid JCB credit card numbers employing various heuristics involving credit card related terms and use of delimiters.
Credit Cards: Maestro, Switch or Solo	Detection of valid Maestro, Switch or Solo credit card numbers employing various heuristics involving credit card related terms in English and Russian, and use of delimiters.
Credit Cards: Master Card	Detection of valid MasterCard credit card numbers employing various heuristics involving credit card related terms and use of delimiters.
Credit Cards: RuPay	Detection of valid Rupay debit card numbers employing various heuristics involving credit card related terms and use of delimiters.

Classifier	Description
Credit Cards: User-Defined IIN (Wide)	Detects potential credit card numbers, based only on format and validation. A list of allowed Issuer Identification Numbers (IIN) is read from the file CCN_IIN_Valid.csv, and a list of unallowed credit card numbers is read from the file CCN_Exceptions.csv. The files reside in the /policies_store/ policies/scripts/ subdirectory where Forcepoint DLP is installed, and can be edited. Deploy settings in the Security Manager to apply any changes. This classifier may cause false positives.
Credit Cards: User-Defined IIN (Default)	Detects valid credit card numbers employing various heuristics involving credit-card-related terms and use of delimiters. A list of allowed Issuer Identification Numbers (IIN) is read from the file CCN_IIN_Valid.csv, and a list of unallowed credit card numbers is read from the file CCN_Exceptions.csv. The files reside in the /policies_store/policies/scripts/ subdirectory where Forcepoint DLP is installed, and can be edited. Deploy settings in the Security Manager to apply any changes.
Credit Cards: User-Defined IIN (Narrow)	A restrictive detection of credit card numbers, tuned to minimize false positives. This rule requires additional evidence, such as credit-card-related terms in proximity, in order to qualify a number as a credit card number. A list of allowed Issuer Identification Numbers (IIN) is read from the file CCN_IIN_Valid.csv, and a list of unallowed credit card numbers is read from the file CCN_Exceptions.csv. The files reside in the /policies_store/policies/scripts/ subdirectory where Forcepoint DLP is installed, and can be edited. Deploy settings in the Security Manager to apply any changes.
Credit Cards: Visa	Detection of valid Visa credit card numbers employing various heuristics involving credit card related terms and use of delimiters.
Credit Cards: Visa with 13 digits	Detection of valid 13 digit Visa credit card numbers employing various heuristics involving credit card related terms and use of delimiters.
Croatian Personal identification number (Wide)	Detects valid 11-digit Personal identification numbers. For example “92103795594”.
Croatian Personal identification number (Default)	Detects valid 11-digit Personal identification numbers. At least 70% of the 11-digit numbers in the text need to be valid. For example “92103795594”.
Croatian Personal identification number Near Term	Detects valid 11-digit Personal identification numbers near a support term. For example “Osobni identifikacijski broj 92103795594”.
Cumulative HTTP number of Posts	Determines how many posts should exist before they are considered suspicious. This will only work on HTTP channel.
Cumulative HTTP number of Posts - Categorized URLs	Determines how many posts should exist before they are considered suspicious. This will only work on HTTP channel. Thresholds are configured for posting to categorized URLs.
Cumulative HTTP number of Posts - Uncategorized URLs	Determines how many posts should exist before they are considered suspicious. This will only work on HTTP channel. Thresholds are configured for posting to uncategorized URLs.

Classifier	Description
Cumulative HTTP Post Size	Determines which posts (according to size) will be counted. This will only work on HTTP channel.
Cumulative HTTP Post Size - Categorized URLs	Determines which posts (according to size) will be counted. This will only work on HTTP channel. Thresholds are configured for posting to categorized URLs.
Cumulative HTTP Post Size - Uncategorized URLs	Determines which posts (according to size) will be counted. This will only work on HTTP channel. Thresholds are configured for posting to uncategorized URLs.
CUSIP Numbers	Detection of validated CUSIP numbers.
Customizable IDs	Detection of ID numbers. The “ID Number pattern” parameter is the only mandatory parameter.
CV and Resume in Chinese (Wide)	A permissive classifier for detection of resumes and CVs in Chinese, using location-sensitive lexical analysis of terms and patterns common in such documents.
CV and Resume in Chinese (Default)	Detection of resumes and CVs in Chinese, using location-sensitive lexical analysis of terms and patterns common in such documents.
CV and Resume in Chinese (Narrow)	A restrictive classifier for detection of resumes and CVs in Chinese, using location-sensitive lexical analysis of terms and patterns common in such documents.
CV and Resume in English	Detection of resumes and CVs in English, using location-sensitive lexical analysis of terms and patterns common in such documents.
CV and Resume in Russian or Ukrainian	Detection of resumes and CVs in Russian or Ukrainian, using location-sensitive lexical analysis of terms and patterns common in such documents.
Cypriot Tax Identification Code Near Term	Detects Cypriot Tax Identification Codes near a support term in Greek or English. For example: “T.I.C. 12000017M”.
Cyrillic User-Defined Weighted Dictionary (non-unique)	Detection of weighted Cyrillic keywords, where each term is counted according to the number of appearances. The terms and weights are supplied from an external file (‘weighted_sections_Cyrillic_dictionary_unique.txt’), each dictionary in a separate section. In order to use it, insert your terms according to the example, and rename the section name in the script classifier parameter. Consider terms unique appearances. Adding wildcard (‘*’) in the beginning/end of the term, allow detecting regardless of the suffix/prefix - (up to 8 Cyrillic characters).
Cyrillic User-Defined Weighted Dictionary (non-unique) with EP Encryption	Detection of weighted Cyrillic keywords, where each term is counted according to the number of appearances. The terms and weights are supplied from an external file (‘weighted_sections_Cyrillic_dictionary_unique.txt’), each dictionary in a separate section. In order to use it, insert your terms according to the example, and rename the section name in the script classifier parameter. Consider terms unique appearances. Adding wildcard (‘*’) in the beginning/end of the term, allow detecting regardless of the suffix/prefix - (up to 8 Cyrillic characters).

Classifier	Description
Cyrillic User-Defined Weighted Dictionary (unique)	Detection of weighted Cyrillic keywords, where each term is counted only once. The terms and weights are supplied from an external file ('weighted_sections_Cyrillic_dictionary_unique.txt'), each dictionary in a separate section. In order to use it, insert your terms according to the example, and rename the section name in the script classifier parameter. Consider terms unique appearances. Adding wildcard ('*') in the beginning/end of the term, allow detecting regardless of the suffix/prefix - (up to 8 Cyrillic characters).
Cyrillic User-Defined Weighted Dictionary (unique) with EP Encryption	Detection of weighted Cyrillic keywords, where each term is counted only once. The terms and weights are supplied from an external file ('weighted_sections_Cyrillic_dictionary_unique.txt'), each dictionary in a separate section. In order to use it, insert your terms according to the example, and rename the section name in the script classifier parameter. Consider terms unique appearances. Adding wildcard ('*') in the beginning/end of the term, allow detecting regardless of the suffix/prefix - (up to 8 Cyrillic characters).
Danish Account Numbers (Default)	Detection of Danish bank account numbers, when found in proximity to bank account related terms.
Danish Account Numbers (Narrow)	Detection of strictly formatted Danish bank account numbers, when found in proximity to bank account related terms.
Danish Account Numbers (Wide)	Detection of Danish bank account numbers.
Date Of Birth	Detection of dates of birth.
Date Of Birth (ages 10-90)	Detection of dates of birth for ages in the range 10-90 without support terms.
Date Of Birth (ages 20-65)	Detection of dates of birth for ages in the range 20-65 without support terms.
Denmark: CPR Number (Default)	Detection of at least 5 CPR numbers, or at least 1 CPR with term such as "CPR".
Denmark: CPR Number (Narrow)	Detection of at least 1 Danish CC number with a term or at least 10 without terms.
Denmark: CPR Number (Wide)	Detection of CPR numbers.
Dictionary Phrases in Header/Footer	Detection of user-defined, case-insensitive dictionary phrases in the header or footer of documents. For example, the dictionary phrase "secret" will be found on the text "TOP SECRET" but not in "Secretive and highly classified." The phrase list "secret, sensitive, private" will be found when any of those exact phrases are in header/footer text. Only the first phrase that is found shows as a violation trigger.

Classifier	Description
Document to Self (Default)	A classifier that returns a match if a CV or resume belongs to its distributer. It does this by extracting a name and an email address from the opening part of the document, and checking whether the corporate user name of the distributer can be extracted from the name found in the document (such as jsmith@mycompany.com can be extracted from John Smith or even Jennifer T. Smith-Brown). It also checks whether the user name and the email address could have been extracted from the same name (jsmith@mycompany.com can match john.smith1@gmail.com). If at least one of those tests is positive, the classifier returns a match.
Document to Self (Wide)	A classifier that returns a match if a CV or resume belongs to its distributer. It does this by extracting a name and an email address from the opening part of the document, and checking whether the corporate user name of the distributer can be extracted from the name found in the document (such as jsmith@mycompany.com can be extracted from John Smith or even Jennifer T. Smith-Brown). It also checks whether the user name and the email address could have been extracted from the same name and with a wide margin for error (jsmith@mycompany.com can match jksmiththegreat@gmail.com). If at least one of those tests is positive, the classifier returns a match.
Driver License: District of Colombia	Detection of valid District of Colombia driver license number, in proximity to driver license terms, including typos and misspellings.
Driver License: Indiana	Detection of valid Indiana driver license number, in proximity to driver license terms, including typos and misspellings.
Driver License: Iowa	Detection of valid Iowa driver license number, in proximity to driver license terms, including typos and misspellings.
Driver License: Japan	Detection of Japanese Driver's License Number in proximity to driver license related terms. The terms and digits are detected in both English and Japanese.
Driver License: Massachusetts	Detection of valid Massachusetts driver license number, in proximity to driver license terms, including typos and misspellings.
Driver License: Missouri	Detection of valid Missouri driver license number, in proximity to driver license terms, including typos and misspellings.
Driver License: Nevada	Detection of valid Nevada driver license number, in proximity to driver license terms, including typos and misspellings.
Driver License: Utah	Detection of valid Utah driver license number, in proximity to driver license terms, including typos and misspellings.
Driver License: Virginia	Detection of valid Virginia driver license number, in proximity to driver license terms, including typos and misspellings.
DSA Private Key	Detection of DSA private keys. The first line of the key contains the string "BEGIN DSA PRIVATE KEY".
EAR - Chemical Data Detection (Default)	Detection of chemical formulas and information related to composite materials.

Classifier	Description
EAR - Chemical Data Detection (Narrow)	Detection of chemical formulas and information related to composite materials. Requires high rate of evidence.
EAR - Chemical Data Detection (Wide)	Detection of chemical formulas and information related to composite materials. May cause false positives.
EIN (Default)	Detection of Employer ID Number (EIN).
Elliptic Curve Private Key	Detection of Elliptic Curve private keys. The first line of the key contains the string "BEGIN EC PRIVATE KEY".
Email Addresses	Detection of email addresses.
Email Addresses Domains	Detection of email addresses with different domains.
Email to Competitors	Detection of email sent to competitors. The competitors' domain names are supplied as a case-insensitive parameter. In order to use it, insert domain names into the parameter, separated by a semicolon.
Email Similarity	Detection of similar names in the source and destination of email addresses. Should be used with an AND condition together with the relevant type of sensitive information.
Encrypted Files - Unknown Format	Detection of encrypted files (unknown format) according to internal file properties.
Encrypted Files - Unknown Format (Wide)	Detection of encrypted files (unknown format) according to internal file properties (Wide)
Encrypted PKCS #8 Private Key	Detection of encrypted PKCS #8 private keys. The first line of the key contains the string "BEGIN ENCRYPTED PRIVATE KEY".
Estonian Personal Identification Code (Wide)	Detects valid 11-digit Estonian personal identification codes (Isikukood). For example: "39001012038".
Estonian Personal Identification Code (Default)	Detects valid 11-digit Estonian personal identification codes (Isikukood). At least 50% of the 11-digit numbers in the text must be valid. For example: "39001012038".
Estonian Personal Identification Code Near Term	Detects valid 11-digit Estonian personal identification codes (Isikukood) near a support term in Estonian or English. For example: "Isikukood 39001012038".
EU Credit Cards	Detection of valid credit card number prevalent in Europe, employing various heuristics involving credit card related terms and use of delimiters.
Expiration Dates: Date After	Return 'True' if the current date is after the date specified in the classifier parameters. Can be used to construct a rule that is valid since a certain date, default expiration date is 31/12/2000. For example, you can set a keyword classifier to be "Code Yellow", and use it in an 'and' relation with the 'Date After' classifier.

Classifier	Description
Expiration Dates: Date Before	Return ‘True’ if the current date is before the date specified in the classifier parameters. Can be used to construct a rule that is valid after a certain date, default date is 31/12/2020. For example, you can set a keyword classifier to be “Code Yellow”, and use it in an ‘and’ relation with the ‘Date Before’ classifier.
Explicit Password	Detection of a phrase that explicitly marks a specific password. For example: “pwd=Qwerty1234” or “My password is ‘123456’”.
F# Source Code (By Content)	Detection of F# source code by content.
Finnish SSN (Default)	Detection of Finnish validated Social Security Numbers, when found in proximity to related terms.
Finnish SSN (Wide)	Detection of Finnish validated Social Security Numbers.
Form 10-K (Standard Fiscal Year)	Detection of 10K forms.
Form 10-K (Non Standard Fiscal Year)	Detection of 10K forms for non standard fiscal years (not ending at 31/12).
Form 10-Q (Standard Fiscal Year)	Detection of 10Q forms.
Form 10-Q (Non Standard Fiscal Year)	Detection of 10Q forms for non standard fiscal years (not ending at 31/12).
France INSEE Number	Detection of valid INSEE (NIR) numbers, validated with or without check digits.
French Names	Detection of French full names.
German Names	Detection of German full names.
Greece: AFM number (Default)	Detection of at least one Greek AFM number with a term in proximity, or several AFM numbers with statistical validation.
Greece: AFM number (Wide)	Detection of Greek AFM number with no term approvement or statistical validation.
Greece: Greek ID number	Detection of Greek ID number.
Greece: Greek Name (Default)	Detection of Greek full name (default behavior).
Greece: Greek Name (Wide)	Detection of Greek full name (wide behavior).
Health Insurance Claim Number (HICN)	Detects Health Insurance Claim Number (HICN). For example: "427432010A".
Hong Kong: Address (default)	Detection of Hong Kong address (default behavior).
Hong Kong: Address (narrow)	Detection of Hong Kong address, tuned to minimize false positives (may cause false negatives).
Hong Kong: Address (wide)	Detection of Hong Kong address, with possible false positives.
Hong Kong: ID - formal	Detection of Hong Kong ID of the form A123456(7).

Classifier	Description
Hong Kong: ID - non formal	Detection of Hong Kong ID of the form A1234567, without requiring ID terms.
Hungary CNP	Detection of Hungary validated Personal Numeric Code Numbers when found in proximity to related terms.
Hungary CNP (Wide)	Detection of Hungary validated Personal Numeric Code Numbers.
Hungary SSN	Detection of Hungary Social Security Numbers, when found in proximity to related terms
Hungary SSN (Wide)	Detection of Hungary validated Social Security Numbers.
Hungary Tax ID	Detection of Hungary validated Tax ID Numbers when found in proximity to related terms.
Hungary Tax ID (Wide)	Detection of Hungary validated Tax ID Numbers.
IBAN Austria	Detection of Austrian IBANs (International Bank Account Numbers). Searches for support terms in proximity to Austrian IBAN format.
IBAN Austria (Wide)	Detection of Austrian IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Belgium	Detection of Belgian IBANs (International Bank Account Numbers). Searches for support terms in proximity to Belgian IBAN format.
IBAN Belgium (Wide)	Detection of Belgian IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Brazil	Detection of Brazilian IBANs (International Bank Account Numbers). Searches for support terms in proximity to Brazilian IBAN format.
IBAN Brazil (Wide)	Detection of Brazilian IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Bulgaria	Detection of Bulgarian International Bank Account Numbers (IBAN) near a support term.
IBAN Bulgaria (Wide)	Detection of Bulgarian International Bank Account Numbers (IBAN).
IBAN Croatia	Detection of Croatian International Bank Account Numbers (IBAN) near a support term.
IBAN Croatia (Wide)	Detection of Croatian International Bank Account Numbers (IBAN).
IBAN Cyprus	Detection of Cypriot International Bank Account Numbers (IBAN) near a support term.
IBAN Cyprus (Wide)	Detection of Cypriot International Bank Account Numbers (IBAN).
IBAN Czech Republic	Detection of Czech IBANs (International Bank Account Numbers). Searches for support terms in proximity to Czech IBAN format.

Classifier	Description
IBAN Czech Republic (Wide)	Detection of Czech IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Denmark	Detection of Danish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Danish IBAN format.
IBAN Denmark (Wide)	Detection of Danish IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Estonia	Detection of Estonian IBANs (International Bank Account Numbers). Searches for support terms in proximity to Estonian IBAN format.
IBAN Estonia (Wide)	Detection of Estonian IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Finland	Detection of Finnish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Finnish IBAN format.
IBAN Finland (Wide)	Detection of Finnish IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN France	Detection of French IBANs (International Bank Account Numbers). Searches for support terms in proximity to French IBAN format.
IBAN France (Wide)	Detection of French IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN General	Detection of general IBAN numbers.
IBAN Germany	Detection of German IBANs (International Bank Account Numbers). Searches for support terms in proximity to German IBAN format.
IBAN Germany (Wide)	Detection of German IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Greece	Detection of Greek IBANs (International Bank Account Numbers). Searches for support terms in proximity to Greek IBAN format.
IBAN Greece (Wide)	Detection of Greek IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Hungary	Detection of Hungarian IBANs (International Bank Account Numbers). Searches for support terms in proximity to Hungarian IBAN format.
IBAN Hungary (Wide)	Detection of Hungarian IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Iceland	Detection of Icelandic IBANs (International Bank Account Numbers). Searches for support terms in proximity to Icelandic IBAN format.
IBAN Iceland (Wide)	Detection of Icelandic IBANs (International Bank Account Numbers) without support terms in proximity.

Classifier	Description
IBAN Ireland	Detection of Irish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Irish IBAN format.
IBAN Ireland (Wide)	Detection of Irish IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Italy	Detection of Italian IBANs (International Bank Account Numbers). Searches for support terms in proximity to Italian IBAN format.
IBAN Italy (Wide)	Detection of Italian IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Kazakhstan	Detection of Kazakh IBANs (International Bank Account Numbers). Searches for support terms in proximity to Kazakh IBAN format.
IBAN Kazakhstan (Wide)	Detection of Kazakh IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Latvia	Detection of Latvian International Bank Account Numbers (IBAN) near a support term.
IBAN Latvia (Wide)	Detection of Latvian International Bank Account Numbers (IBAN).
IBAN Lithuania	Detection of Lithuanian International Bank Account Numbers (IBAN) near a support term.
IBAN Lithuania (Wide)	Detection of Lithuanian International Bank Account Numbers (IBAN).
IBAN Luxembourg	Detection of Luxembourgian IBANs (International Bank Account Numbers). Searches for support terms in proximity to Luxembourgian IBAN format.
IBAN Luxembourg (Wide)	Detection of Luxembourgian IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Malta	Detection of Maltese International Bank Account Numbers (IBAN) near a support term.
IBAN Malta (Wide)	Detection of Maltese International Bank Account Numbers (IBAN).
IBAN Netherlands	Detection of Netherlands IBANs (International Bank Account Numbers). Searches for support terms in proximity to Netherlands IBAN format.
IBAN Netherlands (Wide)	Detection of Netherlands IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Norway	Detection of Norwegian IBANs (International Bank Account Numbers). Searches for support terms in proximity to Norwegian IBAN format.
IBAN Norway (Wide)	Detection of Norwegian IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Poland	Detection of Polish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Polish IBAN format.

Classifier	Description
IBAN Poland (Wide)	Detection of Polish IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Portugal	Detection of Portuguese International Bank Account Numbers (IBAN) near a support term.
IBAN Portugal (Wide)	Detection of Portuguese International Bank Account Numbers (IBAN).
IBAN Qatar	Detection of Qatari IBANs (International Bank Account Numbers). Searches for support terms in proximity to Qatari IBAN format.
IBAN Qatar (Wide)	Detection of Qatari IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Romania	Detection of Romanian IBANs (International Bank Account Numbers). Searches for support terms in proximity to Romanian IBAN format.
IBAN Romania (Wide)	Detection of Romanian IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Saudi Arabia	Detection of Saudi Arabia IBANs (International Bank Account Numbers). Searches for support terms in proximity to Irish IBAN format.
IBAN Saudi Arabia (Wide)	Detection of Saudi Arabia IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Slovakia	Detection of Slovak IBANs (International Bank Account Numbers). Searches for support terms in proximity to Slovak IBAN format.
IBAN Slovakia (Wide)	Detection of Slovak IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Slovenia	Detection of Slovene International Bank Account Numbers (IBAN) near a support term.
IBAN Slovenia (Wide)	Detection of Slovene International Bank Account Numbers (IBAN).
IBAN Spain	Detection of Spanish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Spanish IBAN format.
IBAN Spain (wide)	Detection of Spanish IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Sweden	Detection of Swedish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Swedish IBAN format.
IBAN Sweden (Wide)	Detection of Swedish IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN Switzerland	Detection of Swiss IBANs (International Bank Account Numbers). Searches for support terms in proximity to Swiss IBAN format.
IBAN Switzerland (Wide)	Detection of Swiss IBANs (International Bank Account Numbers) without support terms in proximity.

Classifier	Description
IBAN Turkey	Detection of Turkish IBANs (International Bank Account Numbers). Searches for support terms in proximity to Turkish IBAN format.
IBAN Turkey (Wide)	Detection of Turkish IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN UK	Detection of UK IBANs (International Bank Account Numbers). Searches for support terms in proximity to UK IBAN format.
IBAN UK (Wide)	Detection of UK IBANs (International Bank Account Numbers) without support terms in proximity.
IBAN United Arab Emirates	Detection of Emirati IBANs (International Bank Account Numbers). Searches for support terms in proximity to Emirati IBAN format.
IBAN United Arab Emirates (Wide)	Detection of Emirati IBANs (International Bank Account Numbers) without support terms in proximity.
ICD10 Codes	Detection of codes that belong to the ICD10 system. No additional information is required.
ICD10 English Descriptions	Detection of English descriptions of medical conditions as they appear in the ICD10 manual.
ICD10 Norwegian Descriptions	Detection of Norwegian descriptions of medical conditions as they appear in the ICD10 manual.
Icelandic Kennitala of Individuals (Default)	Detection of Icelandic identification numbers (kennitala) of individuals, employing various heuristics involving kennitala-related terms and other features unique to this number.
Icelandic Kennitala of Individuals (Wide)	Detection of Icelandic identification numbers (kennitala) of individuals, employing various heuristics involving features unique to this number.
IL bank accounts: Benleumi	Detection of validated BenLeumi account numbers in proximity to terms related to accounts in English or Hebrew.
IL bank accounts: Discount	Detection of validated Discount account numbers in proximity to terms related to accounts in English or Hebrew.
IL bank accounts: Hadoar	Detection of validated HaDoar account numbers, when appearing with terms relating to accounts in English or Hebrew.
IL bank accounts: Leumi	Detection of validated Leumi account numbers which include branch numbers, when appearing with terms relating to accounts in English or Hebrew.
IL bank accounts: Leumi no support	Detection of validated Leumi account numbers which include branch numbers.
IL bank accounts: Mizrahi	Detection of validated Mizrahi account numbers which include branch numbers, when appearing with terms relating to accounts in English or Hebrew.
IL bank accounts: Poalim	Detection of validated Poalim account numbers which include branch numbers, when appearing with terms relating to accounts in English or Hebrew.
IL Life Insurance	Detection of Israeli life insurance numbers.

Classifier	Description
IMEI (Default)	Detection of at least two validated IMEI numbers, delimited and non-delimited. Also locates IMEI related term somewhere in the document.
IMEI (Wide)	Detection of at least two validated IMEI numbers, delimited and non-delimited.
India: Form 16	Detection of India Form 16 that has been filled out, using identification of textual patterns common to such forms.
Indian Names (Default)	Detection of Indian full names.
Indian Names (Narrow)	Detection of Indian full names (Narrow).
Indian Names (Wide)	Detection of Indian full names (Wide). This content classifier should be used in conjunction with additional data as it is permissive.
Indonesian Single Identity Numbers (Default)	Detects valid 16-digit delimited or un-delimited Indonesian Single Identity Numbers (Nomor Induk Kependudukan). At least half of all 16-digit numbers need to be valid. For example "3313034604790001".
Indonesian Single Identity Numbers (Narrow)	Detects valid 16-digit delimited or un-delimited Indonesian Single Identity Numbers (Nomor Induk Kependudukan) where the last 4 digits are under 0400. At least half of all 16-digit numbers need to be valid. For example "3313034604790001".
Indonesian Single Identity Numbers Near Term	Detects valid 16-digit delimited or un-delimited Indonesian Single Identity Numbers (Nomor Induk Kependudukan) near a support term in English or in Indonesian. For example "nomor KTP 3313034604790001".
Ireland PRSI/PPS	Detection of Irish Personal Public Service numbers.
ISIN: Default	Detection of valid International Securities Identification Numbers (ISINs).
ISIN: with country code validation	Detection of valid International Securities Identification Numbers (ISINs), with validating country code.
Israel: Common Medical Information	Detection of medical conditions in Hebrew or English.
Israel: Sensitive Medical Information	Detection of medical conditions of sensitive nature in Hebrew or English.
Israeli Credit Cards	Detection of valid credit card number prevalent in Israel.
Israeli Credit Cards (Default)	Detection of Israeli credit card numbers (not including Isracard) employing various heuristics involving credit card related terms and use of delimiters. By default, only the first 4 digits and the last 4 digits are shown in the reports.
Israeli Credit Cards (Narrow)	Detection of Israeli credit card numbers (not including Isracard). Requires additional evidence, such as credit card related terms in proximity, in order to qualify number as a credit card number. By default, only the first 4 digits and the last 4 digits are shown in the reports.

Classifier	Description
Israeli Credit Cards (Wide)	Detection of potential Israeli credit card numbers (not including Isracard), based only on format and validation, may cause false positives. By default, only the first 4 digits and the last 4 digits are shown in the reports.
Israeli IBAN	Detection of Israeli IBANs (International Bank Account Numbers). Searches for support terms in proximity to Israeli IBAN format.
Israeli IBAN (Wide)	Detection of Israeli IBANs (International Bank Account Numbers) without support terms in proximity.
Israeli Identity Number (Default)	Detects valid 9-digit Israeli identity numbers. At least 50% of the 9-digit numbers in the text need to be valid. For example: “064810948”.
Israeli Identity Number Near Term	Detects valid 9-digit Israeli identity numbers near a support term in Hebrew, Arabic, or English. For example: “Teudat Zehut 064810948”.
Israeli Identity Number (Wide)	Detects valid 9-digit Israeli identity numbers. For example: “064810948”.
Israeli Identity Number - 7-Digits (Default)	Detects valid 7-digit Israeli identity numbers where the leftmost 2 digits, “00”, are omitted. At least 50% of the 7-digit numbers in the text must be valid. For example: “9896747”.
Israeli Identity Number (7-Digits) Near Term	Detects valid 7-digit Israeli identity numbers where the leftmost 2 digits, “00”, are omitted near a support term in Hebrew, Arabic, or English. For example: “Teudat Zehut 9896747”.
Israeli Identity Number - 7-Digits (Wide)	Detects valid 7-digit Israeli identity numbers where the leftmost 2 digits, “00”, are omitted. For example: “9896747”.
Israeli Identity Number - 8-Digits (Default)	Detects valid 8-digit Israeli identity numbers where the leftmost digit, “0”, is omitted. At least 50% of the 8-digit numbers in the text must be valid. For example: “64810948”.
Israeli Identity Number (8-Digits) Near Term	Detects valid 8-digit Israeli identity numbers where the leftmost digit, “0”, is omitted near a support term in Hebrew, Arabic, or English. For example: “Teudat Zehut 64810948”.
Israeli Identity Number - 8-Digits (Wide)	Detects valid 8-digit Israeli identity numbers where the leftmost digit, “0”, is omitted. For example: “64810948”.
Israeli Insurance Claims	Detection of Israeli life insurance claims numbers when appearing in proximity to related terms.
Israeli life Insurance	Detection of Israeli life insurance numbers when appearing in proximity to life insurance related terms.
Israeli Names	Detection of Israeli full names.
Israeli Phone Numbers (Default)	Detection of Israeli Phone Numbers, when found in proximity to related terms.
Israeli Phone Numbers (Wide)	Detection of Israeli Phone Numbers.
Israeli generic insurance number (delimited)	Detection of generic Israeli insurance policy numbers in standard delimitation

Classifier	Description
Israeli generic insurance number (non delimited)	Detection of generic Israeli insurance policy numbers without delimitation
Italian Names	Detection of Italian full names.
Italy Codice Fiscale Number	Detection of validated Italy Codice Fiscale, possibly in proximity to related terms.
Japan Emails	Detection of at least 20 email addresses revealing personal information about the owner, such as their full name and place of employment.
Japan Ledger	Detection of Japanese Ledger Number in proximity Ledger related terms. The terms and digits are detected in both English and Japanese.
Japan Pension	Detection of Japanese Pension Number in proximity to pension related terms. The terms and digits are detected in both English and Japanese.
Japan Phone Numbers	Detection of Japanese telephone numbers, where at least one number is in proximity to phone number related terms in English or Japanese.
Japanese Corporate Numbers (Wide)	Detects valid 13-digit delimited or un-delimited Japanese Corporate Numbers. For example “7-0000-1201-1012”.
Japanese Corporate Numbers (Default)	Detects valid 13-digit delimited or un-delimited Japanese Corporate Numbers. At least 70% of all 13-digit numbers need to be valid. For example “7-0000-1201-1012”.
Japanese Corporate Numbers Near Term	Detects valid 13-digit delimited or un-delimited Japanese Corporate Numbers near a support term in English or in Japanese. For example “Corporate Number 7-0000-1201-1012”.
Japanese Credit Cards	Detection of valid credit card number prevalent in Japan, employing various heuristics involving credit card related terms and use of delimiters. The terms and credit card digits are detected in both English and Japanese.
Japanese Individual Numbers (Wide)	Detects valid 12-digit delimited or un-delimited Japanese Individual Numbers (My Numbers). For example “3591 0546 2229”.
Japanese Individual Numbers (Default)	Detects valid 12-digit delimited or un-delimited Japanese Individual Numbers (My Numbers). At least 70% of all 12-digit numbers need to be valid. For example “3591 0546 2229”.
Japanese Individual Numbers Near Term	Detects valid 12-digit delimited or un-delimited Japanese Individual Numbers (My Numbers) near a support term in English or Japanese. For example “My Number 3591 0546 2229".
JSON Keystore File Private Key	Detection of JSON Keystore File private keys that are used to hold Bitcoin's and Ethereum's wallet's private key information.
Kazakh Taxpayer Registration Numbers	Detection of valid Kazakh Taxpayer Registration Numbers.

Classifier	Description
Kazakh Individual Identification Numbers	Detection of valid Kazakh Individual Identification Numbers.
Kazakh Business Identification Numbers	Detection of valid Kazakh Business Identification Numbers.
Key Phrases in Header/ Footer	Detection of user-defined, case-insensitive key phrases in the header or footer of documents. For example, the key phrase “secret” will be found in the text “Secretive and highly classified” and “TOP SECRET.” The phrase list “secret, sensitive, private” will be found when any form of those phases are in header/footer text. Only the first phrase that is found shows as a violation trigger.
Korea Phone Numbers (Narrow)	Detection of Korea phone numbers, employing statistical analysis.
Korea Phone Numbers (Wide)	Detection of Korea phone numbers.
Korea Phone Numbers (With Support)	Detection of Korea phone numbers, when found in proximity to related terms such as ‘phone’ in English or Korean.
Latitude-Longitude coordinates	Detection of Latitude-Longitude coordinates.
Latvian Personal Identity Number (Wide)	Detects valid 11-digit Latvian personal identity numbers (Personas kods). For example: “281247-11862”.
Latvian Personal Identity Number (Default)	Detects valid 11-digit Latvian personal identity numbers (Personas kods). At least 50% of the 11-digit numbers in the text must be valid. For example: “281247-11862”.
Latvian Personal Identity Number Near Term	Detects valid 11-digit Latvian personal identity numbers (Personas kods) near a support term in Latvian or English. For example: “Personas kods 281247-11862”.
Lithuanian Personal Code (Wide)	Detects valid 11-digit Lithuanian Personal Code (Asmens kodas). For example: “46709261415”.
Lithuanian Personal Code (Default)	Detects valid 11-digit Lithuanian Personal Code (Asmens kodas). At least 50% of the 11-digit numbers in the text must be valid. For example: “46709261415”.
Lithuanian Personal Code Near Term	Detects valid 11-digit Lithuanian Personal Code (Asmens kodas) near a support term in Lithuanian or English. For example: “Asmens kodas 46709261415”.
Luxembourgian National Identification Number - 11 Digits (Wide)	Detects valid 11-digit Luxembourgian national identification numbers (Matricule). For example: “1994 01 27 087”.
Luxembourgian National Identification Number - 11 Digits (Default)	Detects valid 11-digit Luxembourgian national identification numbers (Matricule). At least 50% of the 11-digit numbers in the text must be valid. For example: “1994 01 27 087”.
Luxembourgian National Identification Number - 11 Digits Near Term	Detects valid 11-digit Luxembourgian national identification numbers (Matricule) near a support term in French, German, Luxembourgish, or English. For example: “Matricule 1994 01 27 087”.

Classifier	Description
Luxembourgian National Identification Number - 13 Digits (Wide)	Detects valid 13-digit Luxembourgian national identification numbers (Matricule). For example: “1992 0311 426 93”.
Luxembourgian National Identification Number - 13 Digits (Default)	Detects valid 13-digit Luxembourgian national identification numbers (Matricule). At least 50% of the 13-digit numbers in the text must be valid. For example: “1992 0311 426 93”.
Luxembourgian National Identification Number - 13 Digits Near Term	Detects valid 13-digit Luxembourgian national identification numbers (Matricule) near a support term in French, German, Luxembourgish, or English. For example: “Matricule 1992 0311 426 93”.
MAC Address (Default)	Detection of MAC addresses. Detects only delimited MAC addresses.
MAC Address (Narrow)	Detection of MAC addresses, detects delimited MAC addresses with a valid OUI (Organizationally Unique Identifier).
MAC Address (Wide)	Detection of MAC addresses. Detects delimited MAC addresses and non-delimited MAC addresses with support terms in proximity.
Malaysia ID: no date validation	Detection of validated Malaysia ID in a form like dddddd-16-7356. Does not require support term in proximity.
Malaysia ID: no date validation, with proximity	Detection of validated Malaysia ID in a form like dddddd-16-7356 providing that Malaysia ID terms such as MyKad, GMPC or ID appears in proximity.
Malaysia ID: with date and BP validation	Detection of validated Malaysia ID in a form like YYMMDD-BP-7356, where first six digits stand for a birth date. Does not require support term in proximity.
Malaysia ID: with date and BP validation, with proximity	Detection of validated Malaysia ID in a form like dddddd-BP-7356, providing that Malaysia ID terms such as MyKad, GMPC or ID appears in proximity.
Malaysia ID: with date validation	Detection of validated Malaysia ID in a form like YYMMDD-16-7356, where first six digits stand for a birth date. Does not require support term in proximity.
Malaysia ID: with date validation, with proximity	Detection of validated Malaysia ID in a form like YYMMDD-16-7356, where first six digits stand for a birth date, providing that Malaysia ID terms such as MyKad, GMPC or ID appears in proximity.
Malicious Concealment	Detection of content suspected to be manipulated (e.g. by replacing letters with symbols) to avoid detection, using methods such as statistical analysis.
Malicious Concealment (Narrow)	Detection of content suspected to be manipulated (e.g. by replacing letters with symbols) to avoid detection, using methods such as statistical analysis.
Malicious Concealment (Wide)	Detection of content suspected to be manipulated (e.g., by replacing letters with symbols) to avoid detection, using methods such as statistical analysis. May cause false positives.
Malicious Concealment: L33T	Detection of content suspected to be manipulated using “L33T” manipulation.

Classifier	Description
Malicious Concealment: L33T (Narrow)	Detection of content suspected to be manipulated using “L33T” manipulation.
Malicious Concealment: L33T (Wide)	Detection of content suspected to be manipulated using “L33T” manipulation, may cause false positives.
Malicious Concealment: Reversed Text	Detection of content suspected to be manipulated as reversing the text.
Malicious Concealment: Reversed Text (Narrow)	Detection of content suspected to be manipulated as reversing the text.
Malicious Concealment: Reversed Text (Wide)	Detection of content suspected to be manipulated as reversing the text, may cause false positives.
Malicious Concealment: ROT13	Detection of content suspected to be manipulated using “ROT13” manipulation.
Malicious Concealment: ROT13 (Narrow)	Detection of content suspected to be manipulated using “ROT13” manipulation.
Malicious Concealment: ROT13 (Wide)	Detection of content suspected to be manipulated using “ROT13” manipulation, may cause false positives.
Malicious Concealment: Upside Down Text	Detection of content suspected to be manipulated using “upside down” manipulation.
Malicious Concealment: Upside Down Text (Narrow)	Detection of content suspected to be manipulated using “upside down” manipulation.
Malicious Concealment: Upside Down Text (Wide)	Detection of content suspected to be manipulated using “upside down” manipulation, may cause false positives.
Maltese Identity Card Number Near Term	Detects Maltese identity card numbers near a support term in Maltese or English. For example: “Identity Card Number 19999981M”.
Malware (Default)	Identifies HTTP/S transactions that are suspected to be malicious, based, for example, on web category, destination URL structure, and a mathematical analysis of data. This rule is not selected by default. Applies only when Forcepoint Web Security is installed. Administrator tuning of the rule, for example, by excluding specific destinations, is recommended.
Malware (Strict) (Uncategorized)	Identifies HTTP/S transactions that are suspected to be malicious, based, for example, on web category, destination URL structure, and a mathematical analysis of data. This rule is not selected by default. Applies only when Forcepoint Web Security is installed. Administrator tuning of the rule, for example, by excluding specific destinations, is recommended.
MAR: Actuary Reports	Detection of documents contain actuary reports (in attachments or files).
Maximum Age (Wide)	Detection of numbers less than or equal to a user-specified threshold in proximity to an age-related term, or date of birth under the specified threshold. Default age is 13.

Classifier	Description
Maximum Age (Default)	Detection of age-related phrases containing numbers less than or equal to a user-specified threshold or date of birth under the specified threshold. Default age is 13.
Minimum Age (Wide)	Detection of numbers greater than or equal to a user-specified threshold in proximity to an age-related term, or date of birth under the specified threshold. Default age is 13.
Minimum Age (Default)	Detection of age-related phrases containing numbers greater than or equal to a user-specified threshold or date of birth under the specified threshold. Default age is 13.
Mexican Names	Detection of full names (Wide). This content classifier should be used in conjunction with additional data as it is permissive.
Mexican Passport Number Near Term (Default)	Detects Mexican passport numbers, near a term in Spanish or English. Mexican passport numbers consist of 11 digits or of a letter followed by 8 digits. For example, "Passport number: 07460075411".
Mexican Passport Number Near Term (Wide)	Detects case-insensitive Mexican passport numbers, near a permissive term in Spanish or English. Mexican passport numbers consist of 11 digits or of a letter followed by 8 digits. For example, "Passport: 07460075411".
Mexican Social Security Number (NSS) (Default)	Detects valid 11-digit Mexican Social Security Number (NSS). At least 30% of the 11-digit numbers in the text must be valid. For example: "7491761007-8".
Mexican Social Security Number (NSS) (Wide)	Detects valid 11-digit Mexican Social Security Number (NSS). For example: "7491761007-8".
Mexican Social Security Number (NSS) Near Term	Detects valid 11-digit Mexican Social Security Number (NSS), near a support term in Spanish or English. For example: "Numero del Seguro Social 7491761007-8".
Mexican Standardized Bank Code (CLABE) (Default)	Detects valid 18-digit Mexican Standardized Bank Code (CLABE), containing an assigned bank code and branch office code. At least 30% of the 18-digit numbers in the text must be valid. For example: "072 680 005439760704".
Mexican Standardized Bank Code (CLABE) (Wide)	Detects valid 18-digit Mexican Standardized Bank Code (CLABE). For example: "000180000404040406".
Mexican Standardized Bank Code (CLABE) Near Term	Detects valid 18-digit Mexican Standardized Bank Code (CLABE), containing an assigned bank code and branch office code, near a support term in Spanish or English. For example: "CLABE 072 680 005439760704".
Mexico CURP (Clave Unica de Registro de Poblacion)	Detection of Contract Nomenclature of CPISP (Clave Personal Interna del Servidor Publico).
Mexico RFC Number (Default)	Detection of Mexico RFC numbers, employing various heuristics involving RFC related terms and homoclaves.
Mexico RFC Number (Wide)	Detection of Mexico RFC numbers, without requiring homoclave or RFC term in proximity.

Classifier	Description
National Drug Code (Default)	Detection of National Drug Code (NDC) numbers of prescription drugs. Undelimited numbers are subjected to statistical validation.
National Drug Code (Narrow)	Detection of at least one delimited number or 5 undelimited National Drug Code (NDC) numbers of prescription drugs, using statistical validation.
National Drug Code (Wide)	Detection of National Drug Code (NDC) numbers of prescription drugs. All instances are returned and no further check is made, may cause false positives.
National Register of Legal Entities Number (Wide)	Detects valid 14-digit Brazilian National Register of Legal Entities Numbers (CNPJ). For example: “05.211.592/0001-04”.
National Register of Legal Entities Number (Default)	Detects valid 14-digit Brazilian National Register of Legal Entities Numbers (CNPJ). At least 50% of the 14-digit numbers in the text must be valid. For example: “05.211.592/0001-04”.
National Register of Legal Entities Number Near Term	Detects valid 14-digit Brazilian National Register of Legal Entities Numbers (CNPJ) near a support term in Portuguese or English. For example: “CNPJ 05.211.592/0001-04”.
Netherlands: Bank Account	Detection of Elfproef validated Dutch Bank Account numbers.
Netherlands: Citizen Service Number	Detection of Dutch Citizen Service Numbers (Burgerservicenummers or BSNs), in proximity to related terms.
Netherlands: Sofinummer	Detection of validated Netherlands Sofinummers, in proximity to related terms.
New Zealand NHI - no support	Detection of validated NHI Numbers, does not demand further evidence.
NHS Numbers (Default)	Detection of validated NHS numbers.
NHS Numbers (Narrow)	Detection of validated NHS numbers. Requires additional evidence, such as NHS related terms in proximity.
NHS Numbers (Wide)	Detection of all forms of valid NHS numbers.
Norway Personnummer	Detection of Norway Personal Numbers (personnummer), including d-numbers, possibly in proximity to related terms.
Norwegian Names	Detection of Norwegian full names.
OpenSSH Private Key	Detection of OpenSSH private keys. The first line of the key contains the string "BEGIN OPENSSH PRIVATE KEY".
Password (Default)	Detection of 8-25-character strings consisting of at least one letter and at least one digit or special characters that are not followed by a file extension. For example: “Qwerty1234”.
Password (Wide)	Detection of 6-25-character strings consisting of 1) at least one letter and at least one digit or special characters that are not followed by a file extension, or 2) two to three repeated alphanumeric strings, or 3) common passwords. For example: “Qwerty1”, “abcabc” or “letmein”.
Password Files	Detection of password files.

Classifier	Description
Password Files (Wide)	Detection of password files.
Password Near Term (Default)	Detection of password-related terms near 8-25-character strings consisting of at least one letter and at least one digit or special characters that are not followed by a file extension. For example: “Qwerty1234”. the term can be in Arabic, Chinese, Czech, Danish, Dutch, English, Finnish, French, Galician, German, Greek, Hebrew, Indonesian, Japanese, Korean, Norwegian, Portuguese, Russian, Slovak, Spanish, Swedish, Thai, Turkish, or Vietnamese.
Password Near Term (Wide)	Detection of password-related terms near 6-25-character strings consisting of 1) at least one letter and at least one digit or special characters that are not followed by a file extension, or 2) two to three repeated alphanumeric strings, or 3) common passwords. For example: “The Password is Qwerty1”, “das Passwort ist abcabc” or “pwd - letmein”. The term can be in Arabic, Chinese, Czech, Danish, Dutch, English, Finnish, French, Galician, German, Greek, Hebrew, Indonesian, Japanese, Korean, Norwegian, Portuguese, Russian, Slovak, Spanish, Swedish, Thai, Turkish, or Vietnamese.
Passwords - common passwords without term	Detection of common passwords (based on various common passwords lists) with or without trailing digits. No term is required in proximity. The minimal number of passwords is configurable through the parameter.
PCI Audit: CCN with CVV	Detection of valid credit cards near CVV.
PCI Audit: CCN with Expiration Date	Detection of valid credit cards near expiration dates.
PCI Audit: Masked Credit Cards	Detection of masked American Express, Discover, JCB, MasterCard, and Visa credit cards.
PCI Audit: Non-Delimited CCNs with no word boundaries	Detection of possible non-delimited credit card numbers, with no word boundaries.
PCI Audit: Non-Delimited Credit Card Numbers	Detection of valid non-delimited credit card numbers. May cause false positives.
PCI Audit: User-Defined CCN Delimiter	Detection of potential credit-card-numbers, possible delimiters can be added by the user, default delimiter is “-”.
People’s Republic of China Identification Numbers	Detection of validated People’s Republic of China Identification Numbers.
People's Republic of China Passport Number Near Term (Default)	Detects 9-character People's Republic of China passport numbers consisting of "D", "E", "G", "P" or "S" followed by 8 digits, near a term in Chinese or English. For example, "Passport: G45969933".
People's Republic of China Passport Number Near Term (Narrow)	Detects 9-character People's Republic of China passport numbers consisting of "D", "E", "G", "P" or "S" followed by 8 digits, near a strict term in Chinese or English. For example, "Passport No. G45969933".

Classifier	Description
Perl Source Code (By Content)	Detection of Perl source code by content.
Peruvian RUC of Individuals (Near Term)	Detects valid 11-digit Unique Taxpayer Registration Number (RUC) of Individuals near a support term in Spanish or English. For example: "RUC 10328503480".
Peruvian RUC of Individuals (Wide)	Detects valid 11-digit Unique Taxpayer Registration Number (RUC) of Individuals. For example: "10328503480".
Peruvian RUC of Non-Individuals (Near Term)	Detects valid 11-digit Unique Taxpayer Registration Number (RUC) of non-Individuals near a support term in Spanish or English. For example: "RUC 20519354111".
Peruvian RUC of Non-Individuals (Wide)	Detects valid 11-digit Unique Taxpayer Registration Number (RUC) of non-Individuals. For example: "20519354111".
Peruvian Unique Identification Code (CUI) (Default)	Detects valid 9-digit Peruvian Unique Identification Codes (CUI). At least 40% of the 9-digit numbers in the text must be valid. For example: "42158455-4".
Peruvian Unique Identification Code (CUI) (Wide)	Detects valid 9-digit Peruvian Unique Identification Codes (CUI). For example: "42158455-4".
Peruvian Unique Identification Code (CUI) Near Term (Default)	Detects valid 9-digit Peruvian Unique Identification Codes (CUI), near a support term in Spanish or English. For example: "CUI 42158455-4".
Peruvian Unique Identification Code (CUI) Near Term (Narrow)	Detects valid 9-digit Peruvian Unique Identification Codes (CUI), near a support term in Spanish or English. At least 40% of the 9-digit numbers in the text must be valid. For example: "CUI 42158455-4".
PGP Private Key	Detection of PGP private keys. The first line of the key contains the string "BEGIN PGP PRIVATE KEY BLOCK".
PhilHealth Identification Number (Wide)	Detects valid 12-digit Philippine PhilHealth Identification Numbers. For example: “12-000015726-6””.
PhilHealth Identification Number (Default)	Detects valid 12-digit Philippine PhilHealth Identification Numbers. At least 50% of the 12-digit numbers in the text must be valid. For example: “12-000015726-6”.
PhilHealth Identification Number Near Term	Detects valid 12-digit Philippine PhilHealth Identification Numbers near a support term in English. For example: “PhilHealth# 12-000015726-6”.
Philippine SSS Number (Wide)	Detects valid 10-digit Philippine SSS numbers. For example: “06-1739315-5”.
Philippine SSS Number (Default)	Detects valid 10-digit Philippine SSS numbers. At least 30% of the 10-digit numbers in the text must be valid. For example: “06-1739315-5”.
Philippine SSS Number Near Term	Detects valid 10-digit Philippine SSS numbers near a support term in English. For example: “SSS: 06-1739315-5”.
Philippine Taxpayer Identification Number (Wide)	Detects valid 9- or 12-digit Philippine taxpayer identification numbers (TINs). For example: “000 063 471”.

Classifier	Description
Philippine Taxpayer Identification Number (Default)	Detects valid 9- or 12-digit Philippine taxpayer identification numbers (TINs). At least 30% of the 9- and 12-digit numbers in the text must be valid. For example: “000 063 471”.
Philippine Taxpayer Identification Number Near Term	Detects valid 9- or 12-digit Philippine taxpayer identification numbers (TINs) near a support term in English. For example: “T.I.N. 000 063 471”.
Philippines Address (Default)	Detection of Philippines address (default behavior).
Philippines Address (Narrow)	Detection of Philippines address, tuned to minimize false positives (may cause false negatives).
PIN with proximity	Detection of personal identification numbers (PINs) in proximity to a PIN-related term.
PKCS #1 Private Key	Detection of PKCS #1 private keys, also known as SSLeay private keys. The first line of the key contains the string "BEGIN RSA PRIVATE KEY".
Poland: ID	Detection of Polish Identification numbers.
Poland: NIP Number	Detection of Polish NIP numbers.
Poland: PESEL Number	Detection of Polish Pesel numbers.
Poland: REGON Number	Detection of REGON numbers.
Portuguese Document Number (Wide)	Detects valid 12-digit Portuguese Document Numbers or 11-digit numbers where the leftmost digit, “0”, is omitted. For example: “13965280 9ZZ5”.
Portuguese Document Number (Default)	Detects valid 12-digit Portuguese Document Numbers or 11-digit numbers where the leftmost digit, “0”, is omitted. At least 30% of the 12- or 11-digit numbers in the text must be valid. For example: “13965280 9ZZ5”.
Portuguese Document Number Near Term	Detects valid 12-digit Portuguese Document Numbers or 11-digit numbers where the leftmost digit, “0”, is omitted near a support term in Portuguese or English. For example: “n documento 13965280 9ZZ5”.
Portuguese Social Security Number (Wide)	Detects valid 11-digit Social Security Numbers (NISS). For example: “25092822330”.
Portuguese Social Security Number (Default)	Detects valid 11-digit Social Security Numbers (NISS). At least 30% of the 11-digit numbers in the text must be valid. For example: “25092822330”.
Portuguese Social Security Number Near Term	Detects valid 11-digit Social Security Numbers (NISS) near a support term in Portuguese or English. For example: “NISS 25092822330”.
Portuguese Tax Identification Number of Individuals (Wide)	Detects valid 9-digit Portuguese Tax Identification Numbers (NIF) of Individuals. For example: “113469160”.
Portuguese Tax Identification Number of Individuals (Default)	Detects valid 9-digit Portuguese Tax Identification Numbers (NIF) of Individuals. At least 30% of the 9-digit numbers in the text must be valid. For example: “113469160”.

Classifier	Description
Portuguese Tax Identification Number of Individuals Near Term	Detects valid 9-digit Portuguese Tax Identification Numbers (NIF) of Individuals near a support term in Portuguese or English. For example: “N.I.F. 113469160”.
PRC Business Registration Numbers - 15 digits (default)	Detection of People's Republic of China's 15 digits Business Registration Numbers (default behavior).
PRC Business Registration Numbers - 15 digits (narrow)	Detection of People’s Republic of China’s 15 digits Business Registration Numbers (narrow behavior).
PRC Business Registration Numbers - 15 digits (wide)	Detection of People’s Republic of China’s 15 digits Business Registration Numbers (wide behavior).
Proximity Classifier	This classifier is looking for two elements in proximity (determined by the user) to each other. Classifier has three parameters as input. “First Element” and “Second Element” determines the values to be searched, you can write a keyword or a regexp. The parameter “Proximity In Characters” determines the number of characters to look before and after matches of first element.
Python Source Code (Wide)	Detection of Python source code. At least 50 percent of the non-empty lines in the file should be valid Python lines and at least 1 unmistakable Python line should be detected.
Python Source Code (Default)	Detection of Python source code. At least 70 percent of the non-empty lines in the file should be valid Python lines and at least 4 unmistakable Python lines should be detected.
Questionable Image	Detection of nudity images.
Romania - ID	Detection of validated Romanian ID numbers.
Routing Number (Default)	Detection of issued RTNs, includes advanced statistical heuristics.
Routing Number (Narrow)	Detection of issued RTNs, includes advanced statistical heuristics and search for support terms.
Routing Number (Wide)	Detection of issued RTNs.
Russian Classification on Objects of Administrative Division (with check digit)	Detection of Russian Classification on Objects of Administrative Division (with check digit).
Russian Classification on Objects of Administrative Division (without check digit)	Detection of Russian Classification on Objects of Administrative Division (without check digit).
Russian Personal Pension Account Number (SNILS)	Detection of Russian Individual personal pension account numbers (SNILS).
Russian Moscow Social Card number (SOCCARD)	Detection of Russian Moscow Social Card (SOCCARD)

Classifier	Description
Russian Moscow Social Card serial number	Detection of Russian Moscow Social Card (SOCCARD)
Russian Names (Default)	Detection of Russian full names.
Russian Names (Narrow)	Detection of Russian full names.
Russian Names (Wide)	Detection of Russian full names.
Russian Passport Spreadsheet	Detection of Russian passport numbers in spreadsheet files.
Russian Primary State Registration numbers (13 digits)	Detection of 13 digits Russian Primary State Registration numbers
Russian Primary State Registration numbers (15 digits)	Detection of 15 digits Russian Primary State Registration numbers
Russian Taxpayer Identification numbers validator (10 digits)	Detection of 10 digits Russian Taxpayer Identification numbers
Russian Taxpayer Identification numbers validator (12 digits)	Detection of 12 digits Russian Taxpayer Identification numbers
Russian Unified Classifier of Enterprises and Organizations	Detection of Russian Unified Classifier of Enterprises and Organizations number.
Security Accounts Manager (SAM) Files	Detection of SAM files according to internal file properties.
Security Accounts Manager (SAM) Files - Textual (Wide)	Detection of SAM textual files.
Security Accounts Manager (SAM) Files - Textual (Default)	Detection of SAM textual files. All lines in the file should be valid hash lines. Characters statistical analysis is used when parts of a string are repeated, indicating the likelihood of an unintended match.
Security Accounts Manager (SAM) Files - Textual (Narrow)	Detection of SAM textual files. All lines in the file should be valid hash lines. At least 4 lines are needed in order to have a match. Characters statistical analysis is used when parts of a string are repeated, indicating the likelihood of an unintended match.
Shadow Files	Detection of shadow files
Shadow Files (Wide)	Detection of shadow files
SIN (Default)	Detection of valid Canadian social insurance numbers, employing context sensitive lexical analysis, statistical analysis of patterns and custom dictionaries.
SIN (Narrow)	Restricted detection of valid Canadian social insurance numbers, tuned in order to minimize false positives. Requires additional evidence, such as SIN related terms (English or French) in proximity.

Classifier	Description
SIN (Wide)	Permissive detection of valid Canadian social insurance numbers. Does not require support term in proximity.
SIN: with proximity	Detection of valid Canadian social insurance numbers, in proximity to social insurance related terms in English or French.
Singapore Addresses (Default)	Detection of Singapore addresses
Singapore Addresses (Narrow)	Detection of Singapore addresses in the most formal form
Singapore ID	Detection of Singapore NRIC, UIN and FIN identification numbers. Does not require identification related terms in proximity.
Singapore ID with support	Detection of Singapore NRIC, UIN and FIN identification numbers, in proximity to identification related terms.
Singaporean Phone Numbers (Default)	Detection of Singaporean phone numbers.
Singaporean Phone Numbers (Narrow)	Detection of Singaporean phone numbers, employing statistical analysis.
Slovak and Czech Birth Numbers Near Term	Detects valid 9- or 10-digit delimited or un-delimited Slovak and Czech birth numbers (Rodne Cislo) near a support term. For example “Rodne Cislo 8501306605”.
Slovak and Czech Birth Numbers (Wide)	Detects valid 9- or 10-digit delimited or un-delimited Slovak and Czech birth numbers (Rodne Cislo). For example “450819001”.
Source Code: C or JAVA	Detection of source code content written in C, C++, C# or Java, using lexical analysis of terms, patterns and structures for optimal accuracy.
Source Code: C or JAVA (Wide)	Detection of files which are suspicious to be a source code content - written in C, C++, C# or Java, using lexical analysis of terms, patterns and structures.
Source Code: Verilog	Detection of Verilog source code, using lexical analysis of terms, patterns and structures for optimal accuracy.
South Africa ID Number (Default)	Detection of valid 13-digit South African ID numbers. At least 30% of the 13-digit numbers in the text must be valid. For example: "2001014800086".
South Africa ID Number (Near Term)	Detection of valid 13-digit South African ID numbers near a support term in English. For example: "ID number 2001014800086".
South Africa ID Number (Wide)	Detection of valid 13-digit South African ID numbers. For example: "2001014800086".
South Korea ID	Detection of validated South Korea ID in a form like dddddd-ddddddd.
South Korea ID - Wide	Detection of validated South Korea ID, both delimited and non-delimited.
Spain: DNI Number	Detection of Spain DNIs, in proximity to related terms.

Classifier	Description
Spain: DNI Number (Wide)	Detection of Spain DNIs.
Spanish Address	Detection of Spanish addresses composed of address support terms in English or Spanish and a house number.
Spanish Passports	Detection of Spanish Passport numbers (2 letters preceded by 6 numbers) with a support term in proximity.
Spanish Phone Numbers	Detection of Spanish Phone Numbers with 9 or 11 digits, start with 6 or 9 for 9 digits, and 346 or 349 for 11 digits. Supported delimitations are in the following format: ddd-ddd-ddd, ddd ddd ddd, ddddddddd, dd-ddd-ddd-ddd, dd ddd ddd ddd, or ddddddddddd.
Spanish Phone Numbers (Wide)	Detection of Spanish Phone Numbers with 9 or 11 digits, start with 6 or 9 for 9 digits, and 346 or 349 for 11 digits. Supported delimitations are in the following format: ddd-ddd-ddd, ddd ddd ddd, ddddddddd, dd-ddd-ddd-ddd, dd ddd ddd ddd, or ddddddddddd. Note: This classifier may cause false positive and not recommended for use.
Spanish Social Security Number (Default)	Detects valid 12-digit Social Security Numbers (NUSS). At least 30% of the 12-digit numbers in the text must be valid. For example: "28 10497854 66".
Spanish Social Security Number (Wide)	Detects valid 11- or 12-digit Social Security Numbers (NUSS). For example: "28 10497854 66".
Spanish Social Security Number (Near Term)	Detects valid 11- or 12-digit Social Security Numbers (NUSS). near a support term in Spanish or English. For example: "Numero de Seguridad Social 28 10497854 66".
SPSS data files: sps	Detection of SPSS (.sps) text files.
SQL Detection (Default)	Detection of SQL queries (default behavior)
SQL Detection (Narrow)	Detection of SQL queries (narrow behavior)
SQL Detection (Wide)	Detection of SQL queries (wide behavior)
SSH2 Private Key	Detection of encrypted and non-encrypted SSH2 private keys. The first line of the key contains the string "BEGIN SSH2 PRIVATE KEY" or "BEGIN SSH2 ENCRYPTED PRIVATE KEY".
STL Textual Format	Detection of 3D Systems STL textual CAD files.
Suspected Mail to Self	Detection of similar names in the source and destination of email addresses. Should be used with an AND condition together with the relevant type of sensitive information.
Sweden ID - no support	Detection of validated Personal Identity Numbers, does not demand further evidence.
Swedish Names	Detection of Swedish full names.
Swedish Names (Narrow)	Detection of Swedish full names (Narrow).
Swedish Names (Wide)	Detection of Swedish full names (Wide). This content classifier should be used in conjunction with additional data because it is permissive.

Classifier	Description
Taiwan address (default)	Detection of Taiwan address (common street names and county names in English or Chinese) with address support term.
Taiwan address (narrow)	Detection of Taiwan address (common street names and county names in English or Chinese) with address support term in proximity.
Taiwan address (wide)	Detection of Taiwan address (common street names and county names in English or Chinese)
Taiwan ID	Detection of validated Taiwan ID of the form A123456789.
Taiwan ID with support	Detection of validated Taiwan ID of the form A123456789, providing that Taiwan ID terms in English or Chinese appears in proximity.
Taiwan PII: Birthday	Detection of Taiwan birthdays.
Taiwan PII: Marital Status	Detection of Taiwan marital status.
Taiwan PII: Passport Numbers	Detection of passport numbers.
Textual PPK Private Key	Detection of textual PPK private keys. The first line of the key contains the string "PuTTY-User-Key-File".
Thailand ID number (Default)	Detection of at least 1 Thai ID number with support terms.
Thailand ID number (Wide)	Detection of at least 1 Thai ID number without support terms.
Time Of Day - general 1	Return ‘True’ if the current time is after the time specified as the ‘from time’, and before the ‘to time’. The hours are configurable in the classifier’s parameters. You can update the from and to hours by editing the classifier. This classifier can be used to create a rule that is valid in the working hours as determined by the user.
Time Of Day - general 2	Return ‘True’ if the current time is after the time specified as the ‘from time’, and before the ‘to time’. The hours are configurable in the classifier’s parameters. You can update the from and to hours by editing the classifier. This classifier can be used to create a rule that is valid in the working hours as determined by the user.
Time Of Day - general 3	Return ‘True’ if the current time is after the time specified as the ‘from time’, and before the ‘to time’. The hours are configurable in the classifier’s parameters. You can update the from and to hours by editing the classifier. This classifier can be used to create a rule that is valid in the working hours as determined by the user.
Time Of Day - Outside Working Hours	Return ‘True’ if the current time falls between the times specified as Outside working hours (the default values for Outside working hours are from 5 PM to 8 AM). The hours are configurable in the classifier’s parameters. This classifier can be used to create a rule that is valid in the working hours as determined by the user.

Classifier	Description
Time Of Day - Working Hours	Return ‘True’ if the current time falls between the times specified as working hours (the default values for working hours are from 8 AM to 5 PM). The hours are configurable in the classifier’s parameters. This classifier can be used to create a rule that is valid in the working hours as determined by the user.
Turkey PII in Spreadsheets	Detection of spreadsheets containing Turkish personally identifiable information (PII) by looking for column headers related to information such as full name, address, citizenship number, etc.
Turkey TC Kimlik	Detection of validated Turkish Citizenship numbers (TC Kimlik), when appearing in proximity to TC Kimlik related terms in English, Turkish and other European languages.
Turkey TC Kimlik (Wide)	Detection of validated Turkish Citizenship numbers (TC Kimlik).
Turkey TC Kimlik (Wide)	Detection of validated Turkish Citizenship numbers (TC Kimlik).
Turkish Tax IDs	Detection of validated Turkish Tax ID Numbers given by government to persons or companies.
UK Driver Number (Default)	Detection of UK Driver Numbers with support terms.
UK Driver Number (Wide)	Detection of UK Driver Numbers.
UK Names (Default)	Detection of UK full names.
UK Names (Narrow)	Detection of UK full names (Narrow).
UK Names (Wide)	Detection of UK full names (Wide). This content classifier should be used in conjunction with additional data as it is permissive.
UK Voter Number	Detection of UK electoral roll numbers in proximity to related terms.
Uncategorized URL Detection	Detection of uncategorized or suspicious destination URLs. This uses the URL categories list. Applies only when Forcepoint Web Security and Linking Service are installed.
Unencrypted PKCS #8 Private Key	Detection of unencrypted PKCS #8 private keys. The first line of the key contains the string "BEGIN PRIVATE KEY".
Union Pay Credit Cards (Default)	Detection of Union Pay credit card numbers employing various heuristics involving credit card related terms and use of delimiters. By default, only the first 4 digits and the last 4 digits are shown in the reports.
Union Pay Credit Cards (Narrow)	Detection of Union Pay credit card numbers. Requires additional evidence, such as credit card related terms in proximity, in order to qualify number as a credit card number. By default, only the first 4 digits and the last 4 digits are shown in the reports.

Classifier	Description
Union Pay Credit Cards (Wide)	Detection of potential Union Pay credit card numbers, based only on format and validation, may cause false-positives. By default, only the first 4 digits and the last 4 digits are shown in the reports.
Unique Master Citizen Number (Wide)	Detects valid 13-digit Unique Master Citizen Numbers. For example “0801977505006”.
Unique Master Citizen Number (Default)	Detects valid 13-digit Unique Master Citizen Numbers. At least half of the 13-digit numbers in the text need to be valid. For example “0801977505006”.
Unique Master Citizen Number Near Term	Detects valid 13-digit Unique Master Citizen Numbers near a support term. For example “Unique Master Citizen Number 0801977715000”.
Unusual Hours	Detects the transaction time as ‘unusual hour’ if the current time falls between the times specified as parameters for this classifier. The default values for unusual hours are from 21:00 (9 PM) to 5:00 (5 AM). The ‘First working day’ and ‘Last working day’ define the working day range. Transactions that are out of the working days are detected by this classifier regardless of their time.
URL category detection	Uses the inspected URL category as a classifier in the rule’s condition.
US Address	Detection of US address.
US Names - default	Detection of full names.
US Names - narrow	Detection of full names (Narrow).
US Names - wide	Detection of full names (Wide). This content classifier should be used in conjunction with additional data as it is permissive.
US Passport Number Near Term (Default)	Detects US passport numbers or passport card numbers, near a term in English or Spanish. US passport numbers are 9 digits and passport card numbers consist of the letter "C" followed by 8 digits. For example, "Passport number: 340020014".
US Passport Number Near Term (Wide)	Detects case-insensitive US passport numbers or passport card numbers, near a permissive term in English or Spanish. US passport numbers are 9 digits and passport card numbers consist of the letter "C" followed by 8 digits. For example, "Passport: 340020014".
US Phone Numbers	Detection of US phone numbers.
US SSN (Audit)	A permissive classifier for detecting potential social security numbers, possibly with a non-standard delimitation or without definite boundaries. For example, if the string “aaa145-22-5-6-7-8” appears in a single line, it produces a match. This classifier can cause many false positives.
US SSN - Wide Minus Default	Permissive detection of all delimitation forms of valid social security numbers that have been issued by the US Social Security Administration, taking into account SSN randomization. Detects all SSNs that belong to “wide” sensitivity and not to “default.”

Classifier	Description
US SSN (Default)	Detection of valid social security numbers that have been issued by the US Social Security Administration, taking into account SSN randomization, employing context sensitive lexical analysis, statistical analysis of patterns and custom dictionaries.
US SSN (Narrow)	Restricted detection of valid social security numbers, which have been issued by the US Social Security Administration, taking into account SSN randomization, tune in order to minimize false-positives. Requires additional evidences, such as SSN related terms in proximity.
US SSN (Wide)	Permissive detection of all delimitation forms of valid social security numbers that have been issued by the US Social Security Administration, taking into account SSN randomization.
US SSN: not-masked	Detection of valid social security numbers that have been issued by the US Social Security Administration, taking into account SSN randomization, context-sensitive lexical analysis, statistical analysis of patterns, and custom dictionaries. The returned values of this classifier are not masked.
US SSN in Form W-2	Detection of a US social security number in Form W-2.
User-defined file types extension	Detection of specific file types (user-defined) according to their extension.
VIN Code (Default)	Detection of Vehicle Identification Number (VIN) Code in proximity to a VIN-related term, such as ‘Vehicle Identification Number’ (default behavior)
VIN Code (Wide)	Detection of Vehicle Identification Number (VIN) Code - ‘wide’ behavior
Visual Basic (Default)	Detection of Visual Basic Source Code - “default” behavior.
Visual Basic (Narrow)	Detection of Visual Basic Source Code - “narrow” behavior.
Visual Basic (Wide)	Detection of Visual Basic Source Code - “wide” behavior.
W2 Form Support	Detection of IRS W2 forms
x86 Assembly Source Code	Detection of x86 Assembly Source Code.

Dictionaries

This section contains the full list of industry-related dictionaries provided by Forcepoint. You can also create new classifiers. For information, see Adding a dictionary classifier.

Dictionary	Description
401(k) form terms	Detection of 401(k) form terms.
403(b) form terms	Detection of 403(b) form terms.
Adult (Chinese)	Detection of Sexually Explicit, Adult-Oriented terms
Adult (Dutch)	Detection of Sexually Explicit, Adult-Oriented terms
Adult (English)	Detection of Sexually Explicit, Adult-Oriented terms
Adult (French)	Detection of Sexually Explicit, Adult-Oriented terms
Adult (German)	Detection of Sexually Explicit, Adult-Oriented terms
Adult (Italian)	Detection of Sexually Explicit, Adult-Oriented terms
Adult (Japanese)	Detection of Sexually Explicit, Adult-Oriented terms
Adult (Portuguese)	Detection of Sexually Explicit, Adult-Oriented terms
Adult (Russian)	Detection of Sexually Explicit, Adult-Oriented terms
Adult (Spanish)	Detection of Sexually Explicit, Adult-Oriented terms
Adult (Taiwanese)	Detection of Sexually Explicit, Adult-Oriented terms
Adult (Turkish)	Detection of Sexually Explicit, Adult-Oriented terms
Afrikaans first names	Detection of Afrikaans first names
Afrikaans: Crimes	Detection of names of crimes in Afrikaans.
AHV support	Detection of AHV number support terms.
Arabic First Names	Detection of Arabic first names.
Arabic Last Names	Detection of Arabic last names.
Australian racial or ethnic origins	Detects names of Australian races and ethnicities. This dictionary includes dozens of names. For example: Asian, Chinese, Koori.
Belgium: ID Card Number Terms	Detection of Belgium ID terms
Belgium: Passport Terms	Detection of Belgium passport terms
Bids and Tenders	Detection of bids, proposals, and tenders, such as responses to request for proposal (RFP) and invitation for bids (IFB) documents.

Dictionary	Description
Biometric Information support terms in English and Hindi	Detection of India Biometric Information support terms in English and Hindi.
Brazil: Diseases	Detection of Brazilian sensitive health condition in Portuguese or in English.
Canadian Government ID Terms	Detection of Canadian Government ID terms such as “Canadian Government ID”.
Canadian Indian Status Terms	Detection of Canadian Indian Status support terms such as “Indian Status”.
Canadian Permanent Resident Terms	Detection of Canadian Permanent Resident support terms such as “Permanent Card”.
Celebrities	Detection of names of celebrities: famous actresses, sports, Nobel prize winners etc.
Chinese Financial Terms - unique count	Detection of Chinese financial terms (unique count).
Clinical Trials	Detection of terms common in clinical trials information.
Clinical Trials Confidential	Detection of terms that indicate confidential documents.
Common Diseases (Afrikaans)	Detection of common diseases or health issues in Afrikaans language.
Common Diseases (Hindi)	Detection of common diseases or health issues in Hindi language.
Common Medical Conditions (English)	Detection of common diseases or health issues.
Common hashed passwords	Detection of common hashed passwords.
Common salted passwords	Detection of common salted passwords.
Computer Hacking (Dutch)	Detection of common computer hacking terms
Computer Hacking (English)	Detection of common computer hacking terms
Computer Hacking (German)	Detection of common computer hacking terms
Computer Hacking (Japanese)	Detection of common computer hacking terms
Computer Hacking (Portuguese)	Detection of common computer hacking terms
Computer Hacking (Russian)	Detection of common computer hacking terms
Computer Hacking (Spanish)	Detection of common computer hacking terms
Confidential (Chinese)	Detection of the terms that indicate confidentiality such as “secret”, “private”, or “confidential”
Confidential (Dutch)	Detection of the terms that indicate confidentiality such as “secret”, “private”, or “confidential”

Dictionary	Description
Confidential (English)	Detection of the terms that indicate confidentiality such as “secret”, “private”, or “confidential”
Confidential (French)	Detection of the terms that indicate confidentiality such as “secret”, “private”, or “confidential”
Confidential (German)	Detection of the terms that indicate confidentiality such as “secret”, “private”, or “confidential”
Confidential (Japanese)	Detection of the terms that indicate confidentiality such as “secret”, “private”, or “confidential”
Confidential (Portuguese)	Detection of the terms that indicate confidentiality such as “secret”, “private”, or “confidential”
Confidential (Russian)	Detection of the terms that indicate confidentiality such as “secret”, “private”, or “confidential”
Confidential (Spanish)	Detection of the terms that indicate confidentiality such as “secret”, “private”, or “confidential”
Confidential (Taiwanese)	Detection of the terms that indicate confidentiality such as “secret”, “private”, or “confidential”
Controlled Drugs	Detection of Controlled-drugs according to 21 CFR chapter III section 1308.
Credit File (Wide)	Detects Credit Files. Looks for words that usually describe credit files with a Wide filter.
Credit File (Default)	Detects Credit Files. Looks for words that usually describe credit files with a Default filter.
Credit File (Narrow)	Detects Credit Files. Looks for words that usually describe credit files with a Narrow filter.
CUSIP Support terms	Detection of CUSIP related terms.
CV in Russian or Ukrainian support terms	Detection of a Curriculum Vitae in Russian or Ukrainian with support terms.
CV and Resume in French	Detection of resumes and CVs in French.
CV and Resume in German	Detection of resumes and CVs in German.
CV and Resume in Spanish	Detection of resumes and CVs in Spanish.
CV and Resume Terms in Hebrew	Detection of resume and CV terms in Hebrew.
Denmark: CPR terms (narrow)	Detection of Danish CPR narrow terms.
Denmark: CPR terms (wide)	Detection of Danish CPR wide terms.
Denmark: First Name	Detection of Danish first names.
Denmark: Last Name	Detection of Danish last names.
DNA support	Detection of DNA support terms.
Driver License Terms of the Netherlands	Detection of Driver License Terms of the Netherlands.

Dictionary	Description
Driver License: Ireland support	Detection of Ireland DL number support terms.
EAR - Encryption Terms	Detection of encryption related terms - ‘wide’ behavior
EAR - Laser and microelectronics	Detection of information pertaining Laser and microelectronics. May cause false positives.
EAR - Microorganisms and Toxins	Detection of information pertaining Microorganisms and Toxins. May cause false positives.
EAR - Military Terms	Detection of military related terms - ‘wide’ behavior
EAR - Nuclear Terms	Detection of nuclear related terms - ‘wide’ behavior
EAR - Space Terms	Detection of space related terms - ‘wide’ behavior
EIN support terms	Detection of EIN related terms.
Energy (dictionary): Prospecting Terms (High)	Detection of interesting prospecting terms (high severity).
Energy (dictionary): Prospecting Terms (Low)	Detection of interesting prospecting terms (low severity).
Energy (dictionary): Prospecting Terms (Medium)	Detection of interesting prospecting terms (medium severity).
Female Arabic names	Detection of Arabic female names.
Ferc: Disclaimer	Detection of FERC do-not-release disclaimer.
Ferc: Form 567	Detection of terms related to FERC form 567 - Annual Report Of System Flow Diagrams and Capacity.
Ferc: Form 567 support	Detection of “form 567” strings.
Ferc: Form 715	Detection of terms related to FERC form 715 - Annual Transmission Planning and Evaluation Report.
Ferc: Form 715 support	Detection of “form 715” strings.
Ferc: Pipeline Flow	Detection of terms related to FERC Natural gas pipeline flow diagrams and associated information.
Ferc: Pipeline support	Detection of terms related to FERC Natural gas pipeline flow diagrams and associated information.
Finance (Dutch)	Detection of terms related to finance
Finance (English)	Detection of terms related to finance
Finance (French)	Detection of terms related to finance
Finance (German)	Detection of terms related to finance
Finance (Italian)	Detection of terms related to finance
Finance (Japanese)	Detection of terms related to finance
Finance (Portuguese)	Detection of terms related to finance
Finance (Russian)	Detection of terms related to finance
Finance (Spanish)	Detection of terms related to finance

Dictionary	Description
Finance (Taiwanese)	Detection of terms related to finance
Financial General: Common	Detection of common terms related to general financial data.
Financial General: Non-Unique	Detection of non-unique terms related to general financial data.
Financial General: Unique	Detection of unique terms related to general financial data.
Financial Investment: Common	Detection of common terms related to stocks, bonds, options, and other types of investment related financial data.
Financial Investment: Non-Unique	Detection of non-unique terms related to stocks, bonds, options, and other types of investment related financial data.
Financial Investment: Unique	Detection of unique terms related to stocks, bonds, options, and other types of investment related financial data.
Financial Personal: Common	Detection of common terms related to financial transactions, credit history, financial status, and other personal financial data.
Financial Personal: Non-Unique	Detection of non-unique terms related to financial transactions, credit history, financial status, and other personal financial data.
Financial Personal: Unique	Detection of unique terms related to financial transactions, credit history, financial status, and other personal financial data.
Financial Terms	Detection of financial terms.
Finnish SSN support terms	Detection of Finnish SSN support terms.
Form 1040/Form 1040A Terms	Detection of terms found in Form 1040 and Form 1040A (“U.S. Individual Income Tax Return”).
Form 1040EZ Terms	Detection of terms found in Form 1040EZ (“Income Tax Return for Single and Joint Filers with No Dependents”).
Form W-9 Terms	Detection of English and Spanish terms found in Form W-9 (“Request for Taxpayer Identification Number and Certification”).
Form W-9S Terms	Detection of terms found in Form W-9S (“Request for Student’s or Borrower’s Taxpayer Identification Number and Certification”).
Form W-2 Terms	Detection of terms taken from the Form W-2 (“Wage and Tax Statement”).
Form W-4 Terms	Detection of English and Spanish terms found in Form W-4 (“Employee’s Withholding Allowance Certificate”).
Form W-4P Terms	Detection of terms found in Form W-4P (“Withholding Certificate for Pension or Annuity Payments”).
Form W-4V Terms	Detection of terms found in Form W-4V (“Voluntary Withholding Request”).
France: Diseases	Detection of sensitive health condition in French or in English.
Gambling (Chinese)	Detection of Tips, Terms, Online Casinos, Betting Pools

Dictionary	Description
Gambling (Dutch)	Detection of Tips, Terms, Online Casinos, Betting Pools
Gambling (English)	Detection of Tips, Terms, Online Casinos, Betting Pools
Gambling (French)	Detection of Tips, Terms, Online Casinos, Betting Pools
Gambling (German)	Detection of Tips, Terms, Online Casinos, Betting Pools
Gambling (Italian)	Detection of Tips, Terms, Online Casinos, Betting Pools
Gambling (Japanese)	Detection of Tips, Terms, Online Casinos, Betting Pools
Gambling (Portuguese)	Detection of Tips, Terms, Online Casinos, Betting Pools
Gambling (Russian)	Detection of Tips, Terms, Online Casinos, Betting Pools
Gambling (Spanish)	Detection of Tips, Terms, Online Casinos, Betting Pools
Gambling (Taiwanese)	Detection of Tips, Terms, Online Casinos, Betting Pools
Gambling (Turkish)	Detection of Tips, Terms, Online Casinos, Betting Pools
Germany: Crimes	Detection of name of a crime, in German or English.
Germany: Diseases	Detection of sensitive health condition in German or in English.
Germany: Ethnicities	Detection of name of a race or ethnicity, in German or English.
Greek Sensitive Diseases	Detection of Greek names of a diseases.
Hate Speech/Offensive (Chinese)	Detection of Prejudice based on Race, Gender, Religion, etc.
Hate Speech/Offensive (Dutch)	Detection of Prejudice based on Race, Gender, Religion, etc.
Hate Speech/Offensive (English)	Detection of Prejudice based on Race, Gender, Religion, etc.
Hate Speech/Offensive (French)	Detection of Prejudice based on Race, Gender, Religion, etc.
Hate Speech/Offensive (German)	Detection of Prejudice based on Race, Gender, Religion, etc.
Hate Speech/Offensive (Italian)	Detection of Prejudice based on Race, Gender, Religion, etc.
Hate Speech/Offensive (Japanese)	Detection of Prejudice based on Race, Gender, Religion, etc.
Hate Speech/Offensive (Portuguese)	Detection of Prejudice based on Race, Gender, Religion, etc.
Hate Speech/Offensive (Russian)	Detection of Prejudice based on Race, Gender, Religion, etc.
Hate Speech/Offensive (Spanish)	Detection of Prejudice based on Race, Gender, Religion, etc.
Hate Speech/Offensive (Taiwanese)	Detection of Prejudice based on Race, Gender, Religion, etc.

Dictionary	Description
Hate Speech/Offensive Turkish)	Detection of Prejudice based on Race, Gender, Religion, etc.
Health (Chinese)	Detection of health terms
Health (English)	Detection of health terms
Health (Japanese)	Detection of health terms
Health (Russian)	Detection of health terms
Health (Taiwanese)	Detection of health terms
Health Information Dictionary (Swedish)	Detection of sensitive health conditions in Swedish or in English.
Hong Kong: ID - support	Detection of Hong Kong ID related terms.
Hungary CNP Terms	Detection of Hungary Personal Numeric Codes terms
Hungary SSN Terms	Detection of Hungary Social Security Number support terms
Hungary Tax ID Terms	Detection of Hungary Tax ID Number support terms
ICD Descriptions (Swedish, English)	Detection of Swedish/English descriptions of medical conditions as they appear in the ICD10 manual.
ICD9 Descriptions	Detection of ICD9 Descriptions.
ICD9 Codes Support Terms	Detection of ICD9 codes support terms.
ID support	Detection of ID number support terms.
Illegal & Controlled Drugs (Chinese)	Detection of Instructions, Products, Terms, Promotion
Illegal & Controlled Drugs (Dutch)	Detection of Instructions, Products, Terms, Promotion
Illegal & Controlled Drugs (English)	Detection of Instructions, Products, Terms, Promotion
Illegal & Controlled Drugs (French)	Detection of Instructions, Products, Terms, Promotion
Illegal & Controlled Drugs (German)	Detection of Instructions, Products, Terms, Promotion
Illegal & Controlled Drugs (Italian)	Detection of Instructions, Products, Terms, Promotion
Illegal & Controlled Drugs (Japanese)	Detection of Instructions, Products, Terms, Promotion
Illegal & Controlled Drugs (Portuguese)	Detection of Instructions, Products, Terms, Promotion
Illegal & Controlled Drugs (Russian)	Detection of Instructions, Products, Terms, Promotion
Illegal & Controlled Drugs (Spanish)	Detection of Instructions, Products, Terms, Promotion
Illegal & Controlled Drugs (Taiwanese)	Detection of Instructions, Products, Terms, Promotion

Dictionary	Description
Illegal & Controlled Drugs (Turkish)	Detection of Instructions, Products, Terms, Promotion
IMEI - support terms	Detection of IMEI related terms.
India PAN support	Detection of India PAN related terms.
Investment (dictionary): Common	Detection of common terms related to stocks, bonds, options, and other types of investment financial data.
Investment (dictionary): Non-Unique	Detection of non-unique terms related to stocks, bonds, options, and other types of investment financial data.
Investment (dictionary): Unique	Detection of unique terms related to stocks, bonds, options, and other types of investment financial data.
Ireland: Passport support	Detection of Ireland passport number support terms.
ISIN CAM support	Detection of 'CAM' strings.
ISIN support	Detection of ISIN related terms.
Italy: Diseases	Detection of sensitive health condition in Italian or in English.
Japanese Surnames	Detection of Japanese surnames (ASCII and Unicode)
Job Search (Chinese)	Detection of Employment Agencies, Job Listings, Career Searches
Job Search (Dutch)	Detection of Employment Agencies, Job Listings, Career Searches
Job Search (English)	Detection of Employment Agencies, Job Listings, Career Searches
Job Search (French)	Detection of Employment Agencies, Job Listings, Career Searches
Job Search (German)	Detection of Employment Agencies, Job Listings, Career Searches
Job Search (Italian)	Detection of Employment Agencies, Job Listings, Career Searches
Job Search (Japanese)	Detection of Employment Agencies, Job Listings, Career Searches
Job Search (Portuguese)	Detection of Employment Agencies, Job Listings, Career Searches
Job Search (Russian)	Detection of Employment Agencies, Job Listings, Career Searches
Job Search (Spanish)	Detection of Employment Agencies, Job Listings, Career Searches
Job Search (Taiwanese)	Detection of Employment Agencies, Job Listings, Career Searches
Job Search (Turkish)	Detection of Employment Agencies, Job Listings, Career Searches

Dictionary	Description
Kazakh Taxpayer Registration Number Support Terms	Detection of Kazakh Taxpayer Registration Number Support Terms.
Kazakh Individual Identification Number Support Terms	Detection of Kazakh Individual Identification Number Support Terms.
Kazakh Business Identification Number Support Terms	Detection of Kazakh Business Identification Number Support Terms.
Macau ID - support	Detection of Macau ID related terms.
Malay: Crimes	Detection of crimes in Malay.
Malaysia: Ethnicities	Detection of Malayan ethnicities.
Malaysia: Names	Detection of Arabic names and Chinese surnames. For example: “Nurul”.
Male Arabic names	Detection of Arabic male names.
Medical form	Detection of medical forms.
Mergers and Acquisitions: Common	Detection of common Mergers and Acquisitions terms.
Mergers and Acquisitions: Non-Unique	Detection of non-unique Mergers and Acquisitions terms.
Mergers and Acquisitions: Unique	Detection of unique Mergers and Acquisitions terms.
Mexico CPISP Support Terms	Detection of Mexico CPISP Support Terms.
Mexico CURP Support Terms	Mexico CURP Support Terms.
Netherlands: Crimes	Detection of name of a crime, in Dutch or English.
Netherlands: Diseases	Detection of sensitive health condition in Dutch or in English.
Netherlands: Ethnicities	Detection of Dutch name of a race or ethnicity, in Dutch or English.
New Zealand: NHI support	Detection of NHI Numbers related terms.
NHS numbers (support)	Detection of NHS related terms.
Non Acceptable Use - Arabic	Detection of usage of inappropriate or unacceptable language in Arabic, in Hebrew letters.
Non Acceptable Use - Hebrew	Detection of usage of inappropriate or unacceptable language in Hebrew, in Hebrew and English letters.
Non Acceptable Use - Iraqi	Detection of usage of inappropriate or unacceptable language in Iraqi, in Hebrew letters.
Non Acceptable Use - Russian	Detection of usage of inappropriate or unacceptable language in Russian, in Hebrew and Russian letters.

Dictionary	Description
Non Acceptable Use (High)	Detection of high severity breach of Acceptable Use policy, with very explicit sexual terms or racial slurs.
Non Acceptable Use (Low)	Detection of low severity breaches of Acceptable Use policy, with inappropriate language which is not explicit.
Non Acceptable Use (Medium)	Detection of medium severity breach of Acceptable Use policy, with mostly sexually oriented slang terms in multiple languages.
Norway Personnummer Terms	Detection of Norway Personal Numbers (personnummer) related terms
Norway: Diseases	Detection of sensitive health condition in Norwegian or in English.
Norway: First Names	Detection of Norwegian first names.
Norway: Last Names	Detection of Norwegian last names.
Passport Terms of the Netherlands	Detection of Passport Terms of the Netherlands.
Patents (dictionary) Support Terms	Detection of patent related terms.
Patents (dictionary): Common	Detection of common patent terms.
Patents (dictionary): Support	Detection of terms to support detection of patent applications.
Philippines: First Names	Philippines - First Names dictionary
Philippines: First or Last Name	Detection of Philippine first or last name. For example: “Nicole”.
Philippines: Last Names	Philippines - Last Names dictionary
Physical Personal Terms (English/Hindi)	Detection of physical personal terms such as “Personal Data” and “Physical Characteristics”.
Poland: IBAN support	Detection of Poland IBAN number support terms.
Poland: PESEL support	Detection of Poland PESEL number support terms.
Poland: REGON support	Detection of Poland REGON number support terms.
Pricing Support terms	Detection of terms to support detection of pricing information.
Pricing Support terms (Wide)	Detection of terms to support detection of pricing information.
Protein Sequence Support Terms	Detection of Protein Sequence Support Terms.
Romania ID Terms	Detection of Romania ID support terms.
Russian Passport Terms	Detection of Russian passport related terms.
SCADA Terms	Dictionary supervisory control and data acquisition (SCADA) systems related terms

Dictionary	Description
Sensitive Diseases (Hindi)	Detection of name of a disease, drug or a medical condition which is of a sensitive nature in Hindi language.
Sensitive Diseases Dictionary (Swedish)	Detection of names of a disease, drug, or medical condition which are of a sensitive nature (Swedish/English)
Sexual Orientation terms	Detection of Sexual Orientation terms.
Sexual Orientation terms (Hindi)	Detection of Sexual Orientation terms in Hindi language.
Software Design: Common	Detection of common terms related to design requirements, software architecture, user interface, and other software design related data.
Software Design: Non-Unique	Detection of non-unique terms related to design requirements, software architecture, user interface, and other software design related data.
Software Design: Unique	Detection of unique terms related to design requirements, software architecture, user interface, and other software design related data.
Source Code: SPICE spectre	Detection of terms and reserved words in SPICE.
Source Code: Verilog Phrases	Detection of terms and reserved words in Verilog.
South Africa ethnicities	Detection of South African ethnicities
South Korea ID: support terms	Detection of South Korea ID number related terms.
SOX: Audit terms	Detection of SOX terms.
SOX: support	Detection of SOX terms.
Spain: Crimes	Detection of name of a crime, in Spanish or English.
Spain: Diseases	Detection of sensitive health condition in Spanish or in English.
Spain: Ethnicities	Detection of name of a race or ethnicity, in Spanish or English.
Spanish First Names	Detection of Spanish first names
Spanish Last Names	Detection of Spanish last names
Spanish Municipalities	Detection of Spanish municipalities names.
Steganography applications	Detection of Steganography applications
Strategic Planning Terms	Detection of terms related to strategic planning.
Suicidal thoughts (Wide)	Detection of expressions that are indicative of suicidal thoughts. May cause false positives.
Support terms for Russian phone numbers	Detection of related terms to Russian Phone numbers.
Support terms for Russian Primary State Registration 13 digits numbers	Detection of related terms to Russian Primary State Registration 13 digits numbers

Dictionary	Description
Support terms for Russian Primary State Registration 15 digits numbers	Detection of related terms to Russian Primary State Registration 15 digits numbers
Support terms for Russian Classification on Objects of Administrative Division number	Detection of related terms to Russian Classification on Objects of Administrative Division numbers
Support terms for Russian Taxpayer Identification numbers	Detection of related terms to Russian Taxpayer Identification numbers
Support terms for Russian Unified Classifier of Enterprises and Organizations numbers	Detection of related terms to Russian Unified Classifier of Enterprises and Organizations numbers
Support terms for Singaporean phone numbers	Detection of related terms to Singaporean Phone numbers.
Sweden ID support	Detection of Sweden ID related terms.
Thailand ID Terms	Detection of Thai ID support terms.
Turkey TC Kimlik Terms	Detection of Turkey TC Kimlik terms.
Turkish Tax ID Support Terms	Detection of Turkish Tax Id support terms.
UK Postal Code Support Terms	Detection of UK postal code support terms.
UK Sort Code Support Terms	Detection of UK sort code support terms.
UK: Passport Number support	Detection of UK passport number support terms.
UK: Tax ID support	Detection of UK Tax ID number support terms.
US Ethnicities	Detection of US name of a race or ethnicity.
US Sensitive Diseases	Detection of name of a disease, drug or a medical condition which is of a sensitive nature.
US: Crimes	Detection of names of US crimes.
UTM Terms	Detection of UTM (Universal Transverse Mercator) coordinate system terms.
Vietnam CMND Number Support Terms	Detection of Vietnamese CMND number support terms.
Violence/Weapons (Chinese)	Detection of Advocation or depictions of violent acts
Violence/Weapons (Dutch)	Detection of Advocation or depictions of violent acts
Violence/Weapons (English)	Detection of Advocation or depictions of violent acts

Dictionary	Description
Violence/Weapons (French)	Detection of Advocation or depictions of violent acts
Violence/Weapons (German)	Detection of Advocation or depictions of violent acts
Violence/Weapons (Italian)	Detection of Advocation or depictions of violent acts
Violence/Weapons (Japanese)	Detection of Advocation or depictions of violent acts
Violence/Weapons (Portuguese)	Detection of Advocation or depictions of violent acts
Violence/Weapons (Russian)	Detection of Advocation or depictions of violent acts
Violence/Weapons (Spanish)	Detection of Advocation or depictions of violent acts
Violence/Weapons (Taiwanese)	Detection of Advocation or depictions of violent acts
Violence/Weapons (Turkish)	Detection of Advocation or depictions of violent acts
W-2 Form support terms 1	Detection of terms taken from the W-2 Form (Wage and Tax Statement).

Pattern classifiers

This list the predefined pattern classifiers. Administrators can also create new classifiers. For information, see Adding or editing a regular expression classifier.

Classifier	Description
.htpasswd File Name	Detection of file names associated with .htpasswd files.
.REG File	Detection of the content of .REG files (Windows Registry entries).
10 Digit Account Number with support	Detection of any 10 digit number in proximity to an account number support term (can be used for various account types as long as they are 10 digits).
5-8 Digit Account Number with support	Detection of any 5-8 digit number in proximity to an account number support term (can be used for various account types as long as they are 5-8 digits).
5-9 Digit Account Number	Detection of any 5-9 digit account numbers.
9 Digit Account Number with support	Detection of any 9 digit number in proximity to an account number support term (can be used for various account types as long as they are 9 digits).

Classifier	Description
Account 5 to 8 digits	Detection of 5-8 digit account numbers.
Account and Password	Detection of a 5-10 digit account number, in proximity to a password with a password related term next to it.
Account Number 5-9 digits, with Hebrew or English Support	Detection of any 5-9 digit account numbers, when found in proximity to account related terms in English or Hebrew.
Account Number 6-13 digits	Detection of 6-13 digit account numbers.
Account Number 6-13 digits near Account Number Terms in Hebrew and English	Detection of 6-13 digit account numbers, in proximity to account related terms in English or Hebrew.
Account Number Terms Hebrew and English Support	Detection of account terms in English or Hebrew.
Argentina Swift codes	Detection of SWIFT codes for Argentina major banks.
Australia Swift codes	Detection of SWIFT codes for Australia major banks.
Australia: Medicare	Detection of Australian Medicare numbers, each in proximity to Medicare related terms.
Australian Bank Account Numbers	Detects Australian bank account numbers. Looks for 6- to 10-digit numbers. For example: 1234567
Australian Bank Account support terms	Detects Australian bank account support terms. For example: Acc. no., account number
Austria Swift codes	Detection of SWIFT codes for Austria major banks.
Bahrain Swift codes	Detection of SWIFT codes for Bahrain major banks.
Base64/Hexadecimal Characters Block	Detection of a block of Base64 or Hexadecimal Characters.
Belgium Swift codes	Detection of SWIFT codes for Belgium major banks.
Belgium: Passports	Detection of Belgium passport numbers
Brazil Swift codes	Detection of SWIFT codes for Brazil major banks.
Brazil: RG Numbers Terms	Detection of RG (Registro Geral) related terms.
CAD igs text format	Detection of CAD igs text files
Canada Swift codes	Detection of SWIFT codes for Canada major banks.
Canadian Driver License Support	Detection of Canadian driver license support terms.
Canadian Government ID	Detection of Canadian Government IDs.
Canadian Indian Status	Detection of Canadian Indian Status Numbers.
Canadian Permanent Resident	Detection of Canadian Permanent Resident Numbers.
CCN support terms	Detection of credit card support terms.
Chile Swift codes	Detection of SWIFT codes for Chile major banks.
China Swift codes	Detection of SWIFT codes for China major banks.

Classifier	Description
Clinical Trial Numbers	Detection of numbers likely to appear in ‘Clinical Trial’ documents.
Colombia Swift codes	Detection of SWIFT codes for Colombia major banks.
Confidential Arabic Terms in Header/Footer	Detection of documents with terms in English or Arabic indicating confidentiality in the header or footer.
Confidential Header/Footer	Detection of documents with terms indicating confidentiality in the header or footer.
Credit Cards: Isracard support	Detection of Isracard Credit Card support terms (Hebrew and English).
CUI Banner Marking (Wide)	Detection of Controlled Unclassified Information (CUI) banner markings, including the case-insensitive phrases "CONTROLLED" or "CUI". For example: "Controlled".
CUI Banner Marking (Default)	Detection of Controlled Unclassified Information (CUI) banner markings. The classifier will be triggered by the case-insensitive terms "CONTROLLED" or "CUI" followed by category markings and/or limited dissemination control markings. For example: "CONTROLLED//SP-ADJ//FEDCON".
CUI Banner Marking in Header/Footer (Wide)	Detection of Controlled Unclassified Information (CUI) banner markings in the header or footer part of a file, including the case-insensitive phrases "CONTROLLED" or "CUI". For example: "Controlled". Header and footer are extracted as such for some OpenDocument and Microsoft Office file formats (.doc, .docx, .odp, .ods, .odt, .pptx, .xls, .xlsx).
CUI Banner Marking in Header/Footer (Default)	Detection of Controlled Unclassified Information (CUI) banner markings in the header or footer part of a file. The classifier will be triggered by the case-sensitive terms "CONTROLLED" or "CUI" or by the same case-insensitive terms, followed by category markings and/or limited dissemination control markings. For example: "CONTROLLED". Header and footer are extracted as such for some OpenDocument and Microsoft Office file formats (.doc, .docx, .odp, .ods, .odt, .pptx, .xls, .xlsx).
CUI Banner Marking in Header/Footer (Narrow)	Detection of Controlled Unclassified Information (CUI) banner markings in the header or footer part of a file. The classifier will be triggered by the case-insensitive terms "CONTROLLED" or "CUI", followed by category markings and/or limited dissemination control markings. For example: "CONTROLLED//SP-ADJ//FEDCON". Header and footer are extracted as such for some OpenDocument and Microsoft Office file formats (.doc, .docx, .odp, .ods, .odt, .pptx, .xls, .xlsx).
CUI Portion Marking (Wide)	Detection of Controlled Unclassified Information (CUI) portion markings, including the case-insensitive string "(CUI)". For example: "(cui)".

Classifier	Description
CUI Portion Marking (Default)	Detection of Controlled Unclassified Information (CUI) portion markings. The classifier will be triggered by parentheses containing the case-sensitive string "CUI" or by the case-insensitive string, followed by category markings and/or limited dissemination control markings. For example: "(CUI)".
CUI Portion Marking (Narrow)	Detection of Controlled Unclassified Information (CUI) portion markings. The classifier will be triggered by parentheses containing the case-insensitive term "CUI", followed by category markings and/or limited dissemination control markings. For example: "(CUI//SP-ADJ//FEDCON)".
Cyber Bullying	Detection of expressions that are indicative of cyber bullying.
Cypriot Tax Identification Code	Detects Cypriot tax identification codes. For example: “12000017M”.
Czech Republic Swift codes	Detection of SWIFT codes for Czech Republic major banks.
Date Of Birth without support term	Detection of possible dates of birth, without support terms.
Deep Web URLs: .i2p (Wide)	Detects URLs that appear in analyzed content such as textual documents or email messages and end with the .i2p pseudo-top-level domain. For example: The string “forum.i2p”.
Deep Web URLs: .i2p (Default)	Detects URLs that appear in analyzed content such as textual documents or email messages, begin with “http/s” and end with the .i2p pseudo-top-level domain. For example: The string “http://hosts.i2p”.
Deep Web URLs: .onion	Detects URLs that appear in analyzed content such as textual documents or email messages and end with the .onion pseudo-top-level domain designating an anonymous hidden service reachable via the Tor network. For example: The string “i4rx33ibdndtqayr.onion”.
Denmark Swift codes	Detection of SWIFT codes for Denmark major banks.
Disgruntled Employee	Detects expressions that are indicative of disgruntled employees. For example: “I hate my boss”, “I am miserable at my job”.
DNA pattern	Detection of DNA patterns.
Driver License Support	Detection of driver license support terms.
Driver License: Alaska	Detection of Alaska driver license.
Driver License: Alberta	Detection of Alberta driver license.
Driver License: Arizona	Detection of Arizona driver license.
Driver License: Arkansas	Detection of Arkansas driver license.
Driver License: Australia	Detection of Australian driver license.

Classifier	Description
Driver License: British Columbia	Detection of British Columbia driver license.
Driver License: California	Detection of California driver license.
Driver License: Canada all patterns	Detection of various Canadian driver license formats.
Driver License: Colorado	Detection of Colorado driver license.
Driver License: Connecticut	Detection of Connecticut driver license.
Driver License: Florida	Detection of Florida driver license.
Driver License: Georgia	Detection of Georgia driver license.
Driver License: Hawaii	Detection of Hawaii driver license number.
Driver License: Idaho	Detection of Idaho driver license.
Driver License: Illinois	Detection of Illinois driver license.
Driver License: Kansas	Detection of Kansas driver license number.
Driver License: Louisiana	Detection of Louisiana driver license.
Driver License: Maine	Detection of Maine driver license.
Driver License: Manitoba	Detection of Manitoba driver license.
Driver License: Maryland	Detection of Maryland driver license.
Driver License: Michigan	Detection of Michigan driver license.
Driver License: Minnesota	Detection of Minnesota driver license.
Driver License: Montana	Detection of Montana driver license.
Driver License: New Brunswick	Detection of New Brunswick driver license.
Driver License: New Hampshire	Detection of New Hampshire driver license.
Driver License: New Jersey	Detection of New Jersey driver license.
Driver License: New York	Detection of New York driver license.
Driver License: Newfoundland and Labrador	Detection of Newfoundland and Labrador driver license.
Driver License: North Carolina	Detection of North Carolina driver license.
Driver License: Nova Scotia	Detection of Nova Scotia driver license.
Driver License: Ohio	Detection of Ohio driver license.
Driver License: Oklahoma	Detection of Oklahoma driver license.
Driver License: Ontario	Detection of Ontario driver license.
Driver License: Oregon	Detection of Oregon driver license.
Driver License: Pennsylvania	Detection of Pennsylvania driver license.

Classifier	Description
Driver License: Prince Edward Island	Detection of Prince Edward Island driver license.
Driver License: Quebec	Detection of Quebec driver license.
Driver License: Rhode Island	Detection of Rhode Island driver license.
Driver License: Saskatchewan	Detection of Saskatchewan driver license.
Driver License: Tennessee	Detection of Tennessee driver license.
Driver License: Texas	Detection of Texas driver license.
Driver License: US all patterns	Detection of various US driver license formats.
Driver License: US all patterns with Support	Detection of various US driver license formats, with support term in proximity.
Driver License: Washington	Detection of Washington driver license.
Driver License: Wisconsin	Detection of Wisconsin driver license.
EIN pattern	Detection of Employer ID Numbers (EIN).
Energy File Extensions	Detection of files containing petrophysical data.
Energy Logs and Survey Reports	Detection of terms related to Prospecting Logs and Survey Reports.
England Swift codes	Detection of SWIFT codes for England major banks.
Estonia Swift codes	Detection of SWIFT codes for Estonia major banks.
EU National Insurance Number	Detection of various European national insurance number formats (UK NINO, French INSEE, Spanish DNI, Italian Codice Fiscale).
F# Source Code Extensions	Detection of F# files according to their extension.
Finland Swift codes	Detection of SWIFT codes for Finland major banks.
Form 10-Q Phrases	Detection of Form 10-Q phrases.
Form W-2 Header	Detection of terms taken from the Form W-2 Header (e.g., “FORM W 2” or “Form W-2”).
France Swift codes	Detection of SWIFT codes for France major banks.
Germany Swift codes	Detection of SWIFT codes for Germany major banks.
Greece Swift codes	Detection of SWIFT codes for Greece major banks.
Health Insurance Claim number	Detection of a Health Insurance Claim number
Hong Kong: Address in Chinese (Wide)	Permissive detection of Hong Kong address in Chinese.
Hong Kong: Address in Chinese (Default)	Detection of Hong Kong address in Chinese.
Hong Kong: Address in English (Wide)	Permissive detection of Hong Kong address in English. For example: "5 Edinburgh Place, Central".

Classifier	Description
Hong Kong: Address in English (Default)	Detection of Hong Kong address in English. For example: "5 Edinburgh Place, Central District".
Hong Kong: Address in English (Narrow)	Restrictive detection of Hong Kong address in English. For example: "5 Edinburgh Place, Hong Kong Island, Hong Kong".
Hong Kong Swift codes	Detection of SWIFT codes for Hong Kong major banks.
Hungary Swift codes	Detection of SWIFT codes for Hungary major banks.
ICD9 Codes	Detection of ICD9 Codes
Iceland Kennitala of Individuals Pattern	Detection of Icelandic identification numbers (Kennitala) of individuals patterns.
Iceland Kennitala Terms	Detection of Iceland identification numbers (Kennitala) related terms.
Identification Number with proximity	Detection of Identification numbers, when found in proximity to identification related terms.
IL buy or sell instructions	Detection of buy and sell instructions in Hebrew.
IL buy or sell instructions support	Detection of buy and sell support instructions in Hebrew.
IL Insurance Policy: 10 digits	Detection of 10 digit policy numbers.
IL Insurance Policy: 10 digits - support	Detection of 10 digits Israeli Insurance Number with terms in proximity.
IL Insurance Policy: 8 digits	Detection of 8 digit policy numbers.
IL Insurance: Claim support	Detection of terms to support identification of an Israeli Insurance Claim Number.
IL Insurance: Generic with proximity	Detection of a generic Israeli Insurance Number with terms in proximity.
IL Life Insurance support	Detection of insurance terms in Hebrew.
Illinois: State ID	Detection of Illinois state ID.
India Swift codes	Detection of SWIFT codes for India major banks.
India: Form 16 Headings	Detection of India Form 16 headings.
India: PAN	Detection of Indian PAN number.
Indonesia Swift codes	Detection of SWIFT codes for Indonesia major banks.
Indonesian Single Identity Numbers (Wide)	Detects valid 16-digit delimited or un-delimited Indonesian Single Identity Numbers (Nomor Induk Kependudukan) without limitations on the first 2 digits (Province code). For example “3313034604790001”.
IP Address	Detection of an IP Address.
IP Address - Narrow	Detection of an IP address, when found in proximity to IP related term such as “IP” or “subnet”.
IP Address - Wide	Detection of all possible forms of IP addresses.
Ireland Account Pattern	Detection of Irish bank account numbers.

Classifier	Description
Ireland Account Terms	Detection of Ireland Bank Account Terms.
Ireland Swift codes	Detection of SWIFT codes for Ireland major banks.
Irish Drivers License	Detection of Irish driver's license.
Irish Passport	Detection of Irish Passport numbers.
Irish PPS Terms	Detection of terms related to Irish PPS (Personal Public Service) number.
Israel Swift codes	Detection of SWIFT codes for Israel major banks.
Italy Swift codes	Detection of SWIFT codes for Italy major banks.
Japan Swift codes	Detection of SWIFT codes for Japan major banks.
Japan: Account	Detection of a Japanese account number.
Japan: Account 1st Format	Detection of a Japanese account number.
Korea Republic Swift codes	Detection of SWIFT codes for Korea Republic major banks.
Latvia Swift codes	Detection of SWIFT codes for Latvia major banks.
Lithuania Swift codes	Detection of SWIFT codes for Lithuania major banks.
Luxembourg Swift codes	Detection of SWIFT codes for Luxembourg major banks.
Macau ID - formal	Detection of Macau ID number (formal form).
Macau ID - non formal	Detection of Macau ID number (non formal form).
Malaysian Swift codes	Detection of SWIFT codes for Malaysia major banks.
Maltese Identity Card Number	Detects Maltese identity card numbers. For example: "19999981M".
Manuscript Terms 1	Detection of manuscript patterns.
Manuscript Terms 2	Detection of manuscript related terms.
Manuscript Terms 3	Detection of manuscript terms that support detection of manuscripts.
Mexico CPISP (Clave Personal Interna del Servidor Publico)	Detection of Mexico CPISP.
Mexico Swift codes	Detection of SWIFT codes for Mexico major banks.
Microsoft License Keys	Detection of Microsoft license keys.
MySQL-Format Database Dump (Wide)	Detection of textual MySQL-format database dumps using lenient heuristics. For example: CREATE TABLE 'users' ('username' varchar(16) NOT NULL,'password' varchar(16) NOT NULL, PRIMARY KEY ('id')); INSERT INTO 'users' VALUES ('John','QWERTY12'),('Jane','QWERTY13');.

Classifier	Description
MySQL-Format Database Dump (Default)	Detection of textual MySQL-format database dumps using strict heuristics. For example: CREATE TABLE ‘users’ (‘username’ varchar(16) NOT NULL, ‘password’ varchar(16) NOT NULL, PRIMARY KEY (‘id’)); INSERT INTO ‘users’ VALUES (‘John’,’QWERTY12’),(‘Jane’,’QWERTY13’);.
Netherlands Swift codes	Detection of SWIFT codes for Netherlands major banks.
Netherlands Passport Numbers	Detection of Passport Numbers of the Netherlands.
Netherlands: Bank Account Terms	Detection of Dutch Bank Account related terms.
Network Terms	Detection of network related terms.
Network Terms and IP Addresses	Detection of network related terms and IP addresses.
New Zealand Swift codes	Detection of SWIFT codes for New Zealand major banks.
Norway Swift codes	Detection of SWIFT codes for Norway major banks.
Password as URL parameter	Detection of password as URL parameter.
Passwords pattern	Detection of common passwords, maximum of 300 Passwords.
Pattern - 10 digits non delimited	Pattern - 10 digits non-delimited.
Perl Source Code Extensions	Detection of Perl files according to their extension.
Peru Swift codes	Detection of SWIFT codes for Peru major banks.
Philippines Swift codes	Detection of SWIFT codes for Philippines major banks.
Physical Information - Blood Type	Detection of Private Physical Information - Blood Type (English/Hindi).
Physical Information - Build	Detection of Private Physical Information - Build (English/Hindi).
Physical Information - Complexion	Detection of Private Physical Information - Complexion (English/Hindi).
Physical Information - Eye Color	Detection of Private Physical Information - Eye Color (English/Hindi).
Physical Information - Hair Color	Detection of Private Physical Information - Hair Color (English/Hindi).
Physical Information - Height	Detection of Private Physical Information - Height (English/Hindi).
Physical Information - Sex	Detection of Private Physical Information - Sex (English/Hindi).
Physical Information - Weight	Detection of Private Physical Information - Weight (English/Hindi).
Poland Swift codes	Detection of SWIFT codes for Poland major banks.
Polish ID support terms	Detection of terms related to Polish ID number.

Classifier	Description
Polish Name	Detection of a Polish name.
Polish NIP support terms	Detection of terms related to Polish NIP number (a number used for tax identification).
Portugal Swift codes	Detection of SWIFT codes for Portugal major banks.
Prices with Currencies	Detection of a price in various currencies.
Problem Gambling	Detection of expressions that are indicative of problem gambling. For example: “I am addicted to gambling”, “My gambling is out of control”.
Proprietary Header/Footer	Detection of documents with terms with proprietary data in the header or footer.
Protein pattern	Detection of Protein patterns.
Python Source Code Extensions	Detection of file extensions associated with Python source code files.
Romania Swift codes	Detection of SWIFT codes for Romania major banks.
Russia Swift codes	Detection of SWIFT codes for Russia major banks.
Russian Passport - no terms	Detection of a Russian passport ignoring terms
Russian Passport - significant	Detection of a Russian passport with a passport term in proximity
Russian Passport Filter for Spreadsheet Files	Detection of a salient part of a Russian passport
Russian phone numbers pattern (optional delimiters) - wide	Detection of Russian phone numbers with optional delimiters (including period).
Russian phone numbers pattern (with delimiters)	Detection of delimited Russian phone numbers.
Saudi Arabia Swift codes	Detection of SWIFT codes for Saudi Arabia major banks.
Security Accounts Manager (SAM) Files (Registry)	Detection of SAM textual files as they appear in the Windows registry.
Singapore ID Terms	Detection of Singapore NRIC related terms.
Singapore Swift codes	Detection of SWIFT codes for Singapore major banks.
Slovakia Swift codes	Detection of SWIFT codes for Slovakia major banks.
Slovenia Swift codes	Detection of SWIFT codes for Slovenia major banks.
Social Security Numbers Pattern	Detection of Social Security Numbers
Social Security Numbers Pattern (with prefixes)	Detection of Social Security Numbers
Social Security Numbers Terms	Detection of Social Security Numbers support terms.
Source Code Extensions	Detection of C and Java files according to their extension.
South Africa Swift codes	Detection of SWIFT codes for South African major banks.

Classifier	Description
SPICE Source Code - Constant Declaration	Detection of constants declaration in the SPICE programming language.
SPICE Source Code - Simulator Language Declaration	Detection of a SPICE simulator language declaration.
SPICE Source Code - Sub-Circuit Declaration	Detection of a Sub-Circuit declaration in the SPICE programming language.
SPICE Source Code - Various Key Words 1	Detection of various keywords in the SPICE programming language.
SPICE Source Code - Various Key Words 2	Detection of various keywords in the SPICE programming language.
SPICE Source Code - Various Key Words 3	Detection of various keywords in the SPICE programming language.
SSN or TIN in an IRS Form	Detection of a Social Security Number or a Taxpayer Identification Number near a related term in a format common to IRS forms.
Suicidal thoughts (Default)	Detection of expressions that are indicative of suicidal thoughts.
Support term for Russian Moscow Social Card Number (SOCCARD)	Detection of support term related to Russian Moscow Social Card Number (SOCCARD)
Support terms for Russian Personal Pension Account Numbers (SNILS)	Detection of related terms to Russian personal pension account numbers (SNILS).
Sweden ID Pattern	Swedish ID pattern, of structure YYMMDD-dddd.
Sweden Swift codes	Detection of SWIFT codes for Sweden major banks.
Swiss AHV Number (New Format)	Detection of a Swiss AHV (Swiss Social Security) number in its new format (introduced at July 1st, 2008).
Swiss AHV Number (Old Format)	Detection of a Swiss AHV (Swiss Social Security) number in its old format.
Switzerland Swift codes	Detection of SWIFT codes for Switzerland major banks.
Taiwan Swift codes	Detection of SWIFT codes for Taiwan major banks.
Thailand Swift codes	Detection of SWIFT codes for Thailand major banks.
Turkey Swift codes	Detection of SWIFT codes for Turkey major banks.
UK Bank Account Numbers	Detection of United Kingdom bank account numbers.
UK Bank Account support terms	Detection of UK bank account support terms.
UK Bank Sort Codes	Detection of United Kingdom sort codes. This classifier may cause false positives.
UK National Insurance Number	Detection of a UK national insurance number (NINO).

Classifier	Description
UK National Insurance Number - no proximity	Detection of a UK national insurance number (NINO) without terms in proximity.
UK Passport number	Detection of a UK passport number.
UK Postal Codes	Detection of the postal codes used in the United Kingdom according to the BS 7666 postal code format rules.
UK Tax ID	Detection of a UK tax ID number.
United States Swift codes	Detection of SWIFT codes for United States major banks.
US Grades	Detection of grades in proximity to an academic subject.
US ITIN	Detection of Individual Taxpayer Identification Number (ITIN).
UTM distances	Detection of numbers representing distance in meters as used in the UTM coordinate system.
Verilog Source Code - Entire Module Declaration	Detection of Verilog source code - looking for an entire Verilog module declaration.
Verilog Source Code - Module Header Declaration	Detection of Verilog source code - looking for Verilog module declaration (header only).
VHDL Source Code - Declaration Footer	Detection of VHDL source code - looking for a terminating declaration of Architecture, Component, Process or Entity.
VHDL Source Code - Use Statement	Detection of VHDL source code - looking for a use statement declaration.
Vietnam CMND Number	Detects valid 9-digit delimited or un-delimited Vietnamese CMND numbers. For example: 331-147-981.
W-2 Form support terms 2	Detection of terms taken from the W-2 Form Header (like “FORM W 2” or “Form W-2”).
Year Period	Detection of a period denoted by starting year and ending year (e.g,. 1999-2002).
Zip Plus 4	Detection of Zip codes.