TRITON AP-DATA Predefined Policies and Classifiers

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

For your convenience, Forcepoint™ TRITON® AP-DATA includes hundreds of predefined policies and content classifiers.

- *Predefined Policies* enable you to quickly and easily define what type of content is considered a security breach on your network.
- *Predefined Classifiers* can be used to detect events and threats involving secured data.

Predefined Policies

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

Predefined policies enable you to quickly and easily define what type of content is considered a security breach on your network. Many of the TRITON AP-DATA policies are Natural Language Processing (NLP) policies which enable more powerful search and analysis techniques.

While choosing a policy or policy category, some items are set "off" by default, and can be activated individually by checking them according to the specific needs of the organization or business.

The predefined policies included in TRITON AP-DATA are constantly being updated and improved. See Updating Predefined Policies and Classifiers for instructions on keeping your policies current.

Data Loss Prevention policies

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

The predefined data loss prevention policies are based on detection of sensitive content, compliance violations, and data theft.

The acceptable use policies are listed in the following section:

● *Acceptable Use*, page 2

The content protection policies fall into several categories:

● *Company Confidential and Intellectual Property (IP)*, page 3
● *Credit Cards*, page 8
● *Financial Data*, page 10
● *Protected Health Information (PHI)*, page 15
● *Personally Identifiable Information (PII)*, page 18

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

● *Financial Regulations*, page 30
● *Payment Card Industry (PCI)*, page 33
● *Privacy Regulations*, page 34
● *US and Canada Federal Regulations*, page 66

Data theft risk indicator policies are categorized as follows:

● *Suspicious User Activity*, page 76
● *Indicators of Compromise*, page 78
● *Employee Discontent*, page 80

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 81
● *Email DLP policy*, page 82
● *Mobile DLP policy*, page 83

Acceptable Use

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

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

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

TRITON AP-DATA includes the following types of content protection policies:

- *Company Confidential and Intellectual Property (IP)*, page 3
- *Credit Cards*, page 8
- *Financial Data*, page 10
- *Protected Health Information (PHI)*, page 15
- *Personally Identifiable Information (PII)*, page 18

Company Confidential and Intellectual Property (IP)

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

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

- 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 Phrase in Header or Footer
- Dictionary Phrase 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

● Metadata keywords detection

Policy for detection of keywords in metadata. The rules of the policy use script classifiers that you can modify to insert keywords. The rules include:

- Metadata keywords detection (unique)
- Metadata keywords detection (non-unique)

● Project Documents

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

- Project Document

● 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)

● 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: asm file
  ○ Petroleum and Gas-Sensitive Information: CAD Files: drw file
  ○ Petroleum and Gas-Sensitive Information: CAD Files: DWG
  ○ Petroleum and Gas-Sensitive Information: CAD Files: DXF Binary
  ○ Petroleum and Gas-Sensitive Information: CAD Files: DXF Text
  ○ Petroleum and Gas-Sensitive Information: CAD Files: frm file
  ○ Petroleum and Gas-Sensitive Information: CAD Files: igs text format
  ○ Petroleum and Gas-Sensitive Information: CAD Files: JT file
  ○ Petroleum and Gas-Sensitive Information: CAD Files: prt file

- ○ Petroleum and Gas-Sensitive Information: CAD Files: SolidWorks files
- ○ Petroleum and Gas-Sensitive Information: CAD Files: stl binary format
- ○ Petroleum and Gas-Sensitive Information: CAD Files: stl text format
- ○ Petroleum and Gas-Sensitive Information: CAD Files: stp text format
- ○ Petroleum and Gas-Sensitive Information: CAD Files: WHIP
- ○ Petroleum and Gas-Sensitive Information: CAD Files: x_t text format
- ○ 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: Lat-Long 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 Extensions
- ○ Petroleum and Gas-Sensitive Information: pipeline flow diagrams
- ○ Petroleum and Gas-Sensitive Information: Prospecting Related Terms
  - ■ 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 text format
    - ○ Smart Power Grids: CAD Files: stl binary format
    - ○ Smart Power Grids: CAD Files: stp text format
    - ○ Smart Power Grids: CAD Files: igs text format
    - ○ Smart Power Grids: CAD Files: x_t text format
    - ○ Smart Power Grids: Executables or Link Library
    - ○ Smart Power Grids: Microsoft Visio
    - ○ Smart Power Grids: Python (Default)
    - ○ Smart Power Grids: Python (Wide)
    - ○ Smart Power Grids: XML with SCADA terms
    - ○ Smart Power Grids: Spreadsheets with SCADA terms
- ● 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
- ● 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)

- ● 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:

- ○ UTM Location Coordinates
- ○ Lat-Long Location Coordinates

- ● Business and Technical Drawing Files

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

- ○ Microsoft Visio business and technical drawing format
- ○ Corel draw format file
- ○ Catia format files
- ○ Business and Technical Drawing: CAD Files: asm file
- ○ Business and Technical Drawing: CAD Files: drw file
- ○ Business and Technical Drawing: CAD Files: DWG format files
- ○ Business and Technical Drawing: CAD Files: DXF binary format files
- ○ Business and Technical Drawing: CAD Files: DXF text format files
- ○ Business and Technical Drawing: CAD Files: frm file
- ○ Business and Technical Drawing: CAD Files: igs text format
- ○ Business and Technical Drawing: CAD Files: JT file
- ○ Business and Technical Drawing: CAD Files: prt file
- ○ Business and Technical Drawing: CAD Files: SolidWorks files
- ○ Business and Technical Drawing: CAD Files: stl binary format
- ○ Business and Technical Drawing: CAD Files: stl text format

- ○ Business and Technical Drawing: CAD Files: stp text format
- ○ Business and Technical Drawing: CAD Files: WHIP format files
- ○ Business and Technical Drawing: CAD Files: x_t text format
- 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
- 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)
- 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

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
- All CCN: American Express
- All CCN: Bancard
- All CCN: CCN (default)
- All CCN: CCN (narrow)
- All CCN: CCN (wide)
- All CCN: Diners
- All CCN: Discover
- All CCN: EnRoute
- All CCN: JCB 1st format
- All CCN: JCB 2nd format
- All CCN: Maestro, Switch or Solo CCN
- All CCN: MasterCard
- All CCN: RuPay
- All CCN: User-Defined IINs (Wide)
- All CCN: User-Defined IINs (Default)
- All CCN: User-Defined IINs (Narrow)
- All CCN: Visa
- All CCN: Visa 13 digits - obsolete
- All CCN: Wide Minus Default

● 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

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

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)

- 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
- ● 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)
- ● 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)
- ● Netherlands and 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)
- ● Peoples Republic of China Finance

  Policy for detection of PRC financial information. The rules for this policy are
  - ■ Peoples Republic of China Finance: Union Pay Credit Card (wide)
  - ■ Peoples Republic of China Finance: Union Pay Credit Card (default)
  - ■ Peoples Republic of China Finance: Union Pay Credit Card (narrow)
  - ■ Peoples Republic of China Finance: Financial cards Track1
  - ■ Peoples Republic of China Finance: Financial cards Track2 rule for detecting bank card magnetic stripe Track2
  - ■ Peoples Republic of China Finance: Financial cards Track3
  - ■ Peoples Republic of China Finance: Business Registration Number - 15 digits (wide)
  - ■ Peoples Republic of China Finance: Business Registration Number - 15 digits (default)
  - ■ Peoples Republic of China Finance: Business Registration Number - 15 digits (narrow)
  - ■ Peoples Republic of China Finance: Credit Card (Wide)
  - ■ Peoples Republic of China Finance: Credit Card (Default)
  - ■ Peoples 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
- 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
- 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)
- 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)
- 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)

● W-2 Forms

Policy for the detection of tax W-2 forms. The rule for this policy is:

- W-2 form

Protected Health Information (PHI)

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

● 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: SPSS Text files

● 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 cards and Sensitive Disease or drug

- Health Data: DNA profile (default)
- Health Data: DNA profile (narrow)
- Health Data: DOB and Name
- Health Data: ICD10 Code and Description
- Health Data: ICD10 Codes
- Health Data: ICD10 Codes and US full names
- Health Data: ICD10 Descriptions and US full names
- Health Data: ICD9 Code and Description
- Health Data: ICD9 Codes
- Health Data: ICD9 Codes and US full names
- Health Data: ICD9 Descriptions and US full names
- Health Data: Medical Form (Default)
- Health Data: Medical Form (Narrow)
- Health Data: Medical Form (Wide)
- Health Data: Name and Common Medical Condition
- Health Data: Name and Sensitive Disease or drug
- Health Data: Names (Narrow) and Common Medical Condition
- Health Data: Names (Narrow) and Sensitive Disease or drug
- Health Data: NDC number - default
- Health Data: NDC number - narrow
- Health Data: NDC number - wide

- 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: ID and Sensitive Medical Information
  - Israel PHI: Name and Sensitive Medical Information
  - Israel PHI: ID and General Medical Information
  - Israel PHI: Name and General Medical Information
  - Israel PHI:SPSS Text files

- Italy PHI

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

  - Italy PHI:Name and health information
  - Italy PHI:Codice Fiscale and health information
  - Italy PHI:SPSS Text files

- Norway PHI

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

- Norway PHI:Name and health information
- Norway PHI:Personal Number and health information
- Norway PHI:ICD10 Codes
- Norway PHI:ICD10 Code and Description
- Norway PHI: ICD10 Descriptions
- Norway PHI:ICD10 Code and first Name
- Norway PHI:ICD10 Code and Last Name
- Norway PHI: ICD10 Code and Full Name
- Norway PHI:ICD10 Code and PIN number
- Norway PHI:ICD10 Code and Personal number
- Norway PHI:SPSS Text files

● 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: DNA profile
- Sweden PHI: ICD10 Code and Description
- Sweden PHI: ICD10 Code and Name
- Sweden PHI: ICD10 Code and Name (Narrow)
- Sweden PHI: ICD10 Code and Name (Wide)
- Sweden PHI: ICD10 Code and Personal Number
- Sweden PHI: ICD10 Codes
- Sweden PHI: ICD10 Descriptions
- 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

● UK PHI

Policy for detection of UK NHS numbers.The rules for this policy are

- UK PHI: NHS Numbers (wide)
- UK PHI: NHS Numbers (default)
- UK PHI: NHS Numbers (narrow)
- UK PHI: SPSS Text files

● US PHI

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

- US PHI: Name and Common Medical Condition
- US PHI: Name and HICN

- US PHI: Name and Sensitive Disease or drug
- US PHI: Names (Narrow) and Common Medical Condition
- US PHI: Names (Narrow) and Sensitive Disease or drug
- US PHI: SPSS Text files
- US PHI: SSN and Common Medical Condition
- US PHI: SSN and Sensitive Disease or drug

Personally Identifiable Information (PII)

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

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: Australia TFN
  - Australia PII: Driver License and Name

- Belgium PII

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

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

- 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 Health
  - Brazil PII: CPF and Health
  - Brazil PII: RG
  - Brazil PII: RG Narrow

- Canada PII

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

- - Canada PII: SIN
  - Canada PII: SIN + Name
  - Canada PII: SIN + Name (Narrow)
  - Canada PII: Name + Alberta DL
  - Canada PII: Name + British Columbia
  - Canada PII: Name + Manitoba DL
  - Canada PII: Name + New Brunswick DL
  - Canada PII: Name + Newfoundland and Labrador DL
  - Canada PII: Name + Nova Scotia DL
  - Canada PII: Name + Ontario DL
  - Canada PII: Name + Prince Edward Island DL
  - Canada PII: Name + Quebec DL
  - Canada PII: Name + Saskatchewan DL
- 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)
- Czech Republic

  Policy for detection of Czech Republic private information. The rules for this policy are:
  - 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 and Name - Wide
  - Denmark PII: CPR and Name - Default
  - Denmark PII: CPR and Name - Narrow
  - Denmark PII: CPR numbers (Wide)
  - Denmark PII: CPR numbers (Default)
  - Denmark PII: CPR numbers (Narrow)
- 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

● Finland PII

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

- Finland PII: SSN: Wide
- Finland PII: SSN: Default

● France PII

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

- France PII: CCN and Name
- France PII:INSEE numbers .
- France PII:Name and Health
- France PII:INSEE and Health
- France PII:Name and INSEE .

● Germany PII

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

- Germany PII: CCN and Name
- Germany PII: Ethnicity and Name
- Germany PII: Health 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: ID (Default)
- Greece PII: ID and Name (Default)
- Greece PII: ID and Name (Wide)
- Greece PII: Sensitive Medical Information and Name (Default)
- Greece PII: Sensitive Medical Information and Name (Wide)

● Hong Kong PII

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

- Hong Kong PII: Common Surname and Address (default)
- Hong Kong PII: Common Surname and Address (narrow)

- Hong Kong PII: Common Surname and Address (wide)
- Hong Kong PII: Hong Kong ID - default pattern
- Hong Kong PII: Hong Kong ID - wide
- Hong Kong PII: Hong Kong ID (default pattern) and Common Address
- Hong Kong PII: Hong Kong ID (default pattern) and Common Surname
- Hong Kong PII: Hong Kong ID (default pattern) with Common Surname and Address
- Hong Kong PII: Hong Kong ID (formal form) and Common Address
- Hong Kong PII: Hong Kong ID (formal form) and Common Surname
- Hong Kong PII: Hong Kong ID (formal form) with Common Surname and Address
- Hong Kong PII: Hong Kong ID (wide) and Common Address
- Hong Kong PII: Hong Kong ID (wide) and Common Surname
- Hong Kong PII: Hong Kong ID (wide) and Common Surname and Address
- Hong Kong PII: Hong Kong ID formal form

- 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: Form 16
  - India: PAN
  - India: PAN (Wide)

- Indonesia PII

  Policy for detection of Indonesian Single Identity Numbers (Nomor Induk Kependudukan). The rules for this policy are:

  - Indonesia PII: Single Identity Numbers (Wide)
  - Indonesia PII: Single Identity Numbers (Default)

- Ireland PII

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

- Ireland PII: Irish Personal Public Service Number (PRSI/PPS) and Name
- Ireland PII: Irish Driver Number and Name
- Ireland PII: Irish Passport Number and Name

● Israel PII

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

- Israel PII: Israeli Identity Number - 8- or 7-Digits (Wide)
- Israel PII: Israeli Identity Number - 8- or 7-Digits (Default)
- Israel PII: Israeli Identity Number (Default)
- Israel PII: Israeli Identity Number (Wide)
- 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: Telephone Numbers
- Japan PII: Surname and Account
- Japan PII: Surname and Driver License.
- Japan PII: Surname and Pension Number
- Japan PII: Surname and Ledger Number
- Japan PII: E-mail Addresses
- Japan PII: Individual Numbers (Wide)
- Japan PII: Individual Numbers (Default)
- Japan PII: Individual Numbers (Narrow)
- Japan PII: Corporate Numbers (Wide)
- Japan PII: Corporate Numbers (Default)
- Japan PII: Corporate Numbers (Narrow)

● 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)
- ● Macau PII

  Policy for detection of Macau private information.The rules for this policy are:
  - ■ Macau PII: ID (formal form) (v7.8.1 only)
  - ■ Macau PII: ID (default)
  - ■ Macau PII: ID (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
- ● Mexico PII

  Policy for detection of Mexican private information. The rules for this policy are:
  - ■ 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: 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: Sofi and Ethnicities

- Netherlands PII: Sofi and Account with Password
- Netherlands PII: Sofi and CCN delimiters.
- Netherlands PII: Sofi and Crime
- Netherlands PII: Sofi and Diseases
- Netherlands PII: Driver License Numbers
- Netherlands PII: Passport Numbers

● New Zealand PII

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

- 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: Personal Number (Wide)
- Norway PII: Personal Number
- Norway PII: Personal Number (Narrow)
- Norway PII: Name and Personal Number
- Norway PII: Name and health information

● Peoples Republic of China

Policy for detection of Peoples Republic of China private information.

The rules for this policy are

- Peoples Republic of China PII: ID
- Peoples Republic of China PII: Chinese CV

● Philippines PII

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

- Philippines PII: Name and Address (Wide)
- Philippines PII: Name and Address (Default)
- Philippines PII: Name and Address (Narrow)

● Poland PII

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

- Poland: NIP numbers
- Poland: NIP with proximity
- Poland: NIP and Name
- Poland: PESEL numbers
- Poland: PESEL with proximity
- Poland: PESEL and Name
- Poland: Polish ID numbers

- ■ Poland: Polish ID with proximity
- ■ Poland: REGON numbers
- ■ Poland: REGON with proximity
- ■ Poland: REGON and Name
- ● 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: Moscow Social Card Number near Serial Numbers
  - ■ Russia PII: Moscow Social Card Numbers (Default)
  - ■ Russia PII: Moscow Social Card Numbers (Wide)
  - ■ Russia PII: Russian Classification on Objects of Administrative (Wide)
  - ■ Russia PII: Russian Classification on Objects of Administrative Division (Default)
  - ■ Russia PII: Russian Individual Personal Account Insurance (Wide)
  - ■ Russia PII: Russian Individual Personal Account Insurance Numbers (Default)
  - ■ Russia PII: Russian passport and name (Default)
  - ■ Russia PII: Russian passport and name (Narrow)
  - ■ Russia PII: Russian passport and name (Wide)
  - ■ Russia PII: Russian passport number
  - ■ Russia PII: Russian Phone Numbers (Default)
  - ■ Russia PII: Russian Phone Numbers (Narrow)
  - ■ Russia PII: Russian Phone Numbers (Wide)
  - ■ Russia PII: Russian Primary State Registration Numbers - 13-digits (Default)
  - ■ Russia PII: Russian Primary State Registration Numbers - 13-digits (Wide)
  - ■ Russia PII: Russian Primary State Registration Numbers - 15-digits (Default)
  - ■ Russia PII: Russian Primary State Registration Numbers - 15-digits (Wide)
  - ■ Russia PII: Russian Taxpayer Identification Numbers - 10-digits (Default)
  - ■ Russia PII: Russian Taxpayer Identification Numbers - 10-digits (Wide)
  - ■ Russia PII: Russian Taxpayer Identification Numbers - 12-digits (Default)
  - ■ Russia PII: Russian Taxpayer Identification Numbers - 12-digits (Wide)
  - ■ Russia PII: Russian Unified Classifier of Enterprises and Organizations
- ● 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: Singapore Identification numbers
  - Singapore PII: Singapore Identification numbers - No support terms
  - Singapore PII: Singapore Identification numbers with Credit Card
  - 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: 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:SA ID (wide)
  - South Africa PII:SA ID (default)
  - South Africa PII:SA ID (narrow)
  - South Africa PII: SA 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: Korea Phones (default)
  - South Korea PII: Korea Phones (wide)
  - South Korea PII: Korea Phones (with proximity)
  - South Korea PII: South Korea ID (default)
  - South Korea PII: South Korea ID (wide)
  - South Korea PII: South Korea ID (with proximity)

- Spain PII

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

  - Spain PII: DNI and Account with Password
  - Spain PII: DNI and CCN
  - Spain PII: DNI and Crime
  - Spain PII: DNI and Diseases
  - Spain PII: DNI and Ethnicities
  - Spain PII: Spanish Name + Address (default)
  - Spain PII: Spanish Name + Address (narrow)
  - Spain PII: Spanish Name + CCN
  - Spain PII: Spanish Name + DNI
  - Spain PII: Spanish Name + IBAN
  - Spain PII: Spanish Name + Passport
  - Spain PII: Spanish Names + Email Addresses
  - Spain PII: Spanish Names + Phone Numbers

- Sweden PII

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

  - Sweden PII: ID (wide)
  - Sweden PII: ID (default)

- Switzerland

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

  - 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: ID
  - Taiwan PII: ID formal form

- Taiwan PII: ID formal form with Surname
- Taiwan PII: ID formal form with Surname and Private info
- Taiwan PII: ID with Surname
- Taiwan PII: ID with Surname and Private info
- Taiwan PII: Surname and address
- Taiwan PII: Taiwan Address (default)
- Taiwan PII: Taiwan Address (narrow)
- Taiwan PII: Taiwan Address (wide)

● Thailand PII

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

- Thailand: National ID (wide)
- Thailand: National ID (default)

● Turkey PII

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

- 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: NHS Numbers (default)
- UK PII: NHS Numbers (narrow)
- UK PII: NHS Numbers (wide)
- UK PII: Postal Code and Name (Default)
- UK PII: Postal Code and Name (Narrow)
- UK PII: Sort Code and Name
- UK PII: UK Driver Number and Name
- UK PII: UK Driver Number and Name (Wide)
- UK PII: UK National Insurance Number and Name
- UK PII: UK Passport Number and Name
- UK PII: UK Tax ID Number and Name

● US PII

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

- US PII: DNA profile (default)
- US PII: DNA profile (narrow)
- US PII: Name + Arizona DL
- US PII: Name + Arkansas DL
- US PII: Name + California DL
- US PII: Name + Colorado DL

- US PII: Name + Connecticut DL
- US PII: Name + Crime
- US PII: Name + District of Columbia DL
- US PII: Name + Ethnicity
- US PII: Name + Florida DL
- US PII: Name + Georgia DL
- US PII: Name + Illinois DL
- US PII: Name + Illinois State ID
- US PII: Name + Indiana DL
- US PII: Name + Iowa DL
- US PII: Name + Massachusetts DL
- US PII: Name + Michigan DL
- US PII: Name + Minnesota DL
- US PII: Name + Nevada DL
- US PII: Name + New Jersey DL
- US PII: Name + New York DL
- US PII: Name + North Carolina DL
- US PII: Name + Ohio DL
- US PII: Name + Pennsylvania DL
- US PII: Name + Texas DL
- US PII: Name + US Address
- US PII: Name + Utah DL
- US PII: Name + Virginia DL
- US PII: Name + Washington DL
- US PII: Name + Wisconsin DL
- US PII: SSN
- US PII: SSN + Name

- Vietnam PII

  Policy for detection of Vietnamese CMND Numbers. The rules for this policy are:

  - Vietnam PII: CMND number (Wide)
  - Vietnam PII: CMND number (Default)

Regulations, Compliance and Standards

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

TRITON AP-DATA includes the following types of regulatory and compliance policies:

- *Financial Regulations*, page 30
- *Payment Card Industry (PCI)*, page 33
- *Privacy Regulations*, page 34

Financial Regulations

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

TRITON AP-DATA includes policies for the finance industry:

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

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: All Credit Card Numbers
- FFIEC: SSN
- FFIEC: Driver License
- FFIEC: PIN numbers
- FFIEC: Zip codes with Financial Terms
- FFIEC: Suspected password
- FFIEC: Credit Card Magnetic Strips
- FFIEC: Password dissemination for Web traffic
- FFIEC: 10 Digit Account Numbers
- FFIEC: 9 Digit Account Numbers
- FFIEC: 5-8 Digit Account Numbers
- FFIEC: TIFF format file type

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 Reports
- MAR: Financial Investment Information in Excel
- MAR: SOX terms
- MAR: Form 10K - Non Std fiscal year
- MAR: Form 10Q
- MAR: Form 10Q - Non Std fiscal year

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 10K
- SEC: Form 10K - Non Std fiscal year
- SEC: Form 10Q
- SEC: Form 10Q - Non Std fiscal year

Payment Card Industry (PCI)

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

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 with Exp date
- PCI Audit: CCN with CVV
- PCI Audit: CCN without validation
- PCI Audit: Wide
- PCI Audit: CCN - High Accuracy
- PCI Audit: Credit Card Magnetic Strips
- PCI Audit: Masked Credit Cards
- PCI Audit: CCN in non-English characters
- PCI Audit: CCN User-Defined IINs (Wide)
- PCI Audit: CCN User-Defined IINs (Default)
- PCI Audit: CCN User-Defined IINs (Narrow)

Privacy Regulations

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

TRITON AP-DATA 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
  - Australian Privacy Act: Name and TFN
  - Australian Privacy Act: Name and Address
  - Australian Privacy Act: TFN and Address
  - 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: Canadian Name and DL
  - PIPEDA: Canadian Name and Physical Information
  - PIPEDA: Canadian Name and Sensitive Disease

- PIPEDA: Canadian Name with Government Issues ID Card Number w proximity
- PIPEDA: Canadian Name with Indian Status Number w proximity
- PIPEDA: Canadian Name with Permanent Resident Card Number w proximity
- PIPEDA: Credit cards and Common Medical Condition
- PIPEDA: Credit cards and Sensitive Disease or drug
- PIPEDA: DOB with Address or SIN or Name
- PIPEDA: SIN and Common Medical Condition
- PIPEDA: SIN and Sensitive Disease or drug
- PIPEDA: SIN with CCN
- PIPEDA: SIN with proximity
- PIPEDA: SIN and Address or DOB or Name

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: AFM number (Default)
    - Greece: AFM number (Wide)
    - Greece: AFM number and Name (Default)
    - Greece: AFM number and Name (Wide)
    - Greece: ID and Name (Default)
    - Greece: ID and Name (Wide)
    - Greece: Sensitive Medical Information and Name (Default)
    - Greece: 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 unauthorised 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: Codice Fiscale
        - ○ Italy: Name and Codice Fiscale
        - ○ Italy: Name and health information
        - ○ Italy: Codice Fiscale and health information
- 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:
        - ○ DUTCH PDP: Sofi and Ethnicities
        - ○ DUTCH PDP: Sofi and Account with Password
        - ○ DUTCH PDP: Sofi and CCN
        - ○ DUTCH PDP: Sofi and Crime
        - ○ DUTCH PDP: Sofi and Diseases
        - ○ Dutch PDP: Dutch Bank Accounts with proximity
        - ○ Dutch PDP: Dutch Bank Accounts
        - ○ Dutch PDP: Driver License Numbers
        - ○ Dutch PDP: Passport Numbers
- 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: LPPD: NIP and Name
- Poland LPPD: LPPD: PESEL numbers
- Poland LPPD: NIP numbers
- Poland LPPD: NIP with proximity
- Poland LPPD: PESEL and Name
- Poland LPPD: PESEL with proximity
- Poland LPPD: Polish ID and Name
- Poland LPPD: Polish ID numbers
- Poland LPPD: Polish ID with proximity
- Poland LPPD: REGON and Name
- Poland LPPD: REGON numbers
- Poland LPPD: REGON with proximity

- 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 and Ethnicities
    - SPAIN DPA: DNI and Account with Password
    - SPAIN DPA: DNI and CCN
    - SPAIN DPA: DNI and Crime
    - SPAIN DPA: DNI and Diseases

- 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 Files
  - ○ SFS 2008:355: DNA profile
  - ○ SFS 2008:355: ICD10 Code and Description
  - ○ SFS 2008:355: ICD10 Code and Name
  - ○ SFS 2008:355: ICD10 Code and Name (Narrow)
  - ○ SFS 2008:355: ICD10 Code and Name (Wide)
  - ○ SFS 2008:355: ICD10 Code and Personal Number
  - ○ SFS 2008:355: ICD10 Codes
  - ○ SFS 2008:355: ICD10 Descriptions
  - ○ 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 files

- ● UK

  - ■ Information Governance Toolkit

    Policy for compliancy with NHS "Information Governance Toolkit" (IG Toolkit). The rules for this policy are:
    - ○ IG Toolkit: NHS Numbers (wide)
    - ○ IG Toolkit: NHS Numbers (default)
    - ○ IG Toolkit: NHS Numbers (narrow)
    - ○ IG Toolkit: UK National Insurance Number and Name
    - ○ IG Toolkit: UK Driver Number and Name
    - ○ IG Toolkit: UK Driver Number and Name (Wide)
    - ○ IG Toolkit: UK Passport Number and Name
    - ○ IG Toolkit: UK Tax ID Number and Name
    - ○ IG Toolkit: Name and Common Medical Condition
    - ○ IG Toolkit: Names (Narrow) and Common Medical Condition
    - ○ IG Toolkit: Name and Sensitive Disease or drug
    - ○ IG Toolkit: Names (Narrow) and Sensitive Disease or drug
    - ○ IG Toolkit: DNA profile (default)
    - ○ IG Toolkit: DNA profile (narrow)
    - ○ IG Toolkit: DOB and Name

- ○ IG Toolkit: NDC number - default
- ○ IG Toolkit: NDC number - narrow
- ○ IG Toolkit: ICD10 Codes
- ○ IG Toolkit: ICD10 Codes and US full names
- ○ IG Toolkit: ICD10 Descriptions and US full names
- ○ IG Toolkit: ICD9 Codes
- ○ IG Toolkit: ICD9 Codes and US full names
- ○ IG Toolkit: ICD9 Descriptions and US full names

- ■ 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 9546EC

  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 95 46: Dutch Sofinummer and CCN
  - ■ EU 95 46: French INSEE numbers and CCN
  - ■ EU 95 46: Italian Codice Fiscale numbers and CCN
  - ■ EU 95 46: Norway Personal Number and CCN
  - ■ EU 95 46: Spanish DNI numbers and CCN
  - ■ EU 95 46: Swiss new format AHV and CCN
  - ■ EU 95 46: Swiss Old format AHV and CCN
  - ■ EU 95 46: 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:

- ■ PDPO: Common Surname and Address (default)
- ■ PDPO: Common Surname and Address (narrow)
- ■ PDPO: Common Surname and Address (wide)
- ■ PDPO: Hong Kong ID - default pattern
- ■ PDPO: Hong Kong ID - wide
- ■ PDPO: Hong Kong ID (default pattern) and Common Address
- ■ PDPO: Hong Kong ID (default pattern) and Common Surname
- ■ PDPO: Hong Kong ID (default pattern) with Common Surname and Address
- ■ PDPO: Hong Kong ID (formal form) and Common Address
- ■ PDPO: Hong Kong ID (formal form) and Common Surname
- ■ PDPO: Hong Kong ID (formal form) with Common Surname and Address
- ■ PDPO: Hong Kong ID (wide) and Common Address
- ■ PDPO: Hong Kong ID (wide) and Common Surname
- ■ PDPO: Hong Kong ID (wide) and Common Surname and Address
- ■ PDPO: Hong Kong ID formal form

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: Suspected Passwords
  - India IT Act: CCN (Default)
  - India IT Act: CCN (Narrow)
  - India IT Act: Indian Name and Physical Information
  - India IT Act: Indian Name and Sensitive Disease or Drug
  - India IT Act: Indian Name and Common Medical Condition
  - India IT Act: Indian Name and Sexual Orientation
  - India IT Act: Indian Name and Biometric Information
  - India IT Act: Indian Name and Password
  - India IT Act: Password dissemination for Web traffic

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: ID and Sensitive Medical Information
  - Israeli Health Care: Name and Sensitive Medical Information
  - Israeli Health Care: ID and General Medical Information
  - Israeli Health Care: Name and General Medical Information

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: CCN: All Credit Cards
- JPIP: Account and CCN
- 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: Malaysian ID
  - Malaysia PDPA: Malaysian ID and CCN
  - Malaysia PDPA: Malaysian ID and Account number
  - Malaysia PDPA: Malaysian ID and Ethnicities or Religion
  - Malaysia PDPA: Malaysian ID and Crime
  - Malaysia PDPA: Malaysian Name and sensitive health information
  - Malaysia PDPA: DNA Sequences
  - Malaysia PDPA: Malaysian Name and Password

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: Personal Number (Wide)

■ Norway: Personal Number

■ Norway: Personal Number (Narrow)

■ Norway: Name and Personal Number

■ Norway: Name and health information

■ Norway: Personal Number and health information

■ Norway: ICD10 Codes

■ Norway: ICD10 Code and Description

■ Norway: ICD10 Descriptions

■ Norway: ICD10 Code and First Name

■ Norway: ICD10 Code and Last Name

■ Norway: ICD10 Code and Full Name

■ Norway: ICD10 Code and PIN number

Russia

Policies for promoting compliance with Russia Privacy regulations.

● Russia Federal Act 152-FZ

Federal act 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 Account Insurance Number (SNILS), Taxpayer Identification Numbers (INN), personal phone numbers, etc, in proximity to Russian names. The rules for this policy are:

- 152-FZ: Moscow Social Card Number near Russian name
- 152-FZ: Russian Individual Personal Account Insurance Number (SNILS) near Russian name
- 152-FZ: Russian Passport Number near Russian name
- 152-FZ: Russian Phone Number near Russian name
- 152-FZ: Russian Primary State Registration Number (OGRNIP) near Russian name
- 152-FZ: Russian Taxpayer Identification Number (INN) near Russian 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: Passport number
- Russian Federation IIIP: passport and name
- Russian Federation IIIP: passport and name (Default)
- Russian Federation IIIP: passport and name (Wide)
- Russian Federation IIIP: passport and name (Narrow)
- Russian Federation IIIP: DNA Sequence

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: Singapore Identification numbers
- Singapore ETA: Singapore Identification numbers - No support terms
- Singapore ETA: Singapore Identification numbers with Credit Card
- 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 organisations 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: Singapore Identification numbers (Default)
  - Singapore PDPA: Singapore Identification numbers (Wide)
  - Singapore PDPA: Name and Singapore Identification numbers (Narrow)
  - Singapore PDPA: Name and Singapore Identification numbers (Default)
  - Singapore PDPA: Name and CCN
  - Singapore PDPA: Name and sensitive health information
  - Singapore PDPA: DNA Sequences
  - Singapore PDPA: Name and Password
  - Singapore PDPA: Singaporean Phones Numbers (Wide)
  - Singapore PDPA: Singaporean Phones Numbers (Default)
  - Singapore PDPA: Singaporean Phones Numbers (Narrow)
  - Singapore PDPA: Name and Singaporean Phones Number (Wide)
  - Singapore PDPA: Name and Singaporean Phones Number (Default)
  - Singapore PDPA: Name and Singaporean Phones Number (Narrow)
  - Singapore PDPA: Name and Address (Default)
  - Singapore PDPA: Name and Address (Narrow)

South Africa

Policies for promoting compliance with South Africa Privacy regulations.

- SA 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 rule for this policy is:

  - SA ECT: ID with CCN

- SA POPI

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

  - SA POPI: SA ID
  - SA POPI: SA ID and Ethnicities or Religion
  - SA POPI: SA ID and Account number
  - SA POPI: SA ID and CCN
  - SA POPI: SA ID and Crime

- SA POPI: SA ID and Health Information
- SA POPI: SA ID and Date of Birth
- SA POPI: SA Name and Password
- SA POPI: SA Name and sensitive health information
- SA POPI: SA Name and Personal Finance terms
- SA POPI: DNA Sequences

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 Protectiot: 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 formal form
- Taiwan PIPA: ID
- Taiwan PIPA: ID formal form with Surname
- Taiwan PIPA: ID with Surname
- Taiwan PIPA: ID formal form with Surname and Private info
- Taiwan PIPA: ID with Surname and Private info

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

Policies for promoting compliance with various states' privacy regulations

Alaska

Alaska HB 65 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 a social security number, driver's license number, account number, password, or other access codes. The policy detects combination 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:

- HB 65: Name and SSN
- HB 65: Name and DL
- HB 65: Name and CCN
- HB 65: Name and Password
- HB 65: Password dissemination for Web traffic
- HB 65: Account and Password

Arizona

Arizona SB 1338 (http://www.azleg.gov/legtext/47leg/2r/bills/sb1338h.pdf) Requires a person who conducts business in Arizona and owns or licenses unencrypted computerized data that includes personal information to maintain its secrecy and confidentiality and to report about incidents that materially compromises the security or confidentiality of personal information. The rules for this policy are:

- SB 1338: SSN with AZ driver license
- SB 1338: SSN with CCN

Arkansas

Arkansas SB 1167 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 combinations with sensitive information such as private health information, credit card numbers, or passwords. The rules for this policy are:

- SB 1167: SSN with Sensitive Disease or Drug
- SB 1167: Names with Sensitive Disease or Drug
- SB 1167: Names (Narrow) with Sensitive disease or drug
- SB 1167: Arkansas Driver License with Sensitive Disease or Drug
- SB 1167: SSN with CCN
- SB 1167: CCN with AR Driver License
- SB 1167: Suspected Passwords
- SB 1167: Password dissemination for Web traffic

California

- California AB 1298: requires organizations to protect Californians' personal information (including personal health information) and to inform Californians when their private information is disclosed during a security breach. The policy comprises rules that detect combinations of personally identifiable information combinations with sensitive information such as private health information, credit card numbers, or passwords. The rules for this policy are:
    - AB 1298: California Driver License with Sensitive Disease or Drug
    - AB 1298: CCN: with CA Driver License
    - AB 1298: Names with Sensitive Disease or drug
    - AB 1298: Password dissemination for Web traffic
    - AB 1298: SSN with CCN
    - AB 1298: SSN with Sensitive Disease or Drug
    - AB 1298: Suspected Passwords
- California AB 1950: requires organizations 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 extended 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 rules for this policy are:
    - AB 1950: SSN with CCN
    - AB 1950: CCN with CA Driver License
    - AB 1950: Suspected Passwords

- AB 1950: Password dissemination for Web traffic
- California SB 541 and AB 211: these amend the California Health and Safety Code and section 56.36 of the Civil Code. The bills give the state of California the ability to assess and enforce high fines for unauthorized leakage or access of private health information and create a new State Office of Health Information Integrity (OHII) to oversee data issues. The policy detects combinations of Personally Identifiable Information (PII) like names, social security or credit card number, and sensitive health information such as medical condition and DNA profiles. The rules for this policy are:
  - SB 541: SSN and Sensitive Disease or drug
  - SB 541: SSN and Common Medical Condition
  - SB 541: Credit cards and Sensitive Disease or drug
  - SB 541: Credit card and Common Medical Condition
  - SB 541: Name and Common Medical Condition
  - SB 541: Name (Narrow) and Common Medical Condition
  - SB 541: Name and Sensitive Disease or drug
  - SB 541: Names (Narrow) and Sensitive Disease or drug
  - SB 541: Celebrities Names and Sensitive Disease or drug
  - SB 541: Celebrity Name and Common Medical Condition
  - SB 541: DNA profile
  - SB 541: ICD10 Codes and US full names
  - SB 541: ICD10 Descriptions and US full names
  - SB 541: ICD9 Codes and US full names
  - SB 541: ICD9 Descriptions and US full names
- California Financial Information Privacy Act (also known as SB 1) requires financial institutions to provide their consumers notice and meaningful choice about how consumers' non-public personal information is shared or sold by their financial institutions. It provides greater privacy protections than those provided by the Gramm-Leach-Bliley Act. The policy contains rules to detect accounts, credit cards, social security numbers, and California driver license numbers. The rules for this policy are:
  - SB 1: CCN (Default)
  - SB 1: CCN (Narrow)
  - SB 1: SSN
  - SB 1: SSN with CA driver license
  - SB 1: SSN with CCN
  - SB 1: 10 Digit Account Numbers
  - SB 1: 9 Digit Account Numbers
  - SB 1: 5-8 Digit Account Numbers
- California SB 1386: requires organizations to notify Californians if their personal information is disclosed during a security breach. SB 1386 is directed at state agencies and businesses operating in California. Personal information is defined

as an individual's first name or first initial and last name with any of the following.The rules for this policy are.

- CC 1798: SSN with California Driver License
- CC 1798: SSN with CCN
- CC 1798: Name and Common Medical Condition
- CC 1798: Name and Sensitive Disease or Drug
- CC 1798: Name and HICN

Colorado

Colorado HB 1119 requires any individual or commercial entity that conducts business in Colorado and owns or licenses computerized data that includes Private Information or maintains such data to provide consumer notification of data breaches. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and Colorado driver license numbers. The rules for this policy are:

- HB 1119: SSN: with Colorado driver license
- HB 1119: SSN with CCN
- HB 1119: Name with SSN
- HB 1119: Name with Colorado driver license
- HB 1119: Name with CCN
- HB 1119: SSN with DNA profile

Connecticut

Connecticut SB 650 requires a business that has suffered a security breach involving personal information to disclose it to affected consumers, generally without unreasonable delay. The policy detects combinations of Personally Identifiable Information (PII) like full names, social security numbers, Connecticut driver license and credit card numbers. Additional rules detect passwords. The rules for this policy are:

- SB 650: Name and SSN
- SB 650: Name and DL
- SB 650: Name and CCN
- SB 650: Name and Password
- SB 650: Password dissemination for Web traffic
- SB 650: Account and Password

Delaware

Delaware HB 116 helps ensure that personal information about Delaware residents is protected by encouraging data brokers to provide reasonable security for personal information. It requires an individual or a commercial entity that conducts business in Delaware and that owns or licenses computerized data that includes personal information to notify a resident of Delaware of any breach of the security of the

system. The policy detects combinations of Personally Identifiable Information (PII) like full names, social security and credit card numbers, alone or with sensitive health information. Additional rules detect passwords.The rules for this policy are:

- HB 116: Account and Password
- HB 116: Credit cards and Common Medical Condition
- HB 116: Credit cards and Sensitive Disease or drug
- HB 116: Name and CCN
- HB 116: Name and Password
- HB 116: Name and SSN
- HB 116: Password dissemination for Web traffic

District of Columbia

District of Columbia 28-3852 mandates that consumers should be notified when electronically-stored personal information is compromised in a way that increases the risk of identity theft. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names, social security numbers, DC driver license and credit card numbers. Additional rules detect passwords. The rules for this policy are:

- DC 28-3852: Name and SSN
- DC 28-3852: Name and DL
- DC 28-3852: Name and CCN
- DC 28-3852: Name and Password
- DC 28-3852: Password dissemination for Web traffic

Florida

Florida HB 481 requires businesses maintaining computerized data including PI to provide notice of security system breach in certain circumstances. This State law affects any person that conducts business in Florida and owns or licenses computerized data that includes PI or maintains such data. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver license numbers with different thresholds, according to the severity levels mandated. Additional rules detect passwords. The rules for this policy are:

- HB 481: SSN with CCN
- HB 481: CCN with FL Driver License
- HB 481: Suspected passwords

Georgia

Georgia SB 230 requires expeditious notification of unauthorized acquisition and possible misuse of PI. This State policy applies to information brokers that own or license computerized data that includes PI or a person or business who maintains such data on behalf of brokers. The policy detects combinations of Personally Identifiable

Information (PII) like social security, credit card, and driver license numbers. Additional rules detect passwords.The rules for this policy are:

- SB 230: SSN with CCN
- SB 230: CCN with GA Driver License
- SB 230: Suspected passwords
- SB 230: Password dissemination for Web traffic

Hawaii

Hawaii SB 2290 requires businesses and government agencies to notify individual residents when their personal information has been compromised by unauthorized disclosure. Personal information is considered an individual's full name in combination with any of the following: social security number, driver's license number, or financial account information. The policy detects combination 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:

- SB-2290: Name and SSN
- SB-2290: Name and DL
- SB-2290: Name and CCN
- SB-2290: Name and Password
- SB-2290: Password dissemination for Web traffic
- SB-2290: Account and Password

Idaho

Idaho SB-1374 requires agencies, individuals, and commercial entities to disclose when the security of computerized personal information has been breached. Personal information is considered an individual's full name in combination with any of the following: social security number, driver's license number, or financial account information. The policy detects combination 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:

- SB-1374: Name and SSN
- SB-1374: Name and DL
- SB-1374: Name and CCN
- SB-1374: Name and Password
- SB-1374: Password dissemination for Web traffic
- SB-1374: Account and Password

Illinois

Illinois HB 1633 requires data collector to provide notification of security breach after discovery, even if data has not been accessed by unauthorized person. This State law affects all data collectors that own or license 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 license numbers. Additional rules detect passwords. The rules for this policy are:

- HB 1633: SSN with CCN
- HB 1633: CCN with Illinois Driver Lice
- HB 1633: CCN with Illinois State ID
- HB 1633: Suspected passwords
- HB 1633: Password dissemination for Web traffic

Indiana

Indiana HB 1101 requires a business that has suffered a security breach involving personal information to disclose it to affected consumers, generally without unreasonable delay. It generally requires the notice to be given in writing, by telephone, or electronically. The policy detects combinations of Personally Identifiable Information (PII) like full names, social security numbers, Indiana driver license and credit card numbers. Additional rules detect passwords. The rules for this policy are:

- HB 1101: Name and SSN
- HB 1101: Name and DL
- HB 1101: Name and CCN
- HB 1101: Name and Password
- HB 1101: Password dissemination for Web traffic
- HB 1101: Account and Password

Iowa

Iowa SF 2308 requires notification of Iowa consumers of a security breach involving personal information by the person who owns, maintains or otherwise possesses the information. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names, social security numbers, DNA data, Iowa driver license and credit card numbers. Additional rules detect passwords.The rules for this policy are:

- Iowa SF 2308: Name and SSN
- Iowa SF 2308: Name and DL
- Iowa SF 2308: Name and CCN
- Iowa SF 2308: Name and Password
- Iowa SF 2308: Password dissemination for Web traffic
- Iowa SF 2308: DNA profile

Kansas

Kansas SB-196 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 the 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:

- SB-196: Name and SSN
- SB-196: Name and DL
- SB-196: Name and CCN
- SB-196: Name and Password
- SB-196: Password dissemination for Web traffic
- SB-196: Account and Password

Louisiana

Louisiana SB-205 requires that consumers are notified when the security of their personal information has been breached. Personal information is defined to include unencrypted information on an individual consisting of the individual's name and one or more of several other pieces of information, including a Social Security number, driver's license number, account number, password, or other access codes. The policy detects combination 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:

- SB-205: Name and SSN
- SB-205: Name and DL
- SB-205: Name and CCN
- SB-205: Name and Password
- SB-205: Password dissemination for Web traffic
- SB-205: Account and Password

Maine

Maine LD-1671 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 the 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:

- LD-1671: Name and SSN
- LD-1671: Name and DL
- LD-1671: Name and CCN
- LD-1671: Name and Password
- LD-1671: Password dissemination for Web traffic
- LD-1671: Account and Password

Maryland

Maryland SB 194 requires all businesses in Maryland take reasonable steps to ensure that no personal information is accessed by unauthorized individuals. Brokers and

agents should also be taking reasonable steps to ensure that the personal information is stored safely. Personal information is considered the customer's full name in combination with any of the following: Social Security or tax I.D. number, driver's license number, or financial account information. Businesses are required to notify the Attorney General's office and customer if personal information in an electronic database is breached. The policy detects combination 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:

- SB 194: Name and SSN
- SB 194: Name and DL
- SB 194: Name and CCN
- SB 194: Name and Password
- SB 194: Password dissemination for Web traffic
- SB 194: Account and Password

Massachusetts

Massachusetts 201 CMR 17 mandates that a business in Massachusetts shall encrypt any personal information of a customer that is transmitted over public networks or stored on lap tops or removable memory. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names, social security numbers, Massachusetts driver license and credit card numbers. Additional rules detect passwords. The rules for this policy are:

- MA 201 CMR: Name and SSN
- MA 201 CMR: Name and SSN (Wide)
- MA 201 CMR: Name and DL
- MA 201 CMR: Name and DL (Wide)
- MA 201 CMR: Name and CCN
- MA 201 CMR: Name and CCN (Wide)
- MA 201 CMR: Name and ID
- MA 201 CMR: Name and Password
- MA 201 CMR: Password dissemination for Web traffic
- MA 201 CMR: Name with Account and Password
- MA 201 CMR: Account and Password

Michigan

Michigan Privacy Act SB 309 requires a state agency or a private company that maintains computerized data with personalized information on individuals to notify those individuals if a breach of security allows unencrypted personal identifying information to be acquired by an unauthorized person. Failure to comply with the notification requirements would be punishable by civil fines up to a maximum of $2.5 million. The policy detects combinations of Personally Identifiable Information (PII)

like social security numbers, Michigan driver license, credit card numbers, and DNA. The rules for this policy are:

- MI SB 309: SSN
- MI SB 309: SSN with CCN
- MI SB 309: SSN with Michigan DL
- MI SB 309: SSN with Account Number
- MI SB 309: SSN with PIN Number
- MI SB 309: SSN with possible password
- MI SB 309: SSN with DNA profile

Minnesota

Minnesota H.F. 2121 code requires businesses to provide consumer notification of data breaches. It is applicable to any person that conducts business in Minnesota and owns or licenses computerized data that includes PI or maintains such data. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and Minnesota driver license numbers. The rules for this policy are:

- H.F. 2121: SSN: with MN driver license
- H.F. 2121: SSN with CCN
- H.F. 2121: Name with SSN
- H.F. 2121: Name with Minnesota driver license
- H.F. 2121: Name with CCN
- H.F. 2121: SSN with DNA profile

Missouri

Missouri HB 62 requires a notification for breaches of electronically-stored personal information. Any business that owns or licenses personal information belonging to Missouri residents must provide notice to affected individuals in the event of a breach of security involving the individual's personal information. Personal information is defined as an individual's name, in combination with a data element that has not been encrypted, redacted or otherwise made unreadable or unusable. Data elements include an individual's social security number, driver's license number, and financial account numbers with access passwords, access codes to financial accounts, medical information, or health insurance information. The policy detects combination full names with social security, driver's license, or credit card numbers. Additional rules detect passwords, account numbers and medical information. The rules for this policy are:

- HB 62: Account and Password
- HB 62: ICD10 Descriptions and US full names
- HB 62: Name and CCN
- HB 62: Name and DL
- HB 62: Name and Password
- HB 62: Name and Sensitive Disease or drug

- HB 62: Name and SSN
- HB 62: Password dissemination for Web traffic

Montana

Montana HB-732 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 the 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:

- HB-732: Name and SSN
- HB-732: Name and DL
- HB-732: Name and CCN
- HB-732: Name and Password
- HB-732: Password dissemination for Web traffic
- HB-732: Account and Password

Nevada

Nevada SB 227 and NRS 603A require that organizations or business entities in Nevada shall not disseminate unencrypted personal information and shall not move any data storage device containing unencrypted personal information outside of the secure system of the business. NRS 603A also mandates notification of the breach to any resident of this State whose unencrypted personal information is reasonably believed to have been acquired by an unauthorized person. The pre-defined policy detects Personally Identifiable Information (PII) that should be encrypted, like full names with social security numbers, Nevada driver license, credit card numbers, and passwords. The rules for this policy are:

- Nevada SB 227 and NRS 603A: Account and Password
- Nevada SB 227 and NRS 603A: Name and CCN
- Nevada SB 227 and NRS 603A: Name and CCN (Wide)
- Nevada SB 227 and NRS 603A: Name and DL
- Nevada SB 227 and NRS 603A: Name and DL (Wide)
- Nevada SB 227 and NRS 603A: Name and ID
- Nevada SB 227 and NRS 603A: Name and Password
- Nevada SB 227 and NRS 603A: Name and SSN
- Nevada SB 227 and NRS 603A: Name and SSN (Wide)
- Nevada SB 227 and NRS 603A: Name with Account and Password
- Nevada SB 227 and NRS 603A: Password dissemination for Web traffic

New Hampshire

New Hampshire HB-1660 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 combination 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:

- HB-1660: Name and SSN
- HB-1660: Name and DL
- HB-1660: Name and CCN
- HB-1660: Name and Password
- HB-1660: Password dissemination for Web traffic
- HB-1660: Account and Password

New Jersey

New Jersey A 4001 requires businesses or public entities that are compiling or maintaining computerized data with personal information (PI) to disclose a security breach if the personal information is reasonably believed to be acquired by unauthorized persons. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver license numbers. Additional rules detect passwords. The rules for this policy are:

- A 4001: SSN with CCN
- A 4001: CCN with NJ Driver License
- A 4001: Suspected passwords
- A 4001: Password dissemination for Web traffic

New York State

New York AB 4254 guarantees individuals the right to know what information was exposed during a breach, so that they can take the necessary steps to both prevent and repair any damage incurred. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and New York driver license numbers. The rules for this policy are:

- AB 4254: Name with CCN
- AB 4254: Name with New-York driver license
- AB 4254: Name with SSN
- AB 4254: SSN with CCN
- AB 4254: SSN with DNA profile
- AB 4254: SSN: with NY driver license

North Carolina

North Carolina Identity Theft Protection Act, SB 1048, mandates protection of personal information and requires NC businesses to notify consumers in case of a

security breach. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names with social security numbers, NC driver licenses, and credit card numbers. The rules for this policy are:

- NC SB 1048: Name and SSN
- NC SB 1048: Name and DL
- NC SB 1048: Name and CCN

Ohio

Ohio HB 104 mandates that consumers should be notified when electronically-stored personal information is compromised in a way that increases the risk of identity theft. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names, social security numbers, Ohio driver licenses, and credit card numbers. Additional rules detect passwords. The rules for this policy are:

- Ohio HB 104: Name and SSN
- Ohio HB 104: Name and DL
- Ohio HB 104: Name and CCN
- Ohio HB 104: Name and Password
- Ohio HB 104: Password dissemination for Web traffic

Oklahoma

Oklahoma HB-2357 requires that agencies, individuals, and commercial entities disclose when the security of computerized personal information has been breached. Personal information is considered the consumer's full name in combination with any of the following: Social Security number, driver's license number, or financial account information. The policy detects combination 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:

- HB-2357: Name and SSN
- HB-2357: Name and DL
- HB-2357: Name and CCN
- HB-2357: Name and Password
- HB-2357: Password dissemination for Web traffic
- HB-2357: Account and Password

Oregon

Oregon Consumer Identity Protection Act (SB 583) 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 combination 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:

- SB 583: Name and SSN

- SB 583: Name and DL
- SB 583: Name and CCN
- SB 583: Name and Password
- SB 583: Password dissemination for Web traffic
- SB 583: Account and Password

Pennsylvania

Pennsylvania SB 712 provides for the notification of residents whose personal information data was or may have been disclosed due to a security system breach, and imposes penalties. The policy detects combinations of Personally Identifiable Information (PII) like full names, social security numbers, Pennsylvania driver licenses, and credit card numbers. Additional rules detect passwords. The rules for this policy are:

- SB 712: Name and SSN
- SB 712: Name and DL
- SB 712: Name and CCN
- SB 712: Name and Password
- SB 712: Password dissemination for Web traffic
- SB 712: Account and Password

Rhode Island

Rhode Island HB-6191 requires that agencies, individuals, and commercial entities disclose when the security of computerized personal information has been breached. Personal information is considered the consumer's full name in combination with any of the following: Social Security number, driver's license number, or financial account information. The policy detects combination 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:

- HB-6191: Name and SSN
- HB-6191: Name and DL
- HB-6191: Name and CCN
- HB-6191: Name and Password
- HB-6191: Password dissemination for Web traffic
- HB-6191: Account and Password

Tennessee

Tennessee SB 2220 requires notice of a breach of the security, confidentiality, or integrity of unencrypted, personal information by persons doing business in the state. Personal information is defined as an individual's name, in combination with individual's social security number, driver's license number, or financial account numbers with access passwords. The policy detects combinations of Personally Identifiable Information (PII) like full names, social security numbers, driver's

license, and credit card numbers. Additional rules detect passwords. The rules for this policy are:

- SB 2220: Name and SSN
- SB 2220: Name and DL
- SB 2220: Name and CCN
- SB 2220: Name and Password
- SB 2220: Password dissemination for Web traffic
- SB 2220: Account and Password

Texas

Texas SB 122 requires that any person that conducts business in Texas and owns or licenses computerized data that includes sensitive Private Information will take reasonable measures to protect it. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and Texas driver license numbers.The rules for this policy are:

- SB 122: SSN: with Texas driver license
- SB 122: SSN with CCN
- SB 122: Name with SSN
- SB 122: Name with Texas driver license
- SB 122: Name with CCN
- SB 122: SSN with DNA profile

Utah

Utah SB 69's purpose is to address the integrity of consumer credit databases. It is applicable to any person that conducts business in Utah and maintains PI. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver license numbers. Additional rules detect passwords.The rules for this policy are:

- SB 69: SSN with CCN
- SB 69: CCN with Utah Driver License
- SB 69: Suspected passwords
- SB 69: Password dissemination for Web traffic
- SB 69: SSN and Account number and Password

Virginia

Virginia SB 307 mandates that consumers should be notified when their personal information is compromised in a way that increases the risk of identity theft or other fraud. The bill also requires covered entities to notify the state attorney general in the case of breaches of personal information of more than 1,000 residents. The policy detects unencrypted combinations of Personally Identifiable Information (PII) like full names, social security numbers, Virginia driver license and credit card numbers. The rules for this policy are:

- VA SB 307: Name and SSN
- VA SB 307: Name and DL
- VA SB 307: Name and CCN

Washington

Washington SB 6043 requires that any person or business that owns or licenses computerized data that includes PI must disclose security system breach to those whose unencrypted PI is reasonably believed to be acquired by an unauthorized person. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and Washington driver license numbers.The rules for this policy are:

- SB 6043: SSN: with WA driver license
- SB 6043: SSN with CCN
- SB 6043: Name with SSN
- SB 6043: Name with Washington driver license
- SB 6043: Name with CCN
- SB 6043: SSN with DNA profile

Wisconsin

Wisconsin SB 164 requires notice of unauthorized use of personal identifying information. The policy detects combinations of Personally Identifiable Information (PII) like social security, credit card, and driver license numbers, with sensitive private information like DNA profile or password.The rules for this policy are:

- SB 164: SSN with CCN
- SB 164: SSN with Wisconsin DL
- SB 164: SSN with Account Number
- SB 164: SSN with PIN Number
- SB 164: SSN with possible password
- SB 164: SSN with DNA profile

US and Canada Federal Regulations

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

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

- *Check 21 Act*
- *COPPA*, page 67
- *DIACAP*
- *Export Administration Regulations (EAR)*
- *FCRA*
- *FDA- 21 CFR*

- *FERC and NERC*
- *FERPA*
- *FFIEC*
- *FISMA*
- *GLBA*
- *HIPAA*
- *ITAR*
- *MITS*
- *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 rules for this policy is:

- Check 21: TIFF Format

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 rule for this policy is:

- COPPA: PII and Age

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). The rules for this policy are:

- DIACAP: 5400.11-R - Name and Crime
- DIACAP: 5400.11-R - Name and Ethnicity
- DIACAP: 5400.11-R - Name and SSN
- DIACAP: 5400.11-R - SSN and Crimes

- DIACAP: 8520.1 - Confidential Documents
- DIACAP: 8520.1 - Password dissemination for Web traffic
- DIACAP: 8520.1 - Proprietary in Header or Footer
- DIACAP: 8520.1 - Suspected Passwords
- DIACAP: DoD 5400.11-R - SSN and Ethnicities
- DIACAP: DoD 6025.18 - CCN and Sensitive Disease or drug
- DIACAP: DoD 6025.18 - Name and Common Medical Condition
- DIACAP: DoD 6025.18 - Name and Sensitive Diseases
- DIACAP: DoD 6025.18 - Names (Narrow) and Common Medical Condition
- DIACAP: DoD 6025.18 - Names (Narrow) and Sensitive Diseases
- DIACAP: DoD 6025.18 - SSN and Sensitive Disease or Drug
- DIACAP: Network Information and Security (patterns and IP)
- DIACAP: Network Information and Security (textual patterns)

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: C family or Java (Default)
- EAR: C family or Java (Wide)
- EAR: CAD Files: asm file
- EAR: CAD Files: drw file
- EAR: CAD Files: DWG format files
- EAR: CAD Files: DXF binary format files
- EAR: CAD Files: DXF text format files
- EAR: CAD Files: frm file
- EAR: CAD Files: igs text format
- EAR: CAD Files: JT file
- EAR: CAD Files: prt file
- EAR: CAD Files: SolidWorks files
- EAR: CAD Files: stl binary format
- EAR: CAD Files: stl text format
- EAR: CAD Files: stp text format
- EAR: CAD Files: WHIP format files
- EAR: CAD Files: x_t text format

- EAR: Catia format files
- EAR: Chemicals and Materials (Default)
- EAR: Chemicals and Materials (Narrow)
- EAR: Chemicals and Materials (Wide)
- EAR: Confidential documents
- EAR: Corel draw format file
- 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 Business and Technical Drawing format
- 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)

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 : DNA Sequence
- FDA 21 CFR : Name and Common Medical Condition
- FDA 21 CFR : Names (Narrow) and Common Medical Condition
- FDA 21 CFR : Password dissemination for Web traffic
- 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: asm file
- FERC and NERC: CAD Files: drw file
- FERC and NERC: CAD Files: DWG
- FERC and NERC: CAD Files: DXF Binary
- FERC and NERC: CAD Files: DXF Text
- FERC and NERC: CAD Files: frm file
- FERC and NERC: CAD Files: igs text format
- FERC and NERC: CAD Files: JT file
- FERC and NERC: CAD Files: prt file
- FERC and NERC: CAD Files: SolidWorks files
- FERC and NERC: CAD Files: stl binary format
- FERC and NERC: CAD Files: stl text format

- FERC and NERC: CAD Files: stp text format
- FERC and NERC: CAD Files: WHIP
- FERC and NERC: CAD Files: x_t text format
- FERC and NERC: disclaimer
- FERC and NERC: form 567
- FERC and NERC: form 715
- FERC and NERC: Microsoft Visio
- FERC and NERC: pipeline flow diagrams

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 (Narrow) and Common Medical Condition
- FERPA: Name (Narrow) and Sensitive Disease or drug
- FERPA: Name and Common Medical Condition
- FERPA: Name and Sensitive Disease or drug
- 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: 10 Digit Account Numbers

- FFIEC: 5-8 Digit Account Numbers
- FFIEC: 9 Digit Account Numbers
- FFIEC: All Credit Card Numbers
- FFIEC: Credit Card Magnetic Strips
- FFIEC: Driver License
- FFIEC: Password dissemination for Web traffic
- FFIEC: PIN numbers
- FFIEC: SSN
- FFIEC: Suspected passwords
- FFIEC: TIFF format file type
- FFIEC: Zip codes with Financial Terms

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 Crimes
- FISMA: CCN and Ethnicities
- FISMA: CCN and Sensitive Disease or drug
- FISMA: Confidential in Document
- FISMA: Network Information and Security (patterns and IP)
- FISMA: Network Information and Security (textual patterns)
- FISMA: Password dissemination for Web traffic
- FISMA: Proprietary in Document
- FISMA: SSN and Crimes
- FISMA: SSN and Ethnicities
- FISMA: SSN and Sensitive Disease or drug
- FISMA: Suspected Passwords

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

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 cards and Common Medical Condition
- HIPAA: Credit cards and Sensitive Disease or drug
- HIPAA: DNA profile (default)
- HIPAA: DNA profile (narrow)
- HIPAA: DOB and Name (default)
- HIPAA: DOB and Name (wide)
- HIPAA: ICD10 Code and Description
- HIPAA: ICD10 Codes and US full names
- HIPAA: ICD10 Descriptions and US full names
- HIPAA: ICD9 Code and Description
- HIPAA: ICD9 Codes and US full names
- HIPAA: ICD9 Descriptions and US full names
- HIPAA: Medical Form (Default)
- HIPAA: Medical Form (Narrow)
- HIPAA: Medical Form (Wide)
- HIPAA: Name and Common Medical Condition
- HIPAA: Name and Contact Info

- HIPAA: Name and HICN
- HIPAA: Name and Sensitive Disease or drug
- HIPAA: Names (Narrow) and Common Medical Condition
- HIPAA: Names (Narrow) and Sensitive Disease or drug
- HIPAA: NDC number (default)
- HIPAA: NDC number (narrow)
- HIPAA: NDC number (wide)
- 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 Documents
- MITS - Password dissemination for Web traffic
- MITS - Proprietary in Document
- MITS - Suspected Passwords
- MITS: Network Information and Security (patterns and IP)
- MITS: Network Information and Security (textual patterns)
- MITS: SIN and CCN
- MITS: SIN and Common Medical Condition
- MITS: SIN and Sensitive Disease or drug
- MITS: SIN with proximity

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: SOX terms
- SOX: Form 10K
- SOX: Form 10K - Non Std fiscal year
- SOX: Form 10Q
- SOX: Form 10Q - Non Std fiscal year

Data Theft Risk Indicators

TRITON AP-DATA includes the following types of Data Theft Risk Indicator policies:

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

- Database Files

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

  - Database File: Ability Office format
  - 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

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
- Password dissemination for Web traffic
- Password Dissemination: Common Passwords without term

● 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 rule for this policy is also called:

- Suspected Mail to Self
- Source Code C Family or Java in Suspected Mail to Self
- Confidential in Header/Footer in Suspected Mail to Self
- Office Files Sent Over Time in Suspected Mail to Self

- Archive Files Sent Over Time in Suspected Mail to Self
- Encrypted Files of Unknown Format in Suspected Mail to Self
- Encrypted Files of Known Format in Suspected Mail to Self
- Database Files in Suspected Mail to Self
- Python Source Code in 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. (Forcepoint-supported file types do not trigger this policy.)

  For example: If 50 unencrypted files of an unknown format are sent during 1 hour, this policy is triggered. Thresholds are set in the Wide or Default rule."

  - 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: Specific Attachments
  - User Traffic Over Time: CV
  - User Traffic Over Time: Source Codes

Indicators of Compromise

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

- 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 TRITON AP-WEB is installed. Rules in this policy include:

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

- 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:

  - Counter Malicious: Dubious Content
  - Counter Malicious: Encrypted files (known format)

- ■ Counter Malicious: Generic Encryption Detection

- ■ Counter Malicious: Generic Encryption Detection (Wide)

- ■ Counter Malicious: Malicious Concealment

- ■ Counter Malicious: Password files

- ■ Counter Malicious: Password Information

- ■ Counter Malicious: Suspected Applications (Steganography and Encryption)

- Encrypted Files

  Policy for detection of desktop encrypted files. Should be complemented with the unknown file type policy for unknown encryption formats. The rules for this policy are:

  - ■ Encrypted File: Word Binary File (Legacy)

  - ■ Encrypted File: Excel Binary File (Legacy)

  - ■ Encrypted File: Access Database File (Legacy)

  - ■ Encrypted File: Microsoft Office Encrypted Files (OOXML)

  - ■ Encrypted File: PowerPoint Binary File (Legacy)

  - ■ Encrypted File: PDF - encrypted

  - ■ Encrypted File: ZIP archive - encrypted

  - ■ Encrypted File: RAR archive - encrypted

  - ■ Encrypted File: PGP signed and encrypted data format

  - ■ Encrypted File: PGP encrypted data format

  - ■ Encrypted File: Encrypted data of unknown 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: General files

  - ■ Password Files: .htpasswd Files (Default)

  - ■ Password Files: .htpasswd Files (Narrow)

  - ■ Password Files: .htpasswd Files (Wide)

  - ■ Password Files: Password Files

  - ■ Password Files: Password Files (Wide)

  - ■ Password Files: SAM Files (Default)

  - ■ Password Files: SAM Files (Narrow)

  - ■ Password Files: SAM Files (Wide)

  - ■ Password Files: Shadow Files

  - ■ Password Files: Shadow Files (Wide)

- PKCS #12 Files

  Policy for detecting PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate. The rule for this policy is:

  - ? PKCS #12 Files

Employee Discontent

- 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)

- Resume for HR

  Policy for detection of documents comprising resumes (CVs), as part of policy pertaining to Human Resources (HR) information. The rule for this policy is:

  - HR: CV policy

- Resume for HR Cyrillic

  Policy for detection of documents comprising resumes (CVs). The policy contains rules to detect CVs in English and in Russian or Ukrainian. The rules for this policy are:

  - HR Cyrillic: CV in English
  - HR Cyrillic: CV in Russian or Ukrainian

- Resume for HR Israel

  Policy for detection of documents comprising resumes (CVs). The policy contains rules to detect CVs in English and in Hebrew. The rules for this policy are:

  - HR Israel: CV policy in English
  - HR Israel: CV policy in Hebrew

- Self CV Distribution
- Policy for detecting employees who distribute their 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)

Quick Policies

TRITON AP-DATA includes the following types of quick policies:

- *Web DLP policy*, page 81
- *Email DLP policy*, page 82
- *Mobile DLP policy*, page 83

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 TRITON AP-WEB is installed. Rules in this policy include:

■ Suspected Malware Communication (Default)

■ Suspected Malware Communication (Narrow)

● 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 like HTTP 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 TRITON AP-WEB is installed. Rules in this policy include:

  - Number of HTTP Posts per Time
  - Cumulative Post Size per Time
  - Cumulative Generic Encryption per Time

Email DLP policy

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.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

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

● 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

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

● 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

● 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:
  - ■ UTM Location Coordinates
  - ■ Lat-Long Location Coordinates
- ● 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:
  - ■ Logs and Survey Reports
  - ■ Lat-Long Location Coordinates
  - ■ UTM Location Coordinates

- ■ Petroleum File Extensions
- ■ Prospecting Related Terms
- ● 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

- ● Resume for English HR for Discovery

  Policy for detection of documents comprising resumes (CVs), as part of a policy pertaining to Human Resources (HR) information. The rule for this policy is:
  - ■ HR: CV policy
- ● Resume for Israel for Discovery

  Policy for detection of documents comprising resumes (CVs) in Hebrew. The rule for this policy is:
  - ■ HR Israel: CV in Hebrew
- ● HR for Russia and Ukraine for Discovery

  Policy for detection of documents comprising resumes (CVs) in Russian or Ukrainian, as part of a policy pertaining to Human Resources (HR) information. The rule for this policy is:
  - ■ HR Cyrillic: CV in 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

- 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

- 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)

- 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)

● 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)

● Peoples Republic of China for Discovery

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

- ■ Peoples Republic of China Finance: Business Registration Number - 15 digits
- ■ Peoples Republic of China Finance: Credit Card
- ■ Peoples Republic of China Finance: Financial cards Track1
- ■ Peoples Republic of China Finance: Financial cards Track2
- ■ Peoples Republic of China Finance: Financial cards Track3
- ■ Peoples 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)

● 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

● 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)

● 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 Information for Discovery:

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

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

● 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)

● W-2 Forms for Discovery

Policy for the detection of tax W-2 forms. The rule for this policy is:

- W-2 form

Indicators of Compromise

- 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:

  - Counter Malicious: Dubious Content
  - Counter Malicious: Encrypted files (known format)
  - Counter Malicious: Generic Encryption Detection
  - Counter Malicious: Generic Encryption Detection (Wide)
  - Counter Malicious: Malicious Concealment
  - Counter Malicious: Password files
  - Counter Malicious: Password Information
  - Counter Malicious: Suspected Applications (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 Policy 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: CCN - High Accuracy
  - PCI Audit: CCN in non-English characters
  - PCI Audit: CCN with CVV
  - PCI Audit: CCN with Exp date
  - PCI Audit: CCN without validation
  - PCI Audit: CCN User-Defined IINs (Wide)
  - PCI Audit: CCN User-Defined IINs (Default)
  - PCI Audit: CCN User-Defined IINs (Narrow)
  - PCI Audit: Credit Card Magnetic Strips
  - PCI Audit: Masked Credit Cards
  - PCI Audit: No Word Boundaries

- ■ PCI Audit: Non-Delimited
- ■ PCI Audit: User-Defined Delimiter
- ■ PCI Audit: Wide
- ● 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)

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

- ● Australia PHI for Discovery

  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: SPSS Text files
- ● Health data For Discovery

  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 Cards and Sensitive Disease or Drug
  - ■ Health Data: DNA profile (Default)
  - ■ Health Data: DNA profile (Narrow)
  - ■ Health Data: DOB and Name
  - ■ Health Data: ICD10 Code and Description
  - ■ Health Data: ICD10 Codes
  - ■ Health Data: ICD10 Codes and US full names
  - ■ Health Data: ICD10 Descriptions and US full names
  - ■ Health Data: ICD9 Code and Description
  - ■ Health Data: ICD9 Codes
  - ■ Health Data: ICD9 Codes and US full names
  - ■ Health Data: ICD9 Descriptions and US full names

- ■ Health Data: Medical Form (Default)
- ■ Health Data: Medical Form (Narrow)
- ■ Health Data: Medical Form (Wide)
- ■ 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
- ● 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: ID and Sensitive Medical Information
  - ■ Israel PHI: Name and Sensitive Medical Information
  - ■ Israel PHI: ID and General Medical Information
  - ■ Israel PHI: Name and General Medical Information
  - ■ Israel PHI: SPSS Text files
- ● Italy PHI Policy For Discovery

  Policy for detection of protected health information for Italy citizens. The rules for this policy are:
  - ■ Italy PHI: Name and health information
  - ■ Italy PHI: Codice Fiscale and health information
  - ■ Italy PHI: SPSS Text files
- ● Norway PHI For Discovery

  Policy for detection of protected health information for Norwegian citizens. The rules for this policy are:
  - ■ 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 number
  - ■ Norway PHI: ICD10 Codes
  - ■ Norway PHI: ICD10 Descriptions
  - ■ Norway PHI: Name and health information
  - ■ Norway PHI: Personal Number and health information
  - ■ Norway PHI: SPSS Text files
- ● 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: DNA profile
- Sweden PHI: ICD10 Code and Description
- Sweden PHI: ICD10 Code and Name
- Sweden PHI: ICD10 Code and Name (Narrow)
- Sweden PHI: ICD10 Code and Name (Wide)
- Sweden PHI: ICD10 Code and Personal Number
- Sweden PHI: ICD10 Codes
- Sweden PHI: ICD10 Descriptions
- 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

- UK For Discovery

  Policy for detection of UK NHS numbers.The rules for this policy are:
  - UK PHI: NHS Numbers
  - UK PHI: NHS Numbers (narrow)
  - UK PHI: SPSS Text files

- US PHI For Discovery

  A policy for detection of protected health information of US citizens. The rules for this policy are:
  - US PHI: Name and Common Medical Condition
  - US PHI: Name and HICN
  - US PHI: Name and Sensitive Disease or Drug
  - US PHI: Names (Narrow) and Common Medical Condition
  - US PHI: Names (Narrow) and Sensitive Disease or drug
  - US PHI: SPSS Text files
  - US PHI: SSN and Common Medical Condition
  - US PHI: SSN and Sensitive Disease or Drug

Personally Identifiable Information (PII)

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

- Australia Private information for Discovery

  Policy to detect files containing personally identifiable information for residents of Australia. The rules for this policy are:
  - Australia PII: Australia TFN

- - Australia PII: Australia Driver License
- Belgium PII for Discovery

  Policy for detection of Belgian private information. The rules for this policy are:
  - Belgium PII: Name and ID Card Number (Wide)
  - Belgium PII: Name and ID Card Number (Default)
  - Belgium PII: Name and Passport (Wide)
  - Belgium PII: Name and Passport (Default)
  - Belgium PII: ID Card Numbers
  - Belgium PII: Passport Numbers
- Brazil Private Information 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: Name and CPF
  - Brazil PII: Name and Health
  - Brazil PII: CPF and Health
  - Brazil PII: RG Numbers
- Canada PII for Discovery

  Policy for detection of Canadian private information. The rules for this policy are:
  - Canada PII: SIN + Name
  - Canada PII: Name and Canadian Driver License
- Credit Card Numbers for Discovery

  Policy for detection of credit card numbers. The rules for this policy are:
  - Credit Cards - Wide
  - Credit Cards - Default
  - Credit Cards - Narrow
  - Japanese Credit Cards: All Credit Cards
- Czech Republic PII for Discovery

  Policy for detection of Czech Republic private information. The rules for this policy are:
  - Czech Republic PII: Rodne Cislo (wide)
  - Czech Republic PII: Rodne Cislo (default)
- Denmark Private Information for Discovery

  Policy for detection of Danish personally identifiable information. The rule for this policy is:
  - Denmark PII: CPR Numbers
- 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

- Finland Private Information for Discovery

  Policy for detection of Finnish personally identifiable information. The rule for this policy is:

  - Finland PII: SSN (Default)

- France Private information for Discovery

  Policy for detection of French personally identifiable information. The rule for this policy is:

  - France PII: INSEE numbers

- General Sensitive Private 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:

  - Sensitive Private: Credit Card Magnetic Strips
  - Sensitive Private: DNA profile
  - Sensitive Private: EU Credit Card Number
  - Sensitive Private: Name and Account Numbers
  - Sensitive Private: Name and Crime
  - Sensitive Private: Name and Ethnicity
  - Sensitive Private: Name and Grade
  - Sensitive Private: Name and Sensitive Disease
  - Sensitive Private: Passwords
  - Sensitive Private: PIN numbers
  - Sensitive Private: US Credit Card Number

- Germany Private Information for Discovery

  Policy to detect private and sensitive information in German, for German-speaking countries. The rules for this policy are:

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

- Greece Private Information for Discovery

  Policy for detection of Greek personally identifiable 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: ID (Default)
- ■ Greece PII: ID and Name (Default)
- ■ Greece PII: ID and Name (Wide)
- ■ Greece PII: Sensitive Medical Information and Name (Default)
- ■ Greece PII: Sensitive Medical Information and Name (Wide)
- ● Honk Kong PII: Sensitive Medical Information and Name (Default)Hong Kong Private Information for Discovery

  Policy to detect files containing personally identifiable information for residents of Hong Kong. The rules for this policy are:

  - ■ Hong Kong PII: Common Surname and Address (default)
  - ■ Hong Kong PII: Common Surname and Address (narrow)
  - ■ Hong Kong PII: Common Surname and Address (wide)
  - ■ Hong Kong PII: Hong Kong ID - default
  - ■ Hong Kong PII: Hong Kong ID - wide
  - ■ Hong Kong PII: Hong Kong ID (default pattern) and Common Address
  - ■ Hong Kong PII: Hong Kong ID (default pattern) and Common Surname
  - ■ Hong Kong PII: Hong Kong ID (default pattern) with Common Surname and Address
  - ■ Hong Kong PII: Hong Kong ID (formal form) and Common Address
  - ■ Hong Kong PII: Hong Kong ID (formal form) and Common Surname
  - ■ Hong Kong PII: Hong Kong ID (formal form) with Common Surname and Address
  - ■ Hong Kong PII: Hong Kong ID (wide) and Common Address
  - ■ Hong Kong PII: Hong Kong ID (wide) and Common Surname
  - ■ Hong Kong PII: Hong Kong ID (wide) and Common Surname and Address
  - ■ Hong Kong PII: Hong Kong ID formal form
- ● 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 Private Information for Discovery

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

  - India: Form 16
  - India: PAN

- Ireland Private Information for Discovery

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

  - Ireland PII: Irish Personal Public Service Number (PRSI/PPS) and Name
  - Ireland PII: Driver Number
  - Ireland PII: Passport Number

- Israel Data For Discovery

  Policy to identify files containing Israeli confidential and private information. The rules for this policy are:

  - Israel PII: Israeli ID
  - Israel PII: IsraCard
  - Israel PII: CV policy in Hebrew
  - Israel PII: ID and Sensitive Medical Information
  - Israel PII: Name and Sensitive Medical Information
  - Israel PII: ID and General Medical Information
  - Israel PII: Name and General Medical Information
  - Israel PII: Name and ID

- Italy Private Information for Discovery

  Policy to detect private and sensitive information in Italy, including health information. The rules for this policy are:

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

- Japan Private Information for Discovery

  Policy to detect private and sensitive information in Japan. The rules for this policy are:

  - Japan PII: All Credit Cards
  - Japan PII: Individual Numbers (Default)
  - Japan PII: Corporate Numbers (Default)

- 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)

- Macau Private Information for Discovery

  Policy to detect files containing personally identifiable information for residents of Macau. The rules for this policy are:
  - Macau PII: Macau ID formal form
  - Macau PII: Macau ID
  - Macau PII: Macau ID- 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

- Mexico Private Information for Discovery

  Policy for detection of Mexican Personal Information. The rules for this policy are:
  - Mexico PII: Mexico RFC
  - Mexico PII: CURP (Default)
  - Mexico PII: CURP (Narrow)
  - Mexico PII: CPISP (Default)
  - Mexico PII: CPISP (Narrow)
  - Mexico PII: SSP Contratos Internos Detection

- Netherlands Private Information for Discovery

  Policy to detect private and sensitive information in Dutch, for Dutch-speaking countries. The rules for this policy are:
  - DUTCH PII: Driver License Numbers
  - DUTCH PII: Passport Numbers
  - DUTCH PII: Sofi and Account with Password
  - DUTCH PII: Sofi and CCN
  - DUTCH PII: Sofi and Crime
  - DUTCH PII: Sofi and Diseases
  - DUTCH PII: Sofi and Ethnicities

- New Zealand Private Information for Discovery

Policy to detect files containing personally identifiable information for residents of New Zealand. The rule for this policy is:

■ New Zealand PII: New Zealand NHI number

● Norway Private Information for Discovery

Policy to detect private and sensitive information in Norway, including health information. The rules for this policy are:

■ Norway: Personal Number

■ Norway: Name and Personal Number

■ Norway: Name and health information

■ Norway: Personal Number and health information

● Peoples Republic of China Private Information for Discovery

Policy to detect files containing personally identifiable information for residents of People Republic of China. The rule for this policy is:

■ People Republic of China PII: People Republic of China ID

● Peoples Republic of China PII for Discovery

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

■ Peoples Republic of China PII: ID

■ Peoples Republic of China PII: Chinese CV

● Philippines PII for Discovery

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

■ Philippines PII: Name and Address

● Poland Private Information for Discovery

Policy for detection of personal information for residents of Poland. The rules for this policy are:

■ Poland : IBAN and Name

■ Poland : NIP and Name

■ Poland : NIP with proximity

■ Poland : PESEL and Name

■ Poland : PESEL with proximity

■ Poland : Polish ID and Name

■ Poland : Polish ID with proximity

■ Poland : REGON and Name

■ Poland : REGON with proximity

● Romania PII for Discovery

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

■ Romania PII: Personal numeric code

● Russia Private Information for Discovery

Policy for detection of Russian personally identifiable information. The rules for this policy are:

- ■ Russia PII: Passport numbers
- ■ Russia: passport and name

● Singapore Private Information for Discovery

Policy to detect files containing personally identifiable information for residents of Singapore. The rule for this policy is:

- ■ Singapore PII: Singapore Identification numbers

● Slovakia Private Information for Discovery

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

- ■ Slovakia PII: Rodne Cislo (wide)
- ■ Slovakia PII: Rodne Cislo (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 Private Information for Discovery

Policy for detection of personal information of South African citizens. The rule for this policy is:

- ■ South African ID

● South Korea Private Information for Discovery

Policy to detect files containing personally identifiable information for residents of South Korea. The rules for this policy are:

- ■ South Korea PII: South Korea ID
- ■ South Korea PII: Korea Phones (with proximity)

● Spain Private Information 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 and Account with Password
- ■ Spain PII: DNI and CCN
- ■ Spain PII: DNI and Crime
- ■ Spain PII: DNI and Diseases
- ■ Spain PII: DNI and Ethnicities
- ■ Spain PII: DNI numbers
- ■ Spain PII: Spanish Name + Address (default)

- ■ Spain PII: Spanish Name + Address (narrow)
- ■ Spain PII: Spanish Name + CCN
- ■ Spain PII: Spanish Name + DNI
- ■ Spain PII: Spanish Name + IBAN
- ■ Spain PII: Spanish Name + Passport
- ■ Spain PII: Spanish Names + Email Addresses
- ■ Spain PII: Spanish Names + Phone Numbers
- ● Sweden Private Information for Discovery

  Policy for detection of Swedish personally identifiable information. The rule for this policy is:

  - ■ Sweden PII: Swedish ID
- ● Switzerland Private Information for Discovery

  Policy for detection of Swiss personally identifiable information. The rule for this policy is:

  - ■ Switzerland PII: new format AHV numbers
- ● Taiwan Private Information for Discovery

  Policy to detect files containing personally identifiable information for residents of Taiwan. The rules for this policy are:

  - ■ Taiwan PII: Taiwan ID formal form
  - ■ Taiwan PII: Taiwan ID
- ● Thailand Private Information for Discovery

  Policy for detection of Thai personally identifiable information. The rule for this policy is:

  - ■ Thailand: National ID (default)
- ● Turkey Private Information for Discovery

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

  - ■ Turkey PII: TC Kimlik
  - ■ Turkey 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: Postal Code
  - ■ UK PII: Sort Code
  - ■ UK PII: UK Driver Number
  - ■ UK PII: UK National Insurance Number
  - ■ UK PII: UK Passport Number

- UK PII: UK 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: CCN and SSN

- US PII: Name and ITIN

- US PII: Name and SSN

- US PII: Name and US Address

- US PII: Name and US Address - Wide

- US PII: Name and US Driver License

- US PII: SSN

Regulations

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

- 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

- Nevada SB 227 and NRS 603A for Discovery

Nevada SB 227 and NRS 603A require that organizations or business entities in Nevada shall not disseminate unencrypted personal information and shall not move any data storage device containing unencrypted personal information outside of the secure system of the business. NRS 603A also mandates notification of the breach to any resident of this State whose unencrypted personal information is reasonably believed to have been acquired by an unauthorized person. The pre-defined policy detects Personally Identifiable Information (PII) that should be encrypted, like full names with social security numbers, Nevada driver license, credit card numbers, and passwords. The rules for this policy are:

- Nevada SB 227 and NRS 603A: Account and Password

- Nevada SB 227 and NRS 603A: Name and CCN

- Nevada SB 227 and NRS 603A: Name and DL

- Nevada SB 227 and NRS 603A: Name and ID

- Nevada SB 227 and NRS 603A: Name and Password

- Nevada SB 227 and NRS 603A: Name and SSN
        - Nevada SB 227 and NRS 603A: Name with Account and Password
- 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. 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: SOX terms
        - SOX: Form 10K
        - SOX: Form 10Q
- 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 Files
        - SFS 2008:355: DNA profile
        - SFS 2008:355: ICD10 Code and Description
        - SFS 2008:355: ICD10 Code and Name
        - SFS 2008:355: ICD10 Code and Name (Narrow)
        - SFS 2008:355: ICD10 Code and Name (Wide)
        - SFS 2008:355: ICD10 Code and Personal Number
        - SFS 2008:355: ICD10 Codes
        - SFS 2008:355: ICD10 Descriptions
        - 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 files
- 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

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

- Database Files for Discovery

  Policy for the detection of database files. The rules for this policy are:
  - Database File: Ability Office format
  - 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 formatDatabase 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

Predefined Classifiers

This article provides a list of all the predefined content classifiers that TRITON AP-DATA provides for detecting events and threats involving secured data. This includes:

- *File-type classifiers*
- *NLP scripts*
- *Dictionaries*
- *Regular Expression patterns*

The classifiers are constantly being updated and added to. See Updating Predefined Policies and Classifiers for instructions on keeping your classifiers current.

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.
Ability Database File	Detection of Ability Office Database file format according to internal file properties.
Access Database Template Files (.accdt)	Detection of Access Database Template files (.accdt) created in Office 2007 or later.
AD1 Evidence File	Detection of AD1 evidence files
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 DWG File	Detection of Autodesk DWG CAD file format according to internal file properties.
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.
BlackBerry Activation File (etp.dat)	Detection of BlackBerry Activation files (etp.dat)
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.
Disk Image	Detection of Disk Image
Documentum EMCMF format (.emcmf)	Detection of Documentum EMCMF format (.emcmf)
eFax file	Detection of eFax file
Electronic Publication	Detection of Electronic Publication
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.

Encrypted Excel Binary File (Legacy)	Detection of password protected Microsoft Excel Binary files (.xls) that were created before Office 2007 according to internal file properties.
Encrypted Files of Known Formats	Detects encrypted PGP files or password-protected ZIP archives, RAR archives, Microsoft Office Word, Excel and PowerPoint files (both OOXML and Legacy), Access Database files (Legacy), PDF documents or Nero files according to internal properties.
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 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.
Ghost Disk Image File (*.gho, *.ghs)	Detection of Ghost Disk image files (*.gho, *.ghs)
Google SketchUp Format (.skp)	Detection of Google SketchUp format (.skp)
Health level7 Message File	Detection of Health Level 7 file format.
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).
IFilter File	Detection of iFilter file format.
JBIG2 File Format(.jB2, .jbig2)	Detection of JBIG2 file format (.jB2, .jbig2)
JPEG-2000 JP2 File Format Syntax (ISO/IEC 15444-1) (.jp2, .j2k , .pgx)	Detection of JPEG-2000 JP2 file format syntax (ISO/IEC 15444-1) (.jp2, .j2k , .pgx)
JT Assembly File	Detection of JT Assembly 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.

Microsoft Access File - All Versions	Detection of Microsoft Access database files (all versions) according to internal file properties.
Microsoft Compiled HTML Help (.chm)	Detection of Microsoft Compiled HTML Help (.chm)
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 File - Non-RMS-Protected	Detection of older versions of Microsoft Office documents (such as doc, xls, and ppt) that are protected by Windows Rights Management Services (RMS) and all versions (new and old) of Office documents that are not protected by RMS (such as doc, docx, xls, xlsx, etc.). 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 Outlook Express DBX	Detection of Microsoft Outlook Express DBX
Microsoft Outlook OST	Detection of Microsoft Outlook OST
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 Project File - All Versions	Detection of Microsoft Project files (all versions) according to internal file properties.
Microsoft Visio File - All Versions	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.
Milestone Document (.mls,.ml3,.ml4,.ml5,.ml6,.ml7,.ml8,.ml9)	Detection of Milestone Document (.mls,.ml3,.ml4,.ml5,.ml6,.ml7,.ml8,.ml9)
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.
Nero Encrypted File	Detection of encrypted nero files according to internal properties.
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.
PostScript Type 1 Font (*.pfb)	Detection of PostScript Type 1 Font (*.pfb)
PRO/Engineer Format (.asm)	Detection of PRO/Engineer Format (.asm)
PRO/Engineer Format (.drw)	Detection of PRO/Engineer Format (.drw)
PRO/Engineer Format (.frm)	Detection of PRO/Engineer Format (.frm)
PRO/Engineer Format (.prt)	Detection of PRO/Engineer Format (.prt)
RealLegal E-Transcript File(*.ptx)	Detection of RealLegal E-Transcript File(*.ptx)
RMS-Protected Microsoft Office File	Detection of Outlook Restricted-Permission Message (RPMSG) files and Microsoft Office Open XML files that are protected by Windows Rights Management Services (RMS). Open XML files include Word, Excel, PowerPoint and other Office documents created in Office 2007 or later.

Samsung Electronics Jungum Global document (*.gul)	Detection of Samsung Electronics Jungum Global document (*.gul)
Shell Scrap Object File (.shs)	Detection of Shell Scrap Object file format.
Skype Log File	Detection of Skype log files.
SmartWare II Database File	Detection of SmartWare II database files according to internal file properties.
Solid Works File	Detection of SolidWorks files.
STL CAD binary format	Detection of STL CAD binary file
Tagged Image File Format (TIFF) File	Detection of TIFF (Tagged Image File Format) files according to internal properties.
Unicode HTML	Detection of Unicode HTML
Unknown format	Detects files of an unknown format (i.e., those that are not Forcepoint-supported file types).
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 Formats	Detection of Microsoft Access and Microsoft Project.
Various Executables Formats	Detection of Windows Executable files and Link Libraries.
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, 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, 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, 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).
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.
XML Format	Detection of XML files according to internal file properties.
ZIP File	Detection of all unencrypted ZIP files

NLP scripts

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

This section contains the full list of natural language processing scripts provided by Forcepoint. You can edit the classifiers as needed. For information, see Editing a predefined script.

Classifier	Description
10K Form	Detection of 10K forms.
10K Form (Non Standard Fiscal Year)	Detection of 10K forms for non standard fiscal years (not ending at 31/12).
10Q Form	Detection of 10Q forms.
10Q Form (Non Standard Fiscal Year)	Detection of 10Q forms for non standard fiscal years (not ending at 31/12).
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 TFN	Detection of an Australian Tax File (TFN) numbers.
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.
Brazilian CPF Number	Detection of validated Brazil CPF numbers.
Brazilian Name	Detection of Brazilian full names.
CAD stl text format	Detection of CAD stl text files
CAD stp text format	Detection of CAD stp text files
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.

Classifier	Description
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.
Chinese Credit Cards (Default)	Detection of credit card numbers used in the Peoples 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 Peoples 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.
Chinese Credit Cards (Wide)	Detection of potential credit card numbers used in the Peoples 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.
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).
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.
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.

Classifier	Description
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 dedit card numbers employing various heuristics involving credit card related terms and use of delimiters.

Classifier	Description
Credit Cards: User-Defined IINs (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. You can edit both files in the /policies_store/policies/scripts/ directory where TRITON AP-DATA is installed. Deploy your settings in the Data Security manager to apply your changes. This classifier may cause false positives.
Credit Cards: User-Defined IINs (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. You can edit both files in the /policies_store/policies/scripts/ directory where TRITON AP-DATA is installed. Deploy your settings in the Data Security manager to apply your changes.
Credit Cards: User-Defined IINs (Narrow)	A restricted 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. You can edit both files in the /policies_store/policies/scripts/ directory where TRITON AP-DATA is installed. Deploy your settings in the Data Security manager to apply your 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.
CV in Chinese (default)	Detection of Curriculum Vitae (CV) in Chinese, using location sensitive lexical analysis of terms and patterns common in such documents. Default version.
CV in Chinese (narrow)	Detection of Curriculum Vitae (CV) in Chinese, using location sensitive lexical analysis of terms and patterns common in such documents. Narrow version.
CV in Chinese (wide)	Detection of Curriculum Vitae (CV) in Chinese, using location sensitive lexical analysis of terms and patterns common in such documents. Wide version.
CV in English (new in	Detection of Curriculum Vitae (CV) in English, using location sensitive lexical analysis of terms and patterns common in such documents.
CV in Russian or Ukraine	Detection of Curriculum Vitae (CV) in Russian or Ukrainian, using location sensitive lexical analysis of terms and patterns common in such documents.
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 Phrase 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".
Document to Self (Default)	Detection of people sending documents to their personal email address.

Classifier	Description
Document to Self (Wide)	Loose detection of people sending documents to their personal email address.
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.
EAR - Chemical Data Detection (Default)	Detection of chemical formulas and information related to composite materials.
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).
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)

Classifier	Description
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.
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.
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.
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).
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).
Hong Kong: ID - non formal	Detection of Hong Kong ID of the form A1234567, without requiring ID terms.

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".
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.

Classifier	Description
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 Czech Republic	Detection of Czech IBANs (International Bank Account Numbers). Searches for support terms in proximity to Czech IBAN format.
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.

Classifier	Description
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.
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 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 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 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 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.
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.

Classifier	Description
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.
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.

Classifier	Description
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: General Medical Info	Detection of medical conditions in Hebrew or English.
Israel: Sensitive Medical Info	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.
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.

Classifier	Description
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.
Isreali generic insurance number (delimited)	Detection of generic Israeli insurance policy numbers in standard delimitation
Isreali 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.

Classifier	Description
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".
Kazakh Taxpayer Registration Numbers	Detection of valid Kazakh Taxpayer Registration Numbers.
Kazakh Individual Identification Numbers	Detection of valid Kazakh Individual Identification Numbers.
Kazakh Business Identification Numbers	Detection of valid Kazakh Business Identification Numbers.
Key Phrase 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 on the texts "Secretive and highly classified" and "TOP SECRET".
Korea Phone Numbers (Narrow)	Detection of Korea phone numbers, employing statistical analysis.

Classifier	Description
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.
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.
Malicious Concealment: L33T (Narrow)	Detection of content suspected to be manipulated using "L33T" manipulation.

Classifier	Description
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.
Malware (Wide)	Detection of transactions that are suspected to be malicious, based on analysis of traffic of known infected machines (Wide). HTTP/S channel only. Applies only when TRITON AP-WEB is installed.
Malware (Default)	Detection of transactions that are suspected to be malicious, based on analysis of traffic of known infected machines (Default). HTTP/S channel only. Applies only when TRITON AP-WEB is installed.
Malware (Narrow)	Detection of transactions that are suspected to be malicious, based on analysis of traffic of known infected machines (Narrow). HTTP/S channel only. Applies only when TRITON AP-WEB is installed.
Malware (Strict)	Detection of transactions that are suspected to be malicious, based on analysis of traffic of known infected machines (Strict). HTTP/S channel only. Applies only when TRITON AP-WEB is installed.
Malware (Strict) (Uncategorized)	Detection of transactions that are suspected to be malicious, based on analysis of traffic of known infected machines (Strict)(Uncategorized). HTTP/S channel only. Applies only when TRITON AP-WEB is installed.
MAR: Actuary Reports	Detection of documents contain actuary reports (in attachments or files).
Mexican Names	Detection of full names (Wide). This content classifier should be used in conjunction with additional data as it is permissive.

Classifier	Description
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.
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.
Netherlands: Bank Account	Detection of Elfproef validated Dutch Bank Account numbers.
Netherlands: Bank Account with proximity	Detection of Elfproef validated Dutch Bank Account numbers, when found in proximity to bank account related terms, such as "giropas".
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.
Password Files	Detection of password files
Password Files (Wide)	Detection of password files
Passwords	Detection of passwords in proximity to a password term.
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.
Passwords - keyboard sequence	Detection of passwords comprised of adjacent keyboard sequences.
Passwords for HTTP	Detection of passwords in proximity to a password term. Should be used on HTTP channel.

Classifier	Description
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.
Perl Source Code (By Content)	Detection of Perl source code by content.
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.
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.
PRC Business Registration Numbers - 15 digits (default)	Detection of Peoples Republic of China's 15 digits Business Registration Numbers (default behavior)
PRC Business Registration Numbers - 15 digits (narrow)	Detection of Peoples Republic of China's 15 digits Business Registration Numbers (narrow behavior)
PRC Business Registration Numbers - 15 digits (wide)	Detection of Peoples 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.

Classifier	Description
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 Individual Personal Account Insurance number	Detection of Russian Individual Personal Account Insurance number
Russian Moscow Social Card number (SOCCARD)	Detection of Russian Russian Moscow Social Card (SOCCARD)
Russian Moscow Social Card serial number	Detection of Russian 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

Classifier	Description
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.
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.

Classifier	Description
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	Detection of valid South Africa ID numbers (looking for support terms or implying statistical validation).
South Africa ID (narrow)	Detection of valid South Africa ID numbers (looking for support terms and implying statistical validation).
South Africa ID (wide)	Detection of valid South Africa ID numbers (not looking for support terms).
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.
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.
SPSS data files: sps	Detection of SPSS (.sps) text files.

Classifier	Description
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)
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.
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.
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.

Classifier	Description
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.
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.

Classifier	Description
UK Voter Number	Detection of UK electoral roll numbers in proximity to related terms.
Uncategorized URL Detection	Detection of Uncategorized URLs. This uses the URL categories list. Supported only with Linking Service installed. Applies only when TRITON AP-WEB is installed.
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.
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 Age: greater than	Detection of ages greater then the age specified. Default age is 13.
US Age: smaller than	Detection of ages smaller then the age specified. Default age is 13.
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 Phone Numbers	Detection of US phone numbers.

Classifier	Description
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'.
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.
User-defined file types extension	Detection of specific file types (user-defined) according to their extension.
User-defined dictionary (non-unique)	Detection of keywords. The keywords are supplied as a parameter. In order to use it, insert keywords into the parameter, separated by a semicolon. Keywords are case-insensitive.
User-defined dictionary (unique)	Detection of keywords, where each keyword is counted only once. The keywords are supplied as a parameter to the script. In order to use it, insert keywords into the parameter, separated by a semicolon. Consider keyword unique appearances. Keywords are case-insensitive.
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.

Classifier	Description
W2 Form Support	Detection of IRS W2 forms
x86 Assembly Source Code	Detection of x86 Assembly Source Code.

Dictionaries

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

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.
Australian TFN Terms	Detection of Australian Tax File (TFN)-related terms.
Belgium: ID Card Number Terms	Detection of Belgium ID terms

Belgium: Passport Terms	Detection of Belgium passport terms
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 passwords in English	Detection of common English 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"
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 Ukraine support terms	Detection of a Curriculum Vitae in Russian or Ukrainian with support terms.
CV terms - Hebrew	Detection of 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.
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
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.
France: Diseases	Detection of sensitive health condition in French or in English.
Gambling (Chinese)	Detection of Tips, Terms, Online Casinos, Betting Pools
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
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 Hungray 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
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
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.
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.
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 - 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
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 releated terms to Russian Russian Primary State Registration 13 digits numbers
Support terms for Russian Primary State Registration 15 digits numbers	Detection of releated terms to Russian Russian Primary State Registration 15 digits numbers
Support terms for Russian Russian Classification on Objects of Administrative Division number	Detection of released terms to Russian Classification on Objects of Administrative Division numbers
Support terms for Russian Russian Taxpayer Identification numbers	Detection of released terms to Russian Taxpayer Identification numbers
Support terms for Russian Unified Classifier of Enterprises and Organizations numbers	Detection of released 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
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).

Regular Expression patterns

Predefined Policies and Classifiers | TRITON AP-DATA | Version 8.3.x

This section contains the full set of regular expression patterns provided by Forcepoint. You can also create new classifiers. For information, see Adding or editing a regular expression classifier.

Classifier	Description
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).

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.
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).
CV support - period of years	Detection of a period denoted by starting year and ending year (e.g. 1999-2002).
Cyber Bullying	Detection of expressions that are indicative of cyber bullying.
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.
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.
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).
Explicit Password	Detection of explicit password information (e.g. "password xxxx").
F# Source Code Extensions	Detection of F# files according to their extension.
Finland Swift codes	Detection of SWIFT codes for Finland major banks.
France Swift codes	Detection of SWIFT codes for France major banks.
General Password	Detection of passwords comprised of at least 5 characters (must include both letters and digits).
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
Honk Kong Swift codes	Detection of SWIFT codes for Honk 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 .
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.
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.
Netherland Swift codes	Detection of SWIFT codes for Netherland 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.
Password Terms	Detection of password related terms.
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.
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.
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.
SOX: 10Q Form Phrases	detection of 10Q Form Phrases
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.
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 Individual Personal Account Insurance numbers	Detection of related terms to Russian Individual Personal Account Insurance numbers
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).
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").
Zip Plus 4	Detection of Zip codes.