



DATASHEET (DATA CLASSIFICATION)

Fortra Data Classification for Government Agencies

PRODUCT SUMMARY

The Problem

Government agencies collect, use, and store personally identifiable information (PII) about citizens, employees, patients, and other individuals every day. Much of this sensitive information is held in unstructured formats such as documents, emails, and various other file types, but the exact location and storage of the data is difficult to track. This poses a significant risk for government agencies, as it is hard to protect data that is not understood or properly identified.

The escalation of security breaches involving PII has contributed to the loss of millions of records over the past number of years, and these breaches can harm both individuals and government agencies due to identity theft, loss of public trust, legal liability, or remediation costs.

Government agencies must act in a manner that recognizes the rights and privacy of individuals with respect to their personal information. While there is a recognized need for agencies to collect, use, and disclose personal information, they must follow such procedures with appropriate care.

- Detect and label PII and other sensitive data types
- Customize marking schema for specific compliance needs
- Safely share data across users, platforms, and devices
- Facilitate automated data classification
- Enhance efficacy of downstream security tools

The Solution

Fortra Data Classification provides government bodies the ability to identify the data they possess, be it PII or otherwise, using metadata tags. This data can be classified according to specific government regulations and standards, which not only helps to protect that data but educates and builds awareness of PII among employees, contractors, and partners. The classification of this data allows for the appropriate controls and protection to be put in place, based on specific mandated policies, ultimately ensuring the data within government agencies remains secure.

How Fortra's Data Classification Secures Sensitive Government Data

Fortra's Data Classification Suite (DCS) allows government agencies to easily identify PII and other varieties of sensitive information — including unstructured data — to help users make informed categorization decisions and facilitate accurate security automation. By identifying what sensitive information agencies have and how sensitive it is, their downstream security tools will understand how that data should be handled and which security controls should be applied.

Beyond its ease of use and practical benefits, DCS helps solve many agencies' data-security-related concerns:

Preventing Egress of Sensitive Information

DCS actively detects and labels sensitive information according to your agency's data security policies, ensuring only the correct and approved users can access that information — whether those users are internal or external.

Schema Flexibility for Specific Compliance Requirements

DCS allows agencies to fully customize their marking schemas according to specific regulations, standards, and operational needs, facilitating both manual and automated policy enforcement as a result.

Enforcing Proper Data Retention Policies

Agencies can use DCS to apply retention periods to their data at rest, ensuring sensitive information is governed and deleted according to relevant retention policies, and that retention actions are defensible in an audit.

Classifying Data Across All Platforms and Devices

DCS works across all major platforms and devices, ensuring that sensitive data remains secure and properly marked, no matter where that data lives.

Securing Data Sharing Between Users & Third Parties

DCS allows users to share sensitive information with each other, external agencies, and foreign bodies in line with their agency's security policies, ensuring only vetted and approved parties can access and handle that information.

Digital Transformation: Moving From Manual to Automated Classification Processes

DCS empowers government agencies to embrace digital transformation on their own terms. Each agency can choose to move from a fully manual process, to a system-guided solution, or to completely automated processes, based on requirements and needs.

Enhancing Policy Enforcement Capabilities

The persistent metadata DCS applies to sensitive information informs downstream security tools like DLP, making those tools' policy enforcement actions more accurate and strengthening your agency's greater security ecosystem.

Analytics for Improved Reporting Capabilities

Similarly, persistent metadata also provides agencies with the analytics and information necessary to generate reports and audit trails, delivering greater visibility without increasing overhead or disrupting user workflows.



Fortra.com