FORTRA™

SOLUTION BRIEF (DATA CLASSIFICATION)

APRA CPS 234 Compliance Support That Works For Your Business

Data Classification Suite (DCS) Delivers True Data Identity By Tagging Unstructured Data In Motion And At Rest.

DCS helps organisations across the finance and insurance sectors meet the information security regulations mandated by the Australian Prudential Regulation Authority (APRA) Prudential Standard CPS 234. Noncompliance with APRA can result in substantial fines as well as legal risks and damage to your organisation's reputation. A data breach resulting from noncompliance can also negatively affect consumer and investor confidence in your business.

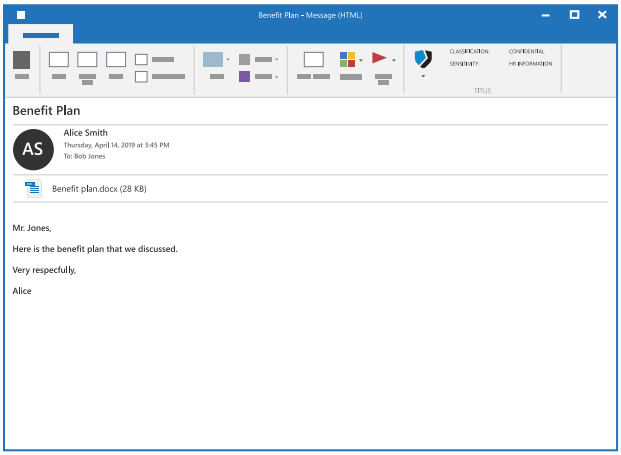
To mitigate these risks, you need a broad solution that can identify personal and sensitive information, classify it, and protect it across your entire security ecosystem. You need consistent, efficient protection throughout the data life cycle, whether it's in transit or at rest, on site or in the cloud. In addition, you need a way to educate users about the value of the data they handle from day to day. And, of course, you need to be able to prove compliance with privacy regulations such as APRA and others.

DCS solutions empower you to more efficiently manage all these dimensions of information security. Deep learning algorithms built into our solutions consistently identify sensitive data in context and automatically classify files in transit and at rest. Open, persistent metadata enables you to write custom identifiers, which in turn inform the other security solutions in your ecosystem, such as data loss prevention (DLP), encryption and rights management technologies, security information and event management (SIEM) solutions, and other technologies. Alerts keep users aware of sensitive data and offer suggestions for how to handle it, and audit logs help administrators keep track of security events and verify compliance.

> "Our members demand a high level of security and privacy for their data. DCS enables us to address the APRA requirement and, more important, it helps my colleagues recognise the value of our members' sensitive data. It complements our existing security technology stack and allows us to enforce data protection rules in an automated fashion."
>
> **— Wilson Chiu, Head of Security, Police Bank**

How DCS Supports Your Compliance

DCS works in concert with your existing cybersecurity infrastructure to help you achieve end-to-end compliance with privacy regulations. The open, configurable policy engine enables your organisation to enforce detailed information handling policies, tailored specifically to your business using award-winning machine learning algorithms.



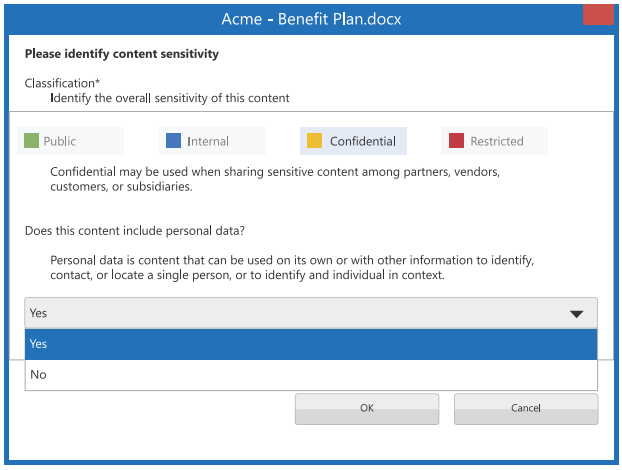
Discover

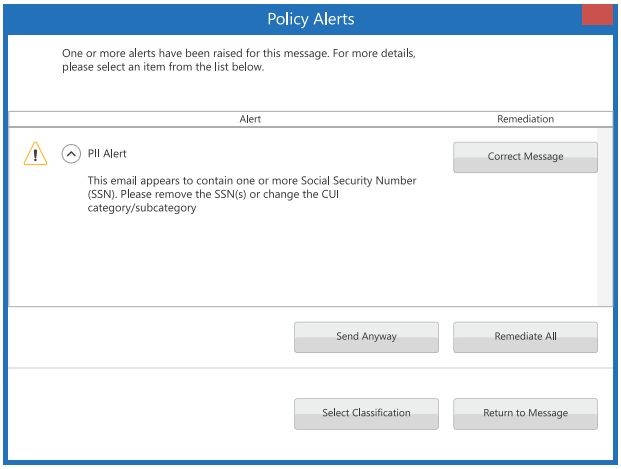
Sensitive information must be identified wherever it sits and however it is created. DCS solutions automatically enforce identification across platforms and devices via easily adoptable workflows to ensure protection of all your information.

Classify And Categorise All Data

The powerful DCS policy engine ensures that data is classified correctly according to your information security policy. Multiple layers of classification allow for highly granular control.

Deep learning AI technology can be deployed to assess your information, recognise sensitive data and autonomously determine appropriate categories.





Protect

DCS integrates with the other technologies in your security ecosystem, such as messaging, DLP and electronic data rights management (EDRM) solutions to enforce your information security policies using open, persistent metadata embedded in documents at creation or upon discovery.

Business leaders can give employees more freedom to innovate and have peace of mind knowing that sensitive information is safe.

The DCS platform supports compliance with the APRA Prudential Standard CPS 234 for information security through the following features and capabilities.

Information Security Foundation

DCS builds and maintains a foundation for your security capability, supporting both your technology infrastructure and your users. The DCS solution can discern the context of data, continuously safeguarding information across many systems by helping users understand its value and by informing your other security technologies.

Policy Framework

Your policy framework defines the value of your information. DCS enables you to build a powerful but flexible framework, customised to your organisation and the specific types of information and forms you use. Revisions can be quickly made and applied to respond to changing vulnerabilities and threats.

Information Asset Identification And Classification

DCS identifies sensitive information as it is created or when it enters your organisation from an outside source. Your policy framework is applied, and files are classified to a highly granular level, which is built in to the datafile. Advanced machine learning can also be enabled to suggest or enforce classifications.

Implementation Of Controls

The controls across your entire security infrastructure must adhere to your policy. DCS prevents unauthorised data access, transmission or loss on any device, whether in your offices or via the cloud. All data files are permanently marked with open metadata, which triggers DLP, email encryption, rights management and other solutions to apply your privacy restrictions as well.

Security policies must apply throughout the information life cycle. That's why DCS classifications impose appropriate storage, transmission, archiving and destruction parameters. Watermarking also permanently identifies classifications and reminds employees of the value of your sensitive information.

As users change roles and departments, and eventually leave the organisation, their access control rights must keep up with their status. DCS allows multiple classifications to strengthen control of the information users can access.

Incident Management

Organisations must be warned of immediate and long-term threats. DCS can scan for anomalous behaviour, such as repeated downclassifying and downloads at unexpected times of day, and then flag it for administrators.

Testing Control Effectiveness

Controls must be thoroughly tested across your organisation as well as any third-party organisations you work with on a regular basis. Use DCS to support end-to-end testing by creating test data with combinations of classifications and monitor the effectiveness of your employee training.

Internal Audit

DCS supports internal audits by logging users' data classification compliance levels with standard and enhanced audit logging capabilities. Audit logs support incident management processes and notification to APRA if necessary.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.