FORTRA™

SOLUTION BRIEF (DATA CLASSIFICATION)

FINMA Compliance Support That Works For Your Business

Fortra's Data Classification Suite (DCS) helps protect your organisation's as well as your clients' valuable information and supports your compliance with the Swiss Financial Market Supervisory Authority FINMA Principles of Confidentiality for Client Identifying Data (CID).

To support your compliance with FINMA principles of data classification, DCS helps ensure that commercially sensitive data and CID is protected throughout the organisation and wider ecosystem.

Since FINMA principles are based on international standards, compliance not only helps you in Switzerland, but it also helps your organisation meet its data protection obligations in other territories where you want to grow.

> "We see ROI through prevention. We've calculated that a breach would cost $350 per record. DCS is the vehicle we use to get effective enforcement by providing identity to the data."
>
> **— Fortune 500 customer.**

Protecting Your information In Compliance With FINMA Principles

Before you can protect your data, you've got to discover what types of information you actually have and accurately classify the value of it. Only then can you truly protect your data.

DCS uses an open, configurable policy engine that enables your organisation to enforce detailed data identification and handling policies with award-winning machine learning, enabling you to monitor compliance and continuously reinforce a culture of security.

Discover

Sensitive information must be identified wherever it sits and however it is created. DCS solutions enforce identification of all information across your organisation to ensure protection becomes part of your users' natural workflow.

Classify

The powerful DCS policy engine ensures that information is classified correctly according to your information security policy. Multiple layers of classification allow for very granular control. Machine learning technology can be deployed to assess the information, recognise sensitive data and determine appropriate categories.

Protect

DCS integrates with your existing security systems such as messaging encryption, data loss protection (DLP) and electronic data rights management (EDRM) technologies to enforce your information security policies using open metadata embedded in documents at their creation.

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

DCS supports compliance with the following principles of risk management for handling electronic client data within FINMA Circular 2008/21 Operational Risks – Banks, Annexe 3.

Principle 1: Governance

Security management requires compliance monitoring and reporting. DCS can log and measure users' data classification compliance levels as needed.

Principle 2: Client Identifying Data

DCS uses an advanced policy engine with highly granular levels of control. A document can be classified as confidential, CID, internal-only or retail division–only. Appropriate protections, such as encryption, DLP, etc., are then enabled accordingly.

Fortra's DCS Intelligent Protection is an optional system that suggests or enforces classification. It can be trained to recognise sensitive intellectual property and data classed as personal within Switzerland.

Data maintains its categorisation throughout its entire life cycle from creation and storage to destruction.

Principle 3: Data Storage Location And Access To Data

After data classification, DCS ensures correct data handling by directing other systems (such as messaging) to apply the necessary restrictions. For example, data that should not leave Switzerland can be given that explicit classification.

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

You can also control the information shared with third parties, such as partners, customers, interest groups, outsourcers, teleworkers, the public and the supply chain.

Principle 4: Security Standard For Infrastructure And Technology

DCS works with your other security systems to prevent CID from escaping. DLP, EDRM and encryption, therefore, all operate more effectively. As new security systems are introduced and upgraded, they fit easily into existing classification policies as DCS adds open metadata to files and X-headers to emails, which other systems can recognise and act upon.

In addition, DCS can discover CID on endpoints, mobile devices and in the cloud and either categorise it

automatically or support users in categorising it manually. Mobile devices and the cloud are essential business tools but come with a higher risk of data leakage. DCS can restrict sensitive information from being shared via mobile and cloud technologies if your organisation requires that.

Principle 5: Selection, Monitoring And Training Of Employees

Security is a continuous process. By using DCS in their everyday work, users are made aware of security policies and reminded to protect valuable information. DCS suggests classifications by understanding the content, thereby continuously training users to recognise its value.

DCS digitally labels CID with open metadata and physically labels it on printed copies (with optional headers, footers and watermarks). This mechanism helps users understand the value of data when sharing it. They will also know to follow retention, clear screen/desk policies and disposal/ reuse of equipment policies.

Principle 8: Incidents Related To The Confidentiality Of CID

Audit logs aid the investigation of noncompliance when CID or other sensitive information has been released inappropriately. Audit logging can be switched on and configured to record the level of user classification activity. Logging can also flag incorrect user data access controls.

Principle 9: Outsourcing Services And Large Orders

Outsourcing partners can maintain the same levels of protection as internal systems. DCS's open metadata classification means their systems recognise and react to the classifications assigned. Large volumes of data can be similarly protected by other third parties.

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.