FORTRA™

SOLUTION BRIEF (DATA CLASSIFICATION)

SIA IAS Compliance Support That Works For Your Business

Data Classification Suite (DCS) helps you protect your organisation's valuable information and supports your compliance with the Information Assurance Standards (IAS) outlined by the UAE Signals Intelligence Agency (SIA) — formerly the National Electronic Security Authority (NESA).

DCS defines and supports your policy across 54 key IAS controls and subcontrols, ensuring that sensitive and personal data is protected throughout your organisation and wider ecosystem. Since the UAE controls are based on international standards, compliance helps your organisation meet its data protection obligations in other jurisdictions as well.

> "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.**

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 enforces your policies across all your security systems, including messaging, data loss prevention (DLP) and electronic data rights management (EDRM), using open metadata embedded in documents at their creation.

Leaders can give their staff more freedom to innovate while knowing that sensitive information will be kept safe.

Protecting Your Information In Compliance With SIA IAS

Protection starts with discovering the information you actually have and accurately classifying the value of it. Only then can information be protected.

Classification With Machine Learning (T1.3.1)

Classification is key to ensuring that sensitive data is handled correctly. DCS uses an advanced policy engine to allow highly granular levels of control.

Fortra's DCS Intelligent Protection is an optional system that will suggest or enforce a particular classification. The system can be trained to recognise IP that is sensitive to your organisation and data classed as personal within the UAE.

External Communications (M1.4.2)

Control the information you share with IAS-defined third parties, such as partners, customers, interest groups, outsourcers, teleworkers, the public and the supply chain. DCS open metadata ensures protection of information shared via email and messaging on desktop computers, laptops or mobile devices.

Awareness And Training (M3.3.3, M3.4.1)

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

Labelling Sensitive Information (T1.3.2)

Sensitive information is labelled digitally with embedded open metadata and physically on printed copies (with headers, footers and watermarks). Users are always reminded of the value of information when sharing it. They will also know when to follow retention, clear-screen and clear-desk policies (T2.3.9), as well as disposal and reuse of equipment policies (T2.3.6).

Mobile devices and the cloud (T1.2.3, T6.3.1)

Mobile devices and the cloud are important business tools but come with higher risk of data leakage. DCS can restrict the most sensitive information from being shared in this way. DCS can also scan cloud accounts to discover information that should be classified.

Reporting And Compliance (M4.3.1)

Management of security in the entity requires monitoring of compliance and reporting to management and SIA if required. DCS can log users' data classification compliance levels as needed to measure the effectiveness of training.

Cryptography, Data Leakage And Rights Management (T7.4.1, T7.6.4, T4.3.1)

DCS works with your other systems to prevent personal data and confidential intellectual property from leaving your organisation unprotected. DLP, EDRM and encryption systems will operate with higher accuracy to secure correctly classified information.

Data Handling (T1.3.3)

Mobile devices and the cloud are important business tools but come with higher risk of data leakage. DCS can restrict the most sensitive information from being shared in this way. DCS can also scan cloud accounts to discover information that should be classified.

User Access Control (T5.2.1)

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

Business Continuity (T3.5.1, T9.2.1)

Backup and restore and other disaster recovery systems must process sensitive data appropriately. DCS labelling enables these systems to work effectively to restrict sensitive data to the right users and locations.

Information Assurance Standards Controls List

DCS solutions apply to the IAS Management and Technical Controls below.
AA=Always Applies (mandatory in all entities)

M1 Strategy & Planning

M1.1.3 AA Roles & Responsibilities

M1.2.1 AA Infosec Policy

M1.2.2 AA Supporting Policies

M1.3.2 Confidentiality Agreements

M1.3.4 Special Interest Groups

M1.3.5 Risks: External Parties

M1.3.6 Customers

M1.4.2 AA Internal and External Communications

M1.4.3 AA Documentation

M2 Risk Management

M2.2.1 AA Risk Identification

M3 Awareness & Training

M3.3.2 AA Implementation Plan

M3.3.3 AA Training Execution

M3.4.1 Awareness Campaign

M4 Human Resources Security

M4.3.1 AA Management Responsibilities

M4.4.3 AA Removal of Access Rights

M5 Compliance

M5.2.2 IP Rights

M5.2.3 Protection of Organisational Records

M5.2.4 Protection of Personal Information

M5.3.1 Standards Compliance

M5.4.1 Technical Compliance Checking

M5.5.1 Audit Controls

M6 Performance Evaluation & Improvement

M6.3.1 AA Corrective Action

M6.3.2 AA Continual Improvement

T1 Asset Management

T1.2.3 Acceptable Use of Assets

T1.3.1 Classification of Information

T1.3.2 Labelling of Information

T1.3.3 Handling of Assets

T2 Physical and Environmental Security

T2.3.6 Disposal/Reuse of Equipment

T2.3.7 Removal of Property

T2.3.9 Clear Desk/Clear Screen Policy

T3 Operations Management

T3.5.1 Information Backup

T3.6.2 Audit Logging

T4 Communications

T4.2.1 Information Transfer Procedures

T4.2.4 Electronic Messaging

T4.2.5 Business Information Systems

T4.3.1 eCommerce

T4.3.3 Publicly Accessible Information

T4.4.2 Information Sharing Communities

T5 Access Control

T5.2.1 User Registration

T5.2.4 Review of User Access Rights

T5.6.1 Information Access Restriction

T5.6.3 Publicly Accessible Content

T5.7.1 Access Control for Mobile Devices

T5.7.2 Teleworking

T6 Third-Party Security

T6.2.1 Service Delivery

T6.3.1 Cloud Environments

T6.3.2 Cloud Provider Agreements

T7 Information Systems Acquisition, Development & Maintenance

T7.2.1 Requirements Analysis and Specification

T7.4.1 Cryptographic Controls

T7.6.4 Information Leakage

T7.6.5 Outsourced Software Development

T7.8.1 Supply Chain Protection

T7.8.3 Limitation of Harm

T9 Information Systems Continuity Management

T9.2.1 Business Continuity

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.