FORTRA

FACT SHEET (Boldon James)

British Standards Institute BS10010:2017

Information Classification, Marking and Handling

BS10010:2017 is a specification for information classification, marking and handling (ICMH) schemes. This guidance is useful for organisations that worry about the sensitivity of the information assets they create, use and share. BS10010:2017 intends to encourage organisations of any size to use a managed, and more consistent, approach to handling information assets on the basis of their classification and marking.

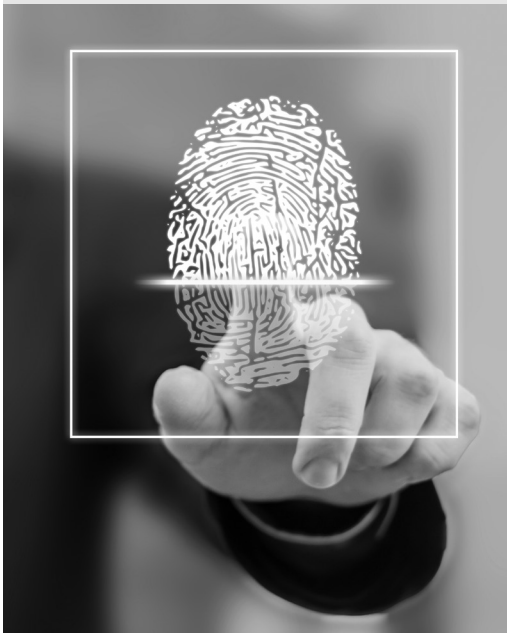
This standard gives you a better understanding of how data classification can help your organisation, as well as the fundamentals of creating a scheme. Data classification can deliver a significant improvement to the way sensitive information is managed, both within the user's own organisation, as well as any external organisation you share information with. It can also contribute to the protection of the organisation's investments, income, reputation and future.

The new standard has been introduced at a time where global data security regulations are being tightened, and completely new regulations are being established such as the European General Data Protection Regulation (GDPR) and a recently approved privacy amendment to the Australian Privacy Act. Data classification is a good place to start in protecting your data in order to begin compliance with these kinds of regulations.

So if your organisation is looking to implement, or even talk internally about establishing a data classification scheme, this standard is a great place to start. BS10010:2017 will guide you through the setup, running and review of a data classification scheme, giving you a framework to help kick start a project rather than having to initiate something from scratch.

This Standard Is Intended To Support Organisations To:

- Meet strategic objectives and risk management goals
- Meet legal, regulatory and standard compliance obligations
- Learn how to secure, protect and share sensitive information appropriately
- Improve user understanding of the value of organisational data, and how to handle it



Secure Your Sensitive Data

The first step in using a data classification approach to ensuring compliance is to understand all of the personal or sensitive data you hold, and the potential risks to its security. You will need to ask:

- What data do you hold?
- What data is being collected, and where from?
- Where is it being stored and processed?
- Why you have it?
- How sensitive it is?
- How it is accessed, used or shared - including externally?

The data should then be classified or tagged according to its sensitivity. Once you have singled out the most confidential information you can determine what higher grade controls should be applied to ensure it is adequately protected.

Don't Delay Your Preparations

The sheer volume of unstructured data within organisations, combined with the ever increasing technical abilities of hackers are finding to breach perimeters, make it impossible to rely on people and processes alone to ensure that sensitive personal data is handled appropriately.

Data classification embeds a culture of compliance by involving users in identifying, managing and controlling regulated data, while automating parts of the protection process to enforce rules and policies consistently.

As you look at your organisations data protection policy, classifying data as a first step will enable the protection strategy and solutions you implement to be built around the types of data you have, and the levels of security they require.

How Can Boldon James Help?

Boldon James Classifier, the market leading data classification product, supports the creation and aplication of a data classification scheme by:

- Ensuring appropriate control of confidential or sensitive information
- Enforcing a classification and security policy consistently across the organisation
- Classifying or labelling data with visual (and metadata) labels to highlight any special handling requirements
- Alerting users when personal data is leaving the organisation to warn or prevent them from sending messages that contain sensitive information
- Educating users about the sensitivity of data whilst ensuring adherence to corporate policy
- Providing critical audit information on classification events to enable remediation activity and demonstrate compliance position to regulatory authorities
- Utilising metadata labels to drive additional security controls and solutions, such as DLP, encryption and rights management

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.