FORTRA

GUIDE (Boldon James)

Meeting The UK Government Security Classifications (GSC) Regulations

Including

- The GSC scheme
- Why the change?
- Meeting GSC requirements
- Benefits of data classification
- Boldon James Classifier solutions for GSC

Introduction

With email now the de-facto method of sharing information, government organisations must balance the need to share with the need to protect highly sensitive information from leakage or loss. In an effort to address a problem which is never far from the headlines, the UK Government has revised the requirements in its Government Security Classification (GSC) scheme to ensure information security, privacy and accountability. This paper provides an overview of the GSC classification requirements and provides an approach to meeting them, in order to adhere to the scheme and prevent data loss incidents from occurring.

Regulatory Requirements

For the UK Government, data protection is governed by a number of legal and regulatory documents. For example, HMG Departments and Agencies must adhere to legal requirements stemming from the Official Secrets Acts, the Data Protection Act and the Freedom of Information Act. The Cabinet Office Security Policy Division is responsible for the Security Policy Framework (SPF), which describes the mandatory minimum requirements for the same community of organisations.

The Government Security Classification (GSC) Scheme

All UK Government & public sector organisations must comply with Her Majesty's Government Security Policy Framework, which requires the application of security classifications to government information assets. Protective marks are composed of classifications and descriptors, but may also include caveats and code words. These mark indicate handling requirements to the people reading the content, helping to provide the security measures the information demands.

The UK Government Protective Marking Scheme (GPMS) comprises three classifications (or markings) which, in descending order of sensitivity, are TOP SECRET, SECRET and OFFICIAL. TOP SECRET and SECRET are rarely used outside of defence or intelligence environments. OFFICIAL refers to the minimum level of classification that any document, file or message should inherit, and replaces the previous levels of CONFIDENTIAL, RESTRICTED and UNCLASSIFIED or NOT PROTECTIVELY MARKED. In practice, this means that all data will have a level of sensitivity – whereas under the previous GPMS scheme information may have been left unmarked in some instances. The criteria below provide an indication of the type of material at each level of classification – detailed requirements are contained in supplementary material within the SPF. Each level provides for a baseline set of personnel, physical and information security controls, as described in the SPF which all UK departments, agencies and authorised UK contractors must follow.

- **TOP SECRET:** The compromise of this information may lead directly to widespread loss of life, threaten the internal stability or security operations of the UK (or its allies), damage relations with friendly governments or cause severe damage to the UK economy
- **SECRET:** The compromise of this information may be lifethreatening, disruptive to public order, security operations, economic & commercial interests or seriously detrimental to diplomatic relations with friendly nations
- **OFFICIAL:** This category is for the majority of information created or processed by government and includes both routine business and some sensitive information. The typical threat profile for the OFFICIAL classification is broadly similar to that face by a large UK private company with valuable information and services

The Need For Consistent And Accurate Classifications

The Cabinet Office's SPF has a number of mandatory requirements for Central Government Departments and Agencies. In addition, the Cabinet Office "Government Security Classifications April 2014" document indicates how sensitive information should be marked and managed:

"There is no requirement to explicitly mark routine OFFICIAL information. Baseline security measures should be enforced through local business processes. A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the need to know. In such cases where there is a clear and justifiable requirement to reinforce the need to know, assets should be conspicuously marked: „OFFICIAL–SENSITIVE".

How To Meet GSC Requirements

Typically there are three approaches which can be taken to meet the requirements of GSC as outlined above;

- **Manual:** Users are required to type the correct GSC classification on emails and documents – typically in the subject line and at the top and bottom of emails. This approach would be driven by policy and would require significant training & monitoring to ensure policy was correctly enforced. Ordinarily there would be a heavy requirement to continually check that users are classifying everything they produce and undoubtedly, there will be a lack of consistency in how classifications are applied
- **Templates:** Some organisations choose to produce document templates for users to select from, with the GSC data classifications already present in the templates, to remove individual variations. While this approach may deliver a marginally greater consistency than the manual approach, it can prove very inflexible – for example, a user may create a document expecting the content to be of one classification and later to find their completed document should be of a higher or lower sensitivity. Generally the best time to make a classification decision is once the email or document is complete
- **Software Tool:** The approach favoured by many organisations is to implement a simple software solution which can help users enforce the GSC classification scheme in a consistent and easy-to-use manner. A good labelling solution should ensure pre-defined GSC labels are applied in a consistent manner without impacting user productivity. A solution can also enable valuable metadata labels to be added to the content which can later be used by other systems, such as encryption or access control, without any further input required by the user

Beyond GSC – The Benefits of Data Classification

In addition to mandated requirements, data classification can provide additional business and security value to any organisation where it is employed.

User Awareness & Education

When organisations apply a consistent approach to labelling content, awareness of security practices and policies is increased. When labels are applied at the desktop, where most content is generated, users are mindful of their security responsibilities. In our experience, organisations that have implemented data classification solutions have seen a 60% increase in security awareness.

Driving IT Security and Information Management Solutions

Numerous internal policies can be supported by data classification: archive and storage plans, access control, log and audit procedures. For many IT solutions that provide information in a structured way (e.g. databases), information management problems are handled by the solutions themselves. However, unstructured information (e.g. email messages and Office documents) is very difficult to manage. By their very nature, email messages are stored in multiple locations with little or no indication as to the value any particular message may have to the organisation. Documents can be even harder to manage as users copy versions to local hard drives, network shares, and even removable media.

IT departments can reduce the difficulty this unstructured information presents by applying protective marks to this material. Protective marks provide an indication of the value of a document or message. Not only do people who are reading the content understand the content's sensitivity (and hence the required duty of care), but so can IT systems.

By adding metadata labels to email and Office documents, data classification can increase the effectiveness and performance of existing technologies, such as DLP, Rights Management, encryption and archiving solutions. Most standard IT security and information management solutions can be easily configured to read metadata and apply tailored policies based on the labels. Examples include:

- **Encryption:** encrypt messages marked OFFICIALSENSITIVE that are destined for external networks
- **DLP Tools:** ensure recipients of email messages are cleared to read content that is protectively-marked before the message is delivered
- **Collaboration Tools (e.g. SharePoint):** define access control policies for document repositories based on classifications
- **Archiving Solutions:** automated archive policy selection based on classification
- **eDiscovery (Search & Retrieval):** improve enterprise search tools by including the classification as a search term

Boldon James Classifier Solutions for GSC

With over 30 years experience in the data classification and secure messaging industry, Boldon James provides organisations with simple extensions to their existing IT application infrastructure that help them meet the UK Government requirements for handling sensitive documents, files and email messages. The Boldon James Classifier product suite is made up of the following core products:

Email And Message Classification:

- **Email Classifier: Classification for Microsoft Outlook and Lotus Notes**
  Provides users with the ability to apply relevant visual labels to email messages and embed those labels into the email metadata. These labels enforce your rules on the handling and release of email, automatically invoking other technologies such as encryption or rights management
- **OWA Classifier: Classification for Microsoft Outlook Web App (OWA)**
  Provides a natural complement to Email Classifier by extending labelling to web-based email users of Microsoft Exchange and supporting the widest range of OWA interfaces to maximise user choice and browser compatibility
- **Mobile Filter: Selective mobile synchronisation for Microsoft Exchange**
  Provides control over which messages can be synchronised to a mobile device from Microsoft Exchange Server - preventing exposure of sensitive data on mobile devices

Document And File Classification:

- **Office Classifier: Classification for Microsoft Word, Excel, PowerPoint, Visio and Project documents**
  Provides a simple means for users of key productivity applications to apply relevant visual labels to documents, which are expanded into the document metadata. These labels enforce your rules on handling and release of documents, automatically invoking other technologies such as rights management
- **File Classifier: Classification for all files in Windows File Store**
  Provides the natural complement to Boldon James Office Classifier by extending the range of information that may be labelled by a user to include any type of file that may be held in Windows File Store
- **SharePoint Classifier: Classification for Microsoft SharePoint documents and files**
  Provides users with the ability to apply relevant labels to any file held in the document libraries of Microsoft SharePoint, with automatic recognition of the labels applied to emails, documents and files by other Classifier products
- **Power Classifier: For bulk classification of files and automation of labelling processes**
  Provides the means to classify and label large sets of static information, as well as applying classification dynamically at the point of capture. The Power Classifier tools can be operated by key knowledge workers, invoked as part of automated tasks or controlled directly by other applications, such as Data Governance tools
- **CAD Classifier: Protect Design Documents and CAD Applications**
  CAD Classifier brings the benefits of data classification to key design documents and CAD applications. Users of Autodesk® AutoCAD® can apply relevant visual and metadata labels to CAD documents and receive guidance on labelling policy, all via the user interface common to all Classifier products

Benefits Of Using Boldon James Classifier

Putting Boldon James Classifier at the heart of your organisation allows you to reduce the business risk of valued and sensitive data ending up in the wrong hands, whilst increasing efficiency, enhancing decision making and reducing archiving and other administrative costs throughout the organisation. Classifier helps organisations proactively manage and protect sensitive information, ensuring it goes to the right people in a safe, controlled and efficient way.

With a centralised administration platform, it is simple to set up and deploy classification policies across an organisation. The customisable policy module can require all users to choose a specific classification label for every email message, document and file that they create. Policy options allow an organisation to choose how visual marks are displayed and enforce rules such as preventing downgrading of the classification of content. Integration with Microsoft's Active Directory allows per user clearance levels for email messages. Additional policies can be created to restrict messages to specific email domains by classification level.

Classifier deployed to the desktop ensures that organisational policy is enforced for each user. Email messages are classified at the desktop by the user and clearance checks are performed before the message is sent. This provides instant feedback to the user regarding messaging policy. The centralised policy dictates whether documents must be classified before they are saved or printed. The plug-in also can enforce a security high-water mark for email messages that have attachments. This policy ensures that email messages are classified at a sensitivity that is at least as high as the sensitivities of any attachments.

With enforcement at the desktop, Classifier can increase user awareness of an organisation's classification policy. Through daily use of data classifications, users are required to take action regarding the sensitivity of content that they create. Classifier can also log each user action and policy decision to the local Windows Event Log, providing an audit trail for user actions.

In addition to the traditional classifications that are applied (e.g. email subject line, headers and footers), Classifier adds equivalent metadata to messages and documents. Using standard locations to store metadata allows thirdparty, downstream infrastructure tools to take advantage of the data classifications. This additional information allows policy decisions to be more accurate and effective. An organisation's IT services branch can increase the ROI of many solutions that are already in place by tuning configurations to read the data classifications applied by users to email messages and documents.

To Summarise, Classifier Can Benefit Organisations By:

- Helping public sector organisations comply with GSC and other regulations
- Increasing user and organisational awareness of the value & sensitivity of data
- Consistent application of policy across organisations
- Educating users on, and support adherence to, corporate governance & data security policies
- Streamlining business processes – increasing operational efficiency & effectiveness
- Completely scalable and easy to deploy solution
- Reducing cost of management, archiving & storage of data
- Helping prevent internal and external data leakage – reducing reputational & business risk

Global brands trust us to protect their sensitive data:

More Information

For more information about how you can implement a data classification solution as part of your data protection strategy, please contact us

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.