boldonjames
A QinetiQ Company

Protective Marking for UK Government

WHITE PAPER

Contents

Introduction

Whilst email is the de-facto method of exchanging 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 stipulated a range of measures that must be taken to ensure information security, privacy and accountability. This paper provides an overview of the UK government protective marking requirements and outlines a proven approach to meeting them to help secure email communications.

Regulatory Requirements

For the UK Government, information 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. Additional policy requirements come from other government programmes, such as Government Connect Code of Connection for GCSx (CoCo).

Government Protective Marking System (GPMS)

One of the requirements set out by these documents is the application of the Government Protective Marking System (GPMS) to documents and email messages. Protective marks are composed of classifications and descriptors, but may also include caveats and code words. These marks are useful to people reading the content by indicating handling requirements for the document, helping to provide the security measures the documents demand.

The Protective Marking System comprises five markings which, in descending order of sensitivity, are TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED and PROTECT. TOP SECRET and SECRET are rarely used outside of defence or intelligence environments. Unmarked material is considered unclassified. The term ‘UNCLASSIFIED’ or ‘NON’ or ‘NOT PROTECTIVELY MARKED’ may be used to indicate positively that a protective marking is not needed.

The criteria below provide a very rough indication of the type of material at each level of protective marking – detailed requirements are contained in supplementary material within the SPF.

- ***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 life-threatening, disruptive to public order, security operations, economic & commercial interests or seriously detrimental to diplomatic relations with friendly nations
- ***CONFIDENTIAL :*** The compromise of this information may impact personal liberties, cause material damage to diplomatic relations or seriously disrupt the economy, major criminal investigations, organisations, government policies or national operations
- ***RESTRICTED :*** The compromise of this information may cause significant distress to individuals, limit the effectiveness of military or security operations, compromise law enforcement or undermine the management or running of government organisations
- ***PROTECT :*** The compromise of this information may breach rules on the disclosure & handling of information by third parties, give unfair advantage for individuals or companies or disadvantage government in commercial or policy negotiations with others

The Cabinet Office's SPF has a number of Mandatory Requirements for Central Government Departments and Agencies. One of these requirements states that all departments must apply the Protective Marking System [i]. These organisations' internal business processes and security practices rely on protective marks to ensure the proper handling of sensitive information. When doing business with the central government, local authorities will often be asked (if not required) to apply GPMS to information that is exchanged. As an example, CoCo version 4.1 requires "labelling emails with protective marks" [ii].

Although the SPF does not specify the exact method of applying protective marks, CoCo's Guidance Notes states "protective marking should appear in full in the subject line or first line of the body text". For documents, the accepted standard is to apply the protective mark either as a watermark, in the header, in the footer or both of each page.

In addition to requiring protective marks on documents and messages, CoCo's Guidance Notes [iii] provides a list of Personal Commitment Statements for end users. These statements are designed to inform users of their responsibilities when using a Government Connect Intranet (GSi) network. In particular, there are a number of these statements that cover the dissemination of protectively-marked information. That is, ensuring that access is granted to those individuals that are cleared to receive the information. For example, users are expected to ensure that recipient email addresses are correct to avoid releasing protectively-marked material to the public. The Guidance Notes also list encrypting RESTRICTED information that is passed across public networks. The GCSx Operational Support Guide lists requirements for processing material marked PROTECT and RESTRICTED, including protecting the material "against illicit internal use or intrusion by external parties." [iv] One of the mechanisms listed to help support this protection is to log each use by an individual.

The Value Beyond Regulatory Requirement - Other Benefits of Protective Marking

In addition to mandated requirements, protective marking can provide additional value to an organisation's IT infrastructure.

Leveraging Other Technologies

By adding well-defined labels to email and office documents, protective marking can increase the effectiveness of existing technologies. Most standard IT solutions can be configured to read labels on content and apply tailored policies based on the labels.

User Awareness & Education

Labels and labelling software can help to reinforce an organisation's business processes carried out by end users. 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.

Information Management

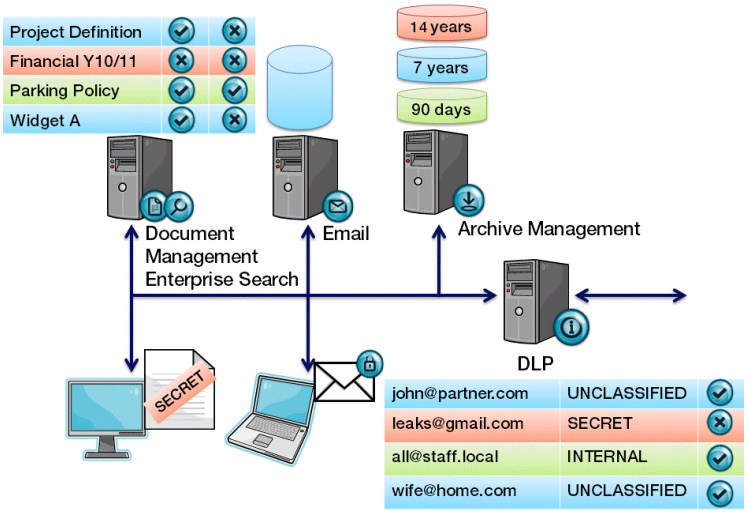
There are numerous internal policies in play: archive and storage plans, access control, log and audit procedures. For many IT solutions that provide information in a structured way (e.g. databases), information management problems are handled by the solutions themselves. However, unstructured information (e.g. email messages and office documents) is 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 poses by taking advantage of protective marks on this material. Protective marks provide an indication of the business 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.

When protective marks are added in a consistent and standard manner to documents and email messages, additional security measures can be applied by IT solutions for example:

- encrypt messages marked RESTRICTED that are destined for external networks
- ensure recipients of email messages are cleared to read content that is protectively-marked before the message is delivered
- define access control policies for document repositories based on protective marks
- automated archive policy selection for each protective mark
- improve enterprise search tools by including the classification as a search term

Figure 1: Protective Marking's role in information management in an IT infrastructure



Common Approaches to Meeting Protective Marking Requirements

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

- ***Manual:*** Users are required to type the correct marking on emails and documents – typically in the into subject line and at the top and bottom of emails. This approach would be driven by policy and would require significant training & monitoring. In some cases there will be a heavy requirement to continually check that users are marking everything they produce and undoubtedly, there will be a lack of consistency in the way that markings are applied.
- ***Templates:*** Some organisations choose to produce document templates for users to select from, with the protective markings 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.
- ***Tool:*** The approach favoured by many organisations is to implement a software tool which helps users enforce classification policy in a consistent manner. A good labelling solution should ensure labels are applied in a consistent manner but provide the flexibility to ensure users remain productive and should also add metadata to the content which can later be read by other systems without any further interaction on the part of the user.

Boldon James Solutions for Protective Marking

Boldon James provides organisations with simple additions to their IT infrastructure that help meet UK Government requirements for handling protectively marked documents and email messages. The Boldon James Information Classification Suite (Classifier/ICS) is made up of two products:

Boldon James Email Classifier - Protective Marking & Release Control for Email

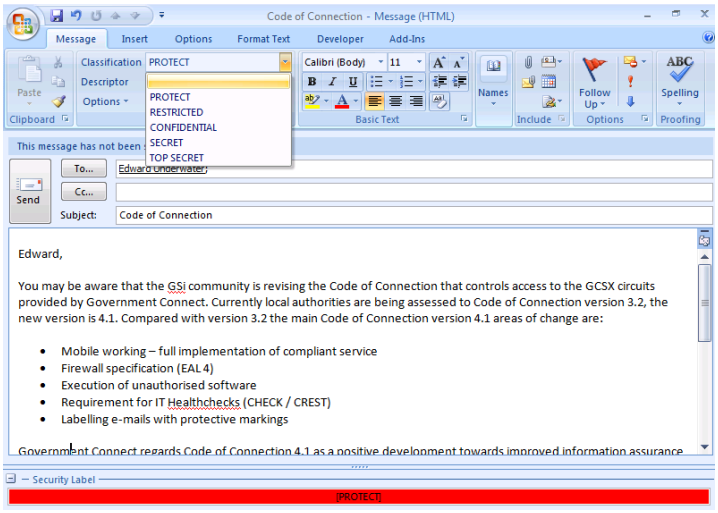
Boldon James Email Classifier is an easy-to-deploy plug-in to Microsoft Outlook which makes it simple for a user to classify emails and provide additional visual indicators that will highlight protective markings to recipients of protected mail, encouraging better recognition and awareness.

Boldon James Office Classifier - Security Labelling for Microsoft Office

Boldon James Office Classifier enables users to add protective marks to Office documents, spreadsheets and presentations. Office Classifier stores the mark or label inside machine-readable document properties, as well as in a user-readable text format.

When combined with Office Classifier, Email Classifier can also check that the document and email classifications match and either warn the user if the document is a higher classification or force them to upgrade the classification of the email - potentially triggering one of the administrator-set rules regarding where this information can be sent.

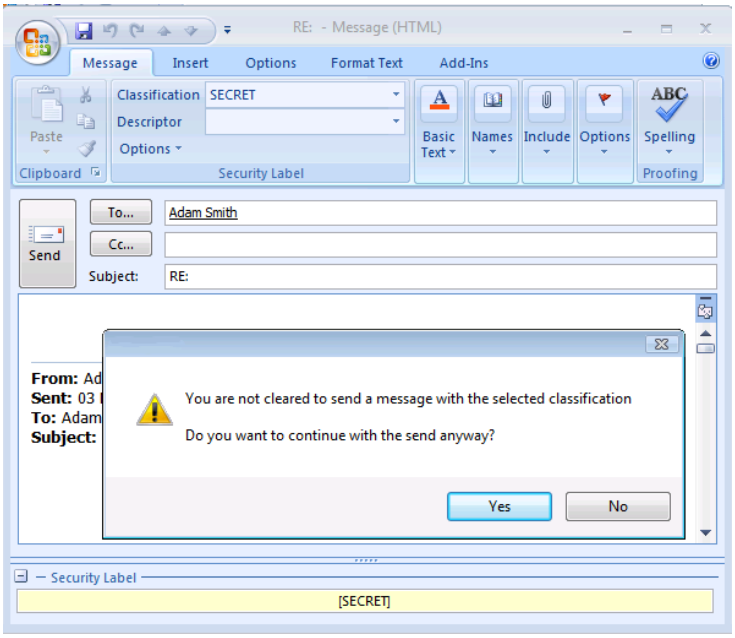
Figure 2: An Email Classifier email with protective marking



With a centralised configuration model, Classifier/ICS can deploy an organisation's marking policy across the user community. The customisable policy module can require all users to choose a protective mark for every email message and Office document that they create. Policy options allow an organisation to choose the visual display of protective marks 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.

Classifier/ICS deployed to desktop ensures that organisational policy is enforced for each user. Email messages are protectively-marked 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 marked before they are saved or printed. The plug-in also can enforce a security high-watermark for email messages that have attachments. This policy ensures that email messages are classified at a protective mark that is at least as high as the protective marks of any attachments.

Figure 3: The Email Classifier policy violation notification dialogue box



With enforcement at the desktop, Classifier/ICS can increase user awareness of an organisation's protective marking policy. Through daily use of protective marking, users are required to take action regarding the sensitivity of content that they create. Classifier/ICS 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 protective marks that are applied (e.g. email subject line, headers and footers), Classifier/ICS adds equivalent metadata to messages and documents. Using standard locations to store metadata allows third-party, downstream infrastructure tools to take advantage of the protective marks. 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 protective marks applied by users to email messages and documents.

References

i HMG Security Policy Framework, v1.0 December 2008, Mandatory Requirement 11, page 17
ii GC Communicate, Issue 11, 3 September 2009, page 2
iii GSi Code of Connection for GCSX v4.1
iv GCSx Operational Support Guide v1.0, 13 February 2008, page 24-27

About Boldon James

For over 20 years we have helped organisations with the most demanding and complex communication requirements manage sensitive information securely and in compliance with legislation and standards.

Our solutions extend the capabilities of Microsoft core infrastructure products to allow secure information exchange and in 2006 we were elevated to Microsoft Global Go-To-Market Partner. Boldon James is a wholly-owned subsidiary of QinetiQ, with offices in the UK, US, Australia and Europe, and channel partners worldwide.