janusNET
security starts with you

Complying with the Protective Marking requirements of UK Government

for Departments, Agencies, Policies Forces and Local Authorities

The use of security classification labels (protective markings) as an effective means to maintain data confidentiality and prevent data leakage is well established in national government circles, especially when dealing with hardcopy material.

These same principles can also be applied to electronic information using the janusSEAL suite of applications from janusNET. The janusSEAL suite is a range of add-ons for Microsoft Office products. The janusSEAL add-ons require end-users to assign security classifications to all the e-mail messages they send and files they create. These security classifications help other users and Information Technology (IT) systems know how valuable or sensitive the information is within the item and hence the appropriate level of protection they should be given.

This briefing paper:

- summarises current protective marking requirements applicable to the United Kingdom (UK) government sector
- demonstrates how the janusSEAL suite can be used to comply with those requirements

1 What are Protective Markings and why are they useful?

A Protective Marking, as the name implies, is a marking on a document or piece of information which identifies the confidentiality requirements of the information. It also conveys those protective requirements to all those who handle it. Protective markings are also known as security classification labels.

Most people would recognise them from movies - a memo with TOP SECRET emblazoned across the top and bottom has been *protectively marked* - the recipient of the memo (and the watching audience) immediately know that the information is highly sensitive and must be protected appropriately.

It is this ease with which other people and (in the electronic information space) other IT systems can interpret and understand the protective marking that shows their benefit. Without needing to be subject matter experts in the item being discussed they are immediately aware of at least how sensitive or valuable the information is under discussion and hence how well they protect that information. The marking in and of itself, however, does not provide any protection.

2 UK Government mandates use of Protective Markings on information assets

Government in the United Kingdom has a long history of using security classifications and protective markings to protect its data. Many of the terms it uses for its security classifications are also used by countries in the Commonwealth.

At the current time the use of protective markings in the UK government is defined in Her Majesty's Government Security Policy Framework (SPF)[1] in particular SP2 - Security of Information[2].

These policies mandate that UK's Government Departments and Agencies:

- Must apply the Protective Marking system... (MR 6)
- Assets must be clearly and conspicuously marked... (MR 7)
- Only the originator or designated owner can protectively mark an asset... (MR 7)

Further, the Government Protective Marking System (GPMS) is defined in the Framework as comprising the five security classifications, in ascending order of sensitivity

- PROTECT
- RESTRICTED
- CONFIDENTIAL
- SECRET
- TOP SECRET

The classification UNCLASSIFIED or NOT PROTECTIVELY MARKED is used for government information to assert that a protective marking is not needed because the information is *not* sensitive.

For the purposes of confidentiality, these classifications can also be mapped to Business Impact Levels (BILs) discussed in SP2.

2.1 Police Forces must use the GPMS

Police forces in the UK must also use the Government Protective Marking Scheme for information assets, as highlighted in the following policy sources.

2.1.1 First adopted the GPMS in 2001

The Association of Chief Police Officers/Association of Chief Police Officers (Scotland) (ACPO/ACPOS) adopted the Government Protective Marking Scheme in 2001.

2.1.2 ACPO/ACPOS Information Systems Community Security Policy

The ACPO/ACPOS Information Systems Community Security Policy (CSP) governs the police community's approach to information assurance. The chief constables and commissioners agreed to adopt and implement the latest version (from 2006) within their forces by March 2010.

The CSP refers to the HMG Security Policy Framework as a standard upon which it is based and hence it forms a benchmark requirement for compliance. On this basis police forces must use the GPMS for appropriate information assets.

[1] https://www.gov.uk/government/publications/security-policy-framework

[2] https://www.gov.uk/government/uploads/system/ uploads/attachment_data/file/200552/HMG_Securi ty_Policy_Framework_v10_0_Apr-2013.pdf

2.1.3 Management of Police Information

An outcome of the Bichard inquiry, the Management of Police Information (MoPI)[3] is a statutory code of practice for the Police Service that requires police forces to improve information management and sharing. Parts of it cover the use of protective markings:

- "Before recording police information consideration must first be given to any sensitivities in recording it to ensure that it is given the appropriate Government Protective Marking Scheme (GPMS) marking." - 4.2 Principles of Recording
- "Information that is to be retained must be managed in accordance with the ACPO/ACPOS (2002) Information Systems Community Security Policy".

2.2 Local Authorities connecting to the PSN must place protective markings on e-mail messages

The PSN (Public Services Network) provides a secure government network between central government and Local Authorities (LAs) in England and Wales. The PSN takes on the role of the Government Connect Secure Extranet (GCSX) and provides connectivity at the IL2 level to the majority of central departments and many other public sector organisations and some commercial organisations. Prior to 1st February 2013 it was IL3(RESTRICTED) but was changed to accommodate migration to the PSN.

The Code of Connection (CoCo) is a list of security requirements with which all LAs must comply before they can connect to the PSN. Since September 2009 the version of CoCo that LAs had to comply with was 3.2 but from March 2010 it's version 4.1.

Historical CoCo security requirements which pertain to protective markings include:

- **CoCo v3.2 R 2.2.2** "Employees of the organisation who handle information carrying a protective marking of RESTRICTED MUST be made of aware of the impact of loss of such material and the actions to take in the event of any loss."

- **CoCo v3.2 R2.13.1** "Audit logs recording user activities, exceptions and information security events MUST be produced to assist in future investigations and access control monitoring."

- **CoCo v3.2 R2.24.7** "E-mail MUST not be automatically forwarded to a lower classification domain."

- **CoCo v3.2 R2.26** "The mail client or user SHOULD add a warning to each e-mail to the effect that all communications sent to or from their organisations may be subject to recording and/or monitoring in accordance with relevant legislation."

The last version of the GCSx Coco was version, 4.1, had a mandatory requirement that all e-mails are labelled with a protective marking. PSN CoCo is based on GCSx CoCo v4.1 and required for a PSN connection. A GCSx CoCo can be migrated to a PSN CoCo.

[3] http://www.acpo.police.uk/documents/information/2010/201004INFMOPI01.pdf

3 What is janusSEAL?

janusSEAL is a suite of software applications designed to work within Microsoft Office products. Their core functionality is to require end-users to specify the security classifications of e-mails they send, or Office files they create. Once the user has specified the security classification of the item janusSEAL then adds this as fields (metadata) to the item and makes it visible as a protective marking.

janusSEAL is available for

- Outlook;
- Outlook Web Access;
- Microsoft Office Documents; and
- some other commonly used applications or platforms.

Markings applied within janusSEAL can be used to interoperate with a wide variety of email, DLP, encryption gateways

3.1 How does janusSEAL work?

The janusSEAL suite ensures that everyone classifies every document and e-mail message they create. This distributes security responsibility across the organization, reduces the time to achieve practical data protection and rapidly builds a security-aware culture.

janusSEAL's benefits include:

- Addresses accidental data loss (the majority) at source
- Protects Intellectual Property and other vital data
- Limits legal liability and exposure
- Is simple to deploy, administer and use
- Is cost-effective to administer and maintain
- Enhances other security systems like e-mail gateways by making vital data easier to recognize and to protect appropriately.

In practice, janusSEAL:

- Forces end-users to classify all information they create (messages, meeting requests, assigned tasks, documents, spreadsheets, presentations etc)
- Adds protective markings (security classification labels) to key information assets
- Is easy and fast to apply, with single-step classification via a drop-down menu
- Ensures that e-mail gateways and the like can process marked messages and enforce your security policy
- Supports many different security classification schemes used by governments around the world

3.2 The sender's use of janusSEAL

The message's security classification must be specified before it is sent. At a bare minimum a default classification may be configured, so there are no additional button clicks for the sender. Alternatively without a default classification, the sender must select a classification before the message is transmitted.

The range of security classifications presented to the sender is controlled by the system administrator. This range would be configured to match those in use by the organisation, such as the GPMS.

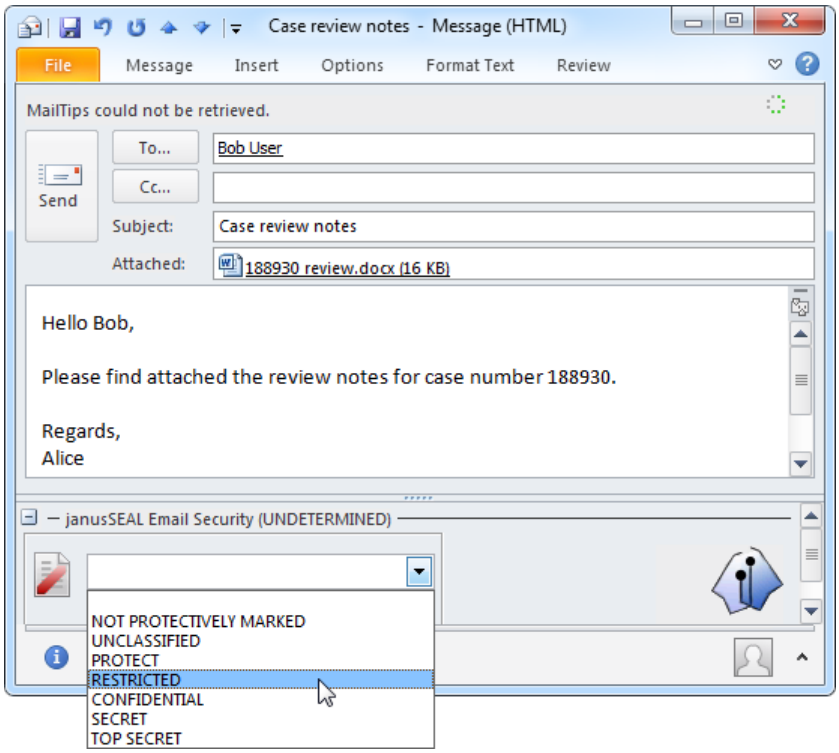


Figure 1: Selecting a GPMS classification using janusSEAL while composing a message

If the sender does not select a security classification when composing the message, then they are forced to do so when sending an e-mail message (or saving an Office file with janusSEAL Documents) via the user-friendly janusSEAL pop-up.

As shown, the pop-up can be configured to use tooltip messages to help explain each security classification to the user.

3.2.1 User Education

Further help beyond the tooltip information is available via the fully configurable help system. The user can click on the Help icon in the classification toolbar, or the Help button in the pop-up. The janusSEAL Help window contains a centrally configured set of hyperlinks to help pages on the organisation's intranet or any internet web site

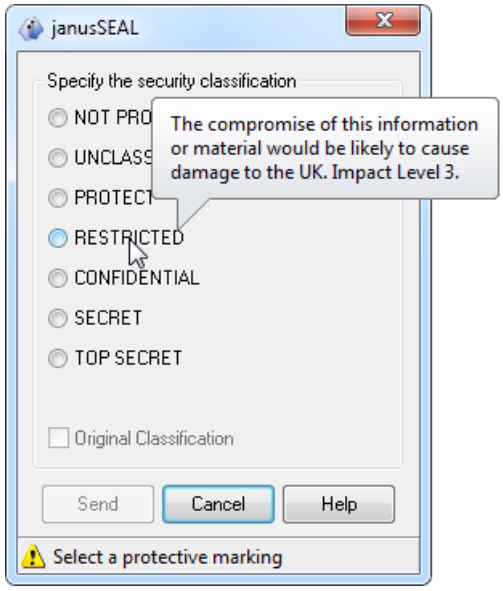


Figure 2: janusSEAL popup forcing classification prior to sending

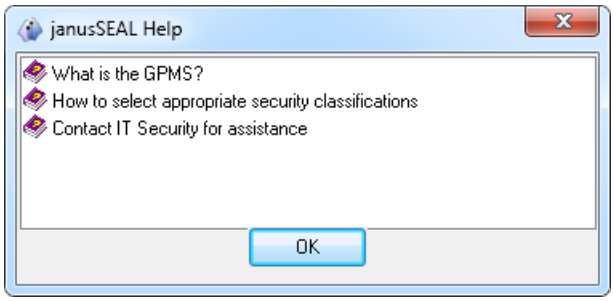


Figure 3: Localised and configurable help aids users with the task of applying a security classification

3.3 The recipient's view of a protectively marked message

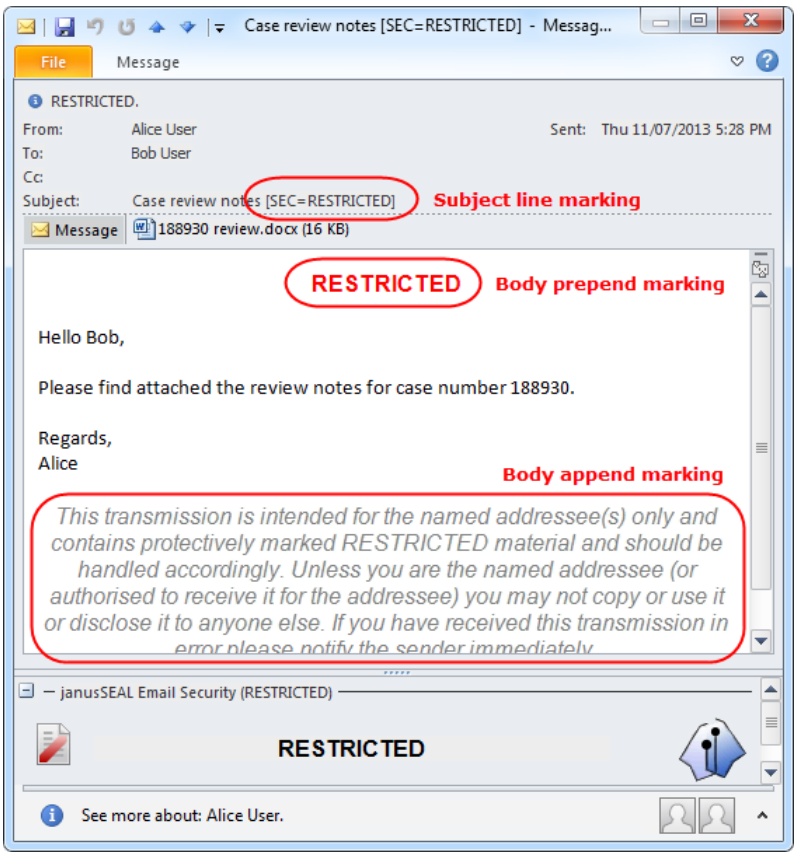
When a user receives a message that has been protectively marked by janusSEAL then the protective marking is visible in numerous places, depending on the janusSEAL configuration.

In this screenshot janusSEAL (at the sender's desktop) has added:

- a subject line marking
- a marking at the start of the message body (body prepend marking)
- a disclaimer that is very specific to the security classification of the message (body append marking)

The message display window also shows the security classification of the message. The reader remains aware of the message's classification, even though the marking at the beginning of the message may have scrolled out of view.

Figure 4 The message is displayed with automatically inserted



protective markings and text

3.4 Event Audit and Security Incident Discovery

High quality audit trails are a cornerstone of good security practice. janusSEAL performs event logging to the Windows Event Log (and/or text file).

The system administrator, when configuring janusSEAL's event logging can define:

- Outputs - where janusSEAL logs information (Event Log and/or text file)
- Levels - the amount of information written to the logs (Error, Warning, Information)
- Event types that are logged at the Information level (when a message is sent, when a reply or forward message's classification is downgraded, when an attachment is added to the message)

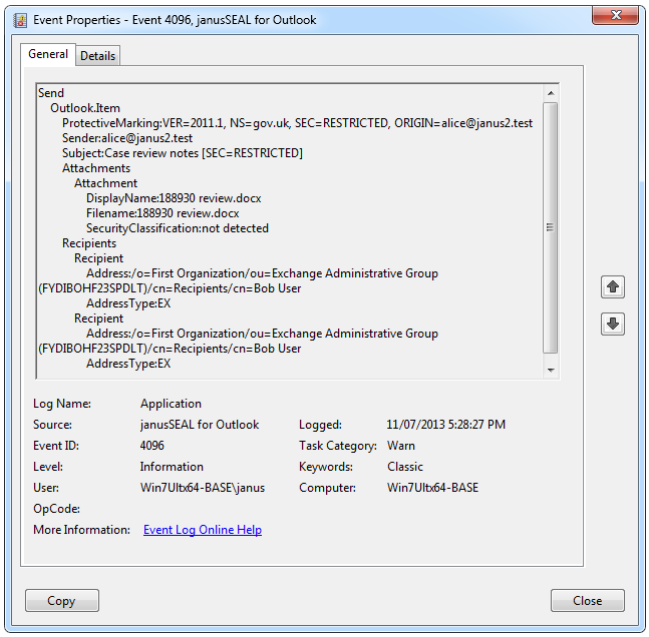
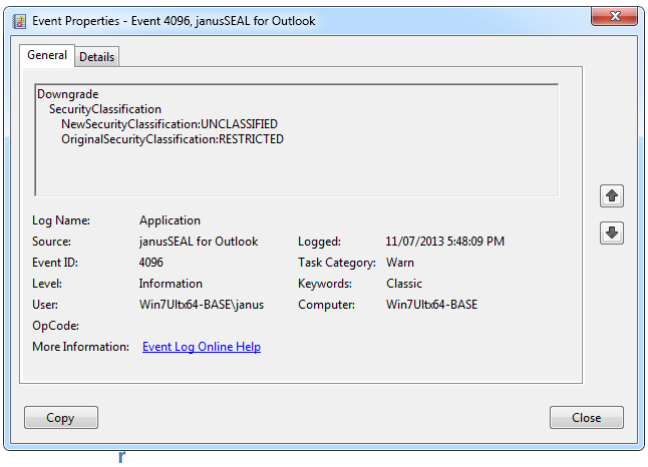


Figure 5: A record in the computer's event log shows the details of a classified message being sent.

3.4.1 Auditing and Security Incident Forensics

janusSEAL captures details about a variety of events that provide good summary information about the event and which can be collated and analysed at a central audit system to detect possible security incidents.

A classification downgrade event, where a sender is replying or forwarding a message and they have chosen to downgrade the security classification[4]



r e 6: A record in the computer's event log show that the sender has downgraded the message's classification

[4] janusSEAL can be configured to disallow classification downgrades, allow them with a warning shown to the sender, or allow them with no warning shown.

4 Using janusSEAL to comply with UK government security requirements

By using an appropriately configured janusSEAL application to protectively mark electronic information assets (e-mail messages, Office files) Her Majesty's Government Departments, Agencies and Local Authorities can readily comply with the protective marking related requirements of the HMG Security Policy Framework.

Security Requirement		janusSEAL Solution
HMG SPF MR 6	...must apply the Protective Marking system...	janusSEAL is easily configured to use the GPMS and ensures electronic information assets such as e-mail messages, meeting requests, assigned tasks and Microsoft Office files have protective markings.
HMG SPF MR 7	Assets must be clearly and conspicuously marked.	janusSEAL has numerous configuration settings about where and how to apply protective markings. janusSEAL can put the markings in message header fields, subject lines, at the start and end of the message body, in Office file fields and in the text, header, footer and watermark areas. The configuration settings also let you use a variety of string tokens related to the security classification and you can also control the font, formatting and paragraph alignment for markings in the message body.
HMG SPF MR 7	Only originator...can protectively mark an asset.	janusSEAL relies on the notion that the person sending the message is the person best able to specify its sensitivity in the form of a security classification. That is why the sender is always forced to select a security classification. With Office files there can be numerous authors of the file over its lifetime. janusSEAL allows each to be the originator but any changes in the security classification are audited.
ACPO/ACPOS CSP	HMG SPF as baseline	*As discussed above, janusSEAL provides compliance for the protective marking requirements of HMG SPF so the protective marking requirements of ACPO/ACPOS CSP are also achieved.*
MoPI 4.2	...ensure that it is given the appropriate GPMS marking.	janusSEAL is easily configured to use the GPMS and ensures electronic information assets such as e-mail messages, meeting requests, assigned tasks and Microsoft Office files have protective markings. janusSEAL's tooltips and configurable help system about the security classifications assist users to apply the appropriate marking.
CoCo v3.2 R2.2.2	Employees...who handle...RESTRICTED must be made aware of the impact of loss of such material...	janusSEAL includes tooltip and help information to assist users on which security classification to use. The help system is fully extensible so that help pages on intranet servers can be quickly accessed.

Security Requirement		janusSEAL Solution
CoCo v3.2 R2.13.1	Audit logs recording user activities, exceptions and information security events must be produced...	janusSEAL can be configured to record audit information to the local Event Log system. These logs can be collated for centralised analysis and incident management.
CoCo v3.2 R2.24.7	E-mail must not be automatically forwarded to a lower classification domain.	Having janusSEAL apply protective markings to e-mails work in conjunction with appropriately configured e-mail gateways ensures e-mail messages cannot be sent to a lower classification domain, user generated or automatically forwarded.
CoCo v3.2 R2.26	The mail client...should add a warning to each e-mail...	janusSEAL can be configured to add text to the end of an e-mail message. This text can include the security classification as well as other text such as a disclaimer. janusSEAL can be configured to use different text depending on the security classification of the sent message. For example, the disclaimer for an UNCLASSIFIED message could be different to that of a RESTRICTED message.
CoCo v4.1/PSN CoCo	Labelling e-mails with protective markings	janusSEAL's core functionality is to ensure senders apply a security classification to all e-mails they send. Once the security classification has been specified by the sender janusSEAL inserts it as one or more protective markings in the message based on its configuration.

4.1 Evaluate janusSEAL

To obtain a fully working evaluation version of a janusSEAL product visit http://www.janusnet.com/evaluate

5 About janusNET, the makers of janusSEAL

janusNET was founded in 2004 following 11 years of research, development and innovative thinking around security for electronic information.

In 2005 janusNET's directors were chosen to co-author the "Protective Markings for Internet E-mail Messages", published by the Australian Government Information Management Office (AGIMO). This standard enables Australian Government Agencies to use a common format for e-mail security classifications, greatly simplifying protection of their information, whether shared between or outside government.

Since then their janusSEAL suite of products has evolved, providing comprehensive classification and protection of files created in Microsoft environments, from Word documents to PowerPoint presentations, and e-mails in Outlook, Pocket Outlook and Outlook Web Access. As a result janusSEAL has become a standard for document classification and protection within government and industry.

6 Contact janusNET in the UK

Telephone: +44 20 3318 0785
e-mail: info@janusnet.com
web: http://www.janusnet.com/