Compliance with the Queensland Government Information Security Classification Framework

Janusnet

Introduction

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.

The Queensland Government Information Security Classification Framework (QGISCF) supports the Information security policy (IS18:2018). The third requirement of this policy states that "Departments must meet minimum security requirements" and that they must comply with the QGISCF, wherein agencies "should classify their information and assets according to business impact and implement appropriate controls according to the classification."

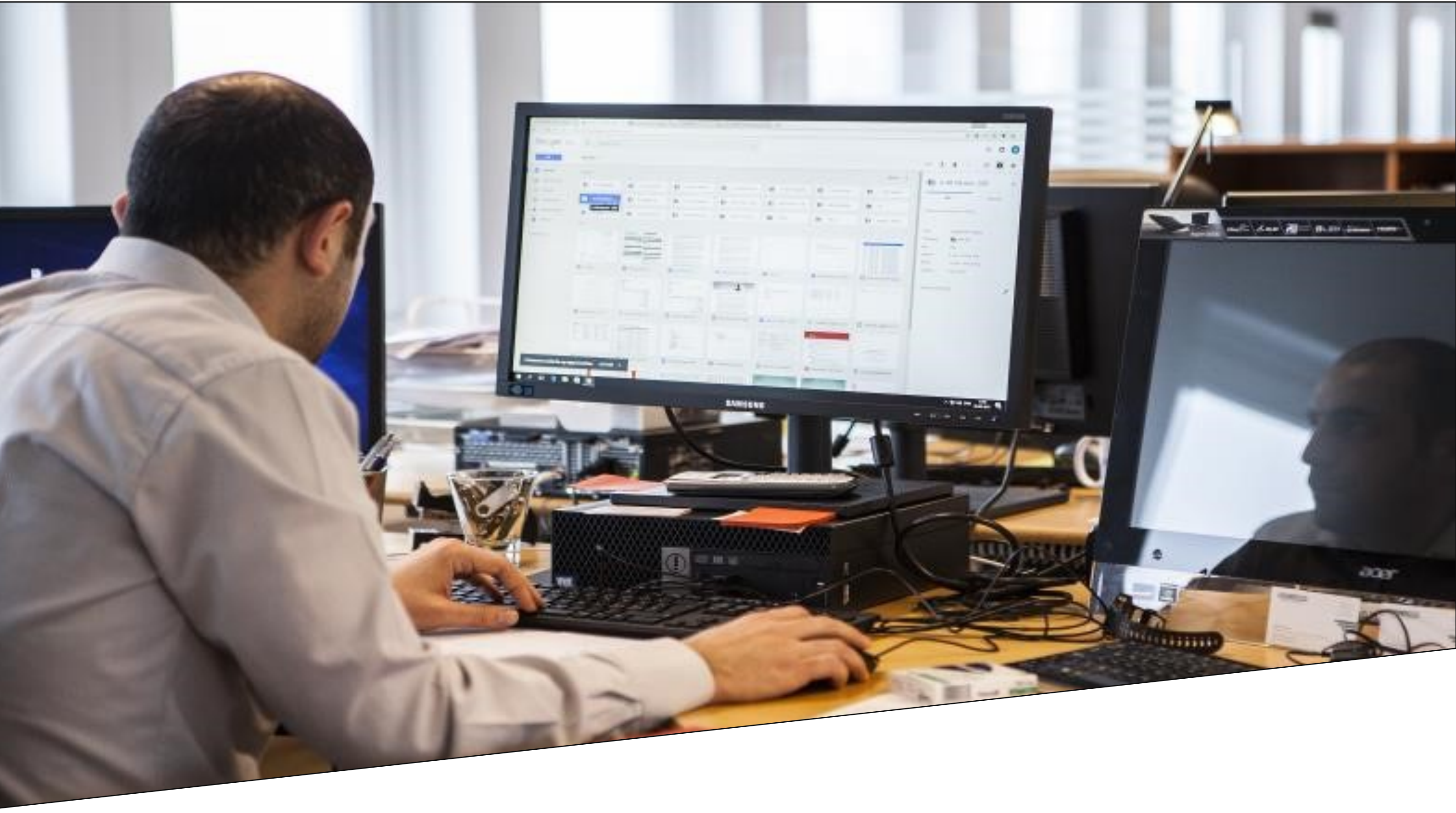
Many agencies can meet these requirements using the Janusseal suite of applications from Janusnet. The Janusseal suite is a range of add-ons for Microsoft Office products. The Janusseal add-ons require end-users to assign security classifications to all the e-mail messages they send and files they create. These security classifications help other users and Information Technology (IT) systems measure 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 Queensland Government departments
- Demonstrates how the Janusseal suite can be used to comply with those requirements

Applicability

Does the Queensland Government Information Security Classification Framework (QGISCF) apply to your organisation? The QGISCF is a subset of the Queensland Government Information Security Policy (IS18:2018) which applies to all Queensland Government departments (as defined by its Public Service Act 2008). So if the IS18:2018 applies to your organisation, then so does the QGISCF.



Protective Markings

What are they 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 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 depicting wartime events. 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 should protect that information. The marking in, and of itself, however, does not provide any protection.

The Queensland Government advocates classification of information according to business impact so that appropriate controls can be implemented to protect the information accordingly.

> *Consistent classification of information helps Queensland government agencies make more informed and timely decisions about how they should capture, store, maintain, transmit, process, use and share information to best deliver services to Queenslanders.*

The QGISCF discusses classification from three dimensions of information security – integrity, availability and confidentiality. Classification regarding confidentiality is to be considered in relation to the increasing business impact. These three levels of confidentiality depend on whether the information is to be compromised or shared inappropriately and consist of:

- OFFICIAL – low or negligible confidentiality impact
- SENSITIVE – moderate confidentiality impact
- PROTECTED – high confidentiality impact

The QGISCF *mandates* that agencies label (protectively mark) all new information with a moderate to high confidentiality impact (higher than OFFICIAL) and that they *should* apply labels to all information to signify confidentiality levels.

Email Protective Markings

As is the case for paper-based information, electronic-based information needs to be marked with an appropriate protective marking. This ensures that appropriate security measures are applied to the information and helps prevent unauthorised disclosure of the information in the public domain. When a protective marking is applied to an email, it is important that it reflects the sensitivity or classification of the information in the body of the email and in any attachments of the email.

Protective Marking tools

Requiring user intervention in the marking of user generated emails assures a conscious decision by the user, lessening the chance of incorrectly marked emails. Allowing users to choose only protective markings for which the system is accredited, lessens the chance of a user inadvertently over-classifying an email. It also reminds users of the maximum sensitivity or classification of information permitted on the system.

Protective Markings in use in QLD

The QGISCF details the classification labels that are to be used for confidentiality purposes. As mentioned already, these are: OFFICIAL, SENSITIVE and PROTECTED.

For agencies that deal with National Security Information that is above PROTECTED then the framework integrates into the broader Australian Government approach to allow interoperability.

Appendix G of QGISCF also allows the use of optional descriptors added to the protective marking to support specific business requirements and the compartmentalisation of the information. But such descriptors might not be understood outside of the organisation and therefore the information may not be handled and protected in the required manner.

Protective Marking	Description
OFFICIAL	OFFICIAL information is routine information without special sensitivity or handling requirements. All routine public-sector business, operations and services is treated as OFFICIAL. At the OFFICIAL classification there is a general presumption that data may be shared across government. Security measures should be proportionate and driven by the business requirement.
SENSITIVE	The use of SENSITIVE indicates that information requires additional handling care due to its sensitivity or moderate business impact if compromised or lost. Examples of SENSITIVE information may include: • government or agency business, whose compromise could affect the government's capacity to make decisions or operate, the public's confidence in government, the stability of the market place and so on • commercial interests, whose compromise could significantly affect the competitive process and provide the opportunity for unfair advantage • legal professional privilege • law enforcement operations whose compromise could adversely affect crime prevention strategies, particular investigations or adversely affect personal safety • personal information, which is required to be safeguarded under the Information Privacy Act 2009, or other legislation.
PROTECTED	PROTECTED information requires the most careful safeguards due to its sensitivity or major business impact if compromised or lost. PROTECTED information assets require a substantial degree of control as compromise could cause serious damage to the State, the Government, commercial entities or members of the public. For instance, compromise could: • endanger individuals' lives and private entities; • work substantially against government finances or economic and commercial interests; • substantially undermine the financial viability of major organisations; and/or • impede the investigation or facilitate the commission of serious crime. • Information passed by other governments that is marked PROTECTED

Queensland Cabinet information is treated as PROTECTED, but should also be marked with Cabinet-in-Confidence. Janusnet advises that this Cabinet-in-Confidence marking be implemented as a special-handling caveat to be consistent with the notion used at the Federal Government level.

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 emails 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 (Windows and Mac)
- Outlook on the Web; Outlook Web App
- Outlook Mobile (Android and iOS)
- Office Suite: Word, Excel, Powerpoint
- Windows File Explorer for non-Microsoft file types

How does Janusseal work?

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

Janusseal 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 email gateways by making valuable data easier to recognise and to protect appropriately.

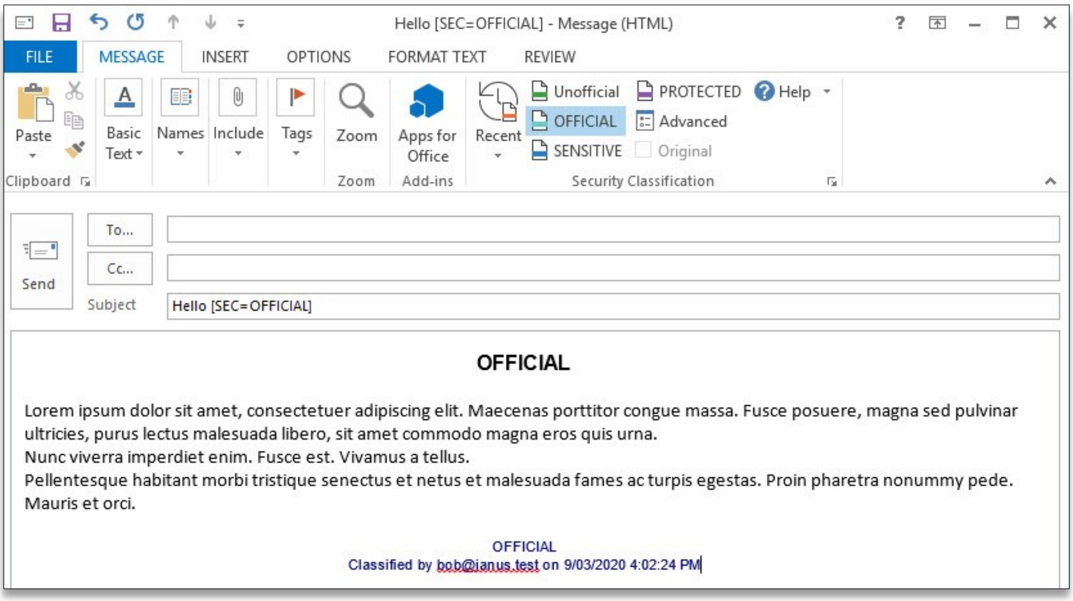
In practice, Janusseal:

- Forces end-users to classify all information they create (presentations, messages, meeting requests, assigned tasks, documents, spreadsheets)
- 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 email 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

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.



Subject: Hello [SEC=OFFICIAL]

OFFICIAL

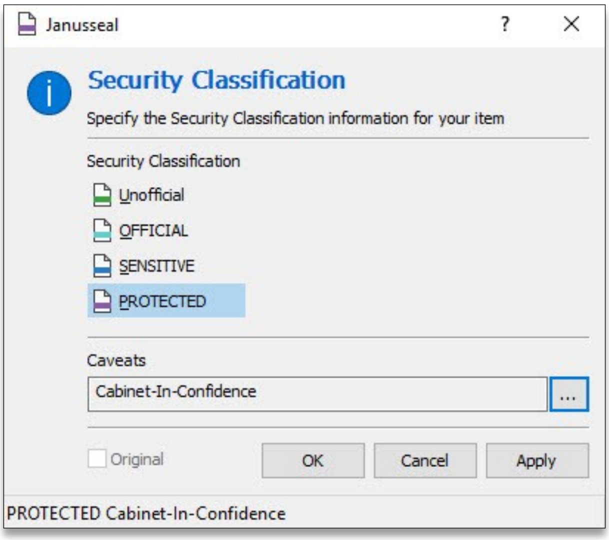
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. Fusce posuere, magna sed pulvinar ultricies, purus lectus malesuada libero, sit amet commodo magna eros quis urna.
Nunc viverra imperdiet enim. Fusce est. Vivamus a tellus.
Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Proin pharetra nonummy pede. Mauris et orci.

OFFICIAL
Classified by bob@ianus.test on 9/03/2020 4:02:24 PM

Figure 1: Selecting a QLD 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 email message (or saving an Office file with Janusseal Documents) via the user-friendly Janusseal pop-up.

Figure 2: Janusseal pop-up forcing classification prior to sending



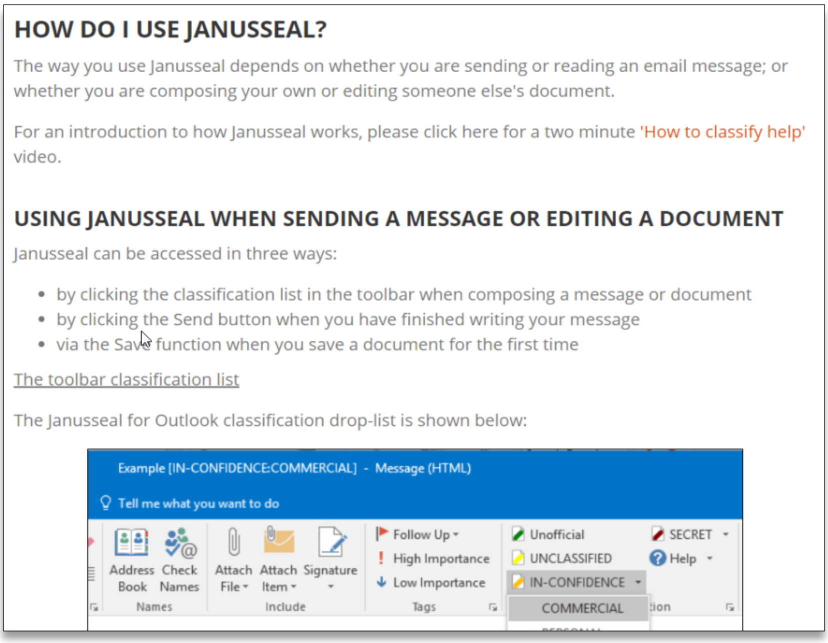
Security Classification: PROTECTED

Caveats: Cabinet-In-Confidence

PROTECTED Cabinet-In-Confidence

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 website.



HOW DO I USE JANUSSEAL?

The way you use Janusseal depends on whether you are sending or reading an email message; or whether you are composing your own or editing someone else's document.

For an introduction to how Janusseal works, please click here for a two minute 'How to classify help' video.

USING JANUSSEAL WHEN SENDING A MESSAGE OR EDITING A DOCUMENT

Janusseal can be accessed in three ways:

- by clicking the classification list in the toolbar when composing a message or document
- by clicking the Send button when you have finished writing your message
- via the Save function when you save a document for the first time

The toolbar classification list

The Janusseal for Outlook classification drop-list is shown below:

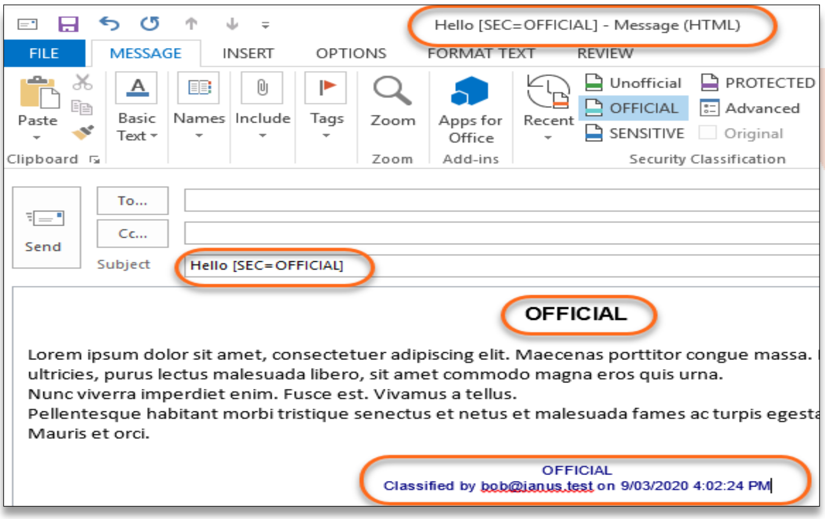
Example [IN-CONFIDENCE:COMMERCIAL] - Message (HTML)

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

The recipient’s view of a protectively marked message

When a user receives a message that has been protectively marked by Janusseal, 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 title of the message dialog box
- a subject line marking
- a marking at the start of the message body (body prepend marking). Also shown here a body append marking.



Hello [SEC=OFFICIAL] - Message (HTML)

Subject: Hello [SEC=OFFICIAL]

OFFICIAL

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Maecenas porttitor congue massa. ultricies, purus lectus malesuada libero, sit amet commodo magna eros quis urna.
Nunc viverra imperdiet enim. Fusce est. Vivamus a tellus.
Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egesta
Mauris et orci.

OFFICIAL
Classified by bob@janus.test on 9/03/2020 4:02:24 PM

Figure 4: recipient’s view of a protectively marked email

Optional capabilities available at customer request (not shown here):

- a disclaimer that is very specific to the security classification of the message (body append marking / disclaimer)
- Outlook form region

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.

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, a text file and/or a syslog server.

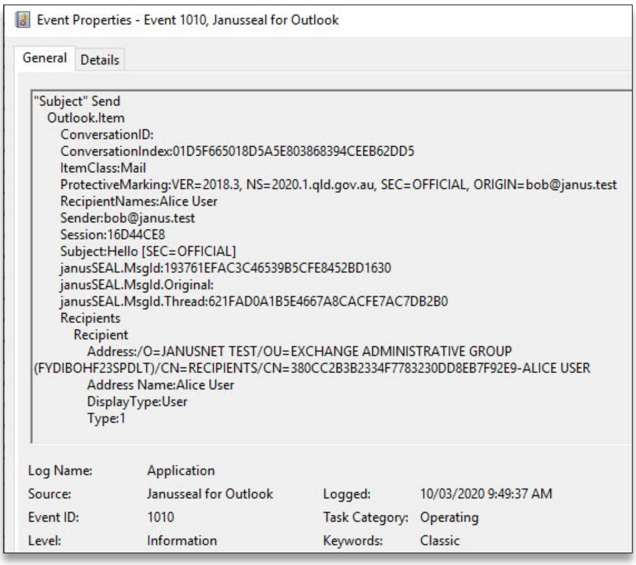
The system administrator, when configuring Janusseal's event logging, can define:

- Outputs - where Janusseal logs information (Event Log, text file, and/or syslog server)
- Levels - the amount of information written to the logs (Error, Warning, Information)

Event types that are logged at the Information Level include: when a message is sent, when a reply or forward message's classification is downgraded and when an attachment is added to the message.

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.

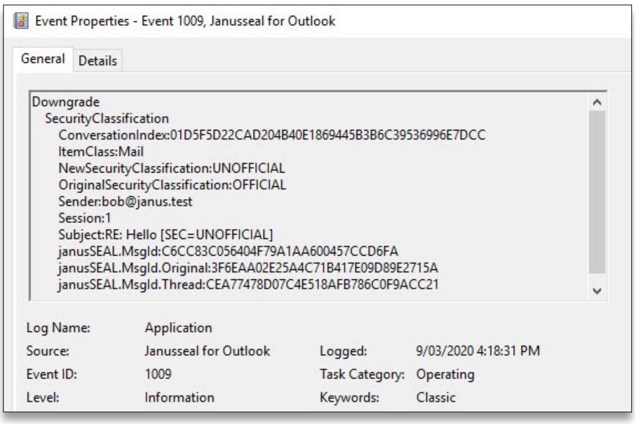


```
"Subject" Send
  Outlook.Item
    ConversationID:
    ConversationIndex:01D5F665018D5A5E803868394CEEB62DD5
    ItemClass:Mail
    ProtectiveMarking:VER=2018.3, NS=2020.1.qld.gov.au, SEC=OFFICIAL, ORIGIN=bob@janus.test
    RecipientNames:Alice User
    Sender:bob@janus.test
    Session:16D44CE8
    Subject:Hello [SEC=OFFICIAL]
    janusSEAL.MsgId:193761EFAC3C46539B5CFE8452BD1630
    janusSEAL.MsgId.Original:
    janusSEAL.MsgId.Thread:621FAD0A1B5E4667A8CACFE7AC7DB2B0
    Recipients
      Recipient
        Address:/O=JANUSNET TEST/OU=EXCHANGE ADMINISTRATIVE GROUP
(FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=380CC2B3B2334F7783230DD8EB7F92E9-ALICE USER
        Address Name:Alice User
        DisplayType:User
        Type:1

Log Name:   Application
Source:     Janusseal for Outlook    Logged:          10/03/2020 9:49:37 AM
Event ID:   1010                     Task Category:   Operating
Level:      Information              Keywords:        Classic
```

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

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



```
Downgrade
  SecurityClassification
    ConversationIndex:01D5F5D22CAD204B40E1869445B3B6C39536996E7DCC
    ItemClass:Mail
    NewSecurityClassification:UNOFFICIAL
    OriginalSecurityClassification:OFFICIAL
    Sender:bob@janus.test
    Session:1
    Subject:RE: Hello [SEC=UNOFFICIAL]
    janusSEAL.MsgId:C6CC83C056404F79A1AA600457CCD6FA
    janusSEAL.MsgId.Original:3F6EAA02E25A4C71B417E09D89E2715A
    janusSEAL.MsgId.Thread:CEA77478D07C4E518AFB786C0F9ACC21

Log Name:   Application
Source:     Janusseal for Outlook    Logged:          9/03/2020 4:18:31 PM
Event ID:   1009                     Task Category:   Operating
Level:      Information              Keywords:        Classic
```

Figure 6: A record shows that the sender has downgraded the message's classification

Janusseal event logging can be directed to syslog servers and/or Security Information and Event Management (SIEM) systems, so log events can be transmitted over the network and collated at a centralised system. Thus, with some design, and depending on the capabilities of the system, forensic reporting can be developed for management reports of classification related activity and investigations.

EVALUATE JANUSSEAL

By obtaining a fully working evaluation version with SAPSF configuration of one of the suite available at www.janusnet.com/evaluate

About Janusnet, the makers of Janusseal

Janusnet is an Australian software developer. Janusseal products are used in organisations worldwide to enforce their security classification policies to distinguish between public, private and highly sensitive information; and Janusgate technology is used to better manage message flow.

Janusnet was incorporated in 2004. Around that time the founders had co-authored the original Email Protective Marking Standard (EPMS). This open standard spawned several new products for the marking of emails in a consistent and non-proprietary manner. Janusseal for Outlook was one of those products.

Over the years, Janusnet’s reputation has grown and customers have converted from alternative marking software to become Janusnet customers. Today Janusseal for Outlook is used in the majority of Commonwealth Departments and agencies and in many state agencies. The EPMS has changed over time and each time Janusnet has been the leader in the application of the new standard.

Contact Janusnet

phone:	02 8004 9300
email:	info@janusnet.com
web:	www.janusnet.com/

References

Queensland Government Information Security Policy – IS18:2018:

- https://www.qgcio.qld.gov.au/documents/information-security-policy

Queensland Government Information Security Classification Framework (QGISCF)

- https://www.qgcio.qld.gov.au/documents/information-security-classification-framework-qgiscf

Queensland Cabinet Handbook

- https://www.premiers.qld.gov.au/publications/categories/policies-and-codes/handbooks/cabinet-handbook.aspx