Compliance with the Victorian Protective Data Security Standards 2019

Protective Markings

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 Victorian Protective Data Security Standards (VPDSS) establish 12 high level mandatory requirements to protect public sector information across all security areas including governance, information, personnel, Information Communications Technology (ICT) and physical security." Ref: https://ovic.vic.gov.au/data-protection/standards/. The second requirement of the VPDSS is titled 'Information Security Value' and the standard is that "An organisation identifies and accesses the security value of public sector information".

To assist organisations with meeting the VPDSS requirements, the Office of the Victorian Information Commissioner (OVIC) also provides an implementation guide that describes a security measure, or measures, which can be implemented to meet the requirement; these measures are called elements (often termed a control in risk assessment methodology). In this guide, VPDSS requirement #2 has several elements, but of particular relevance to this paper is E2.050 – "The organisation applies appropriate protective markings to information throughout its lifecycle."

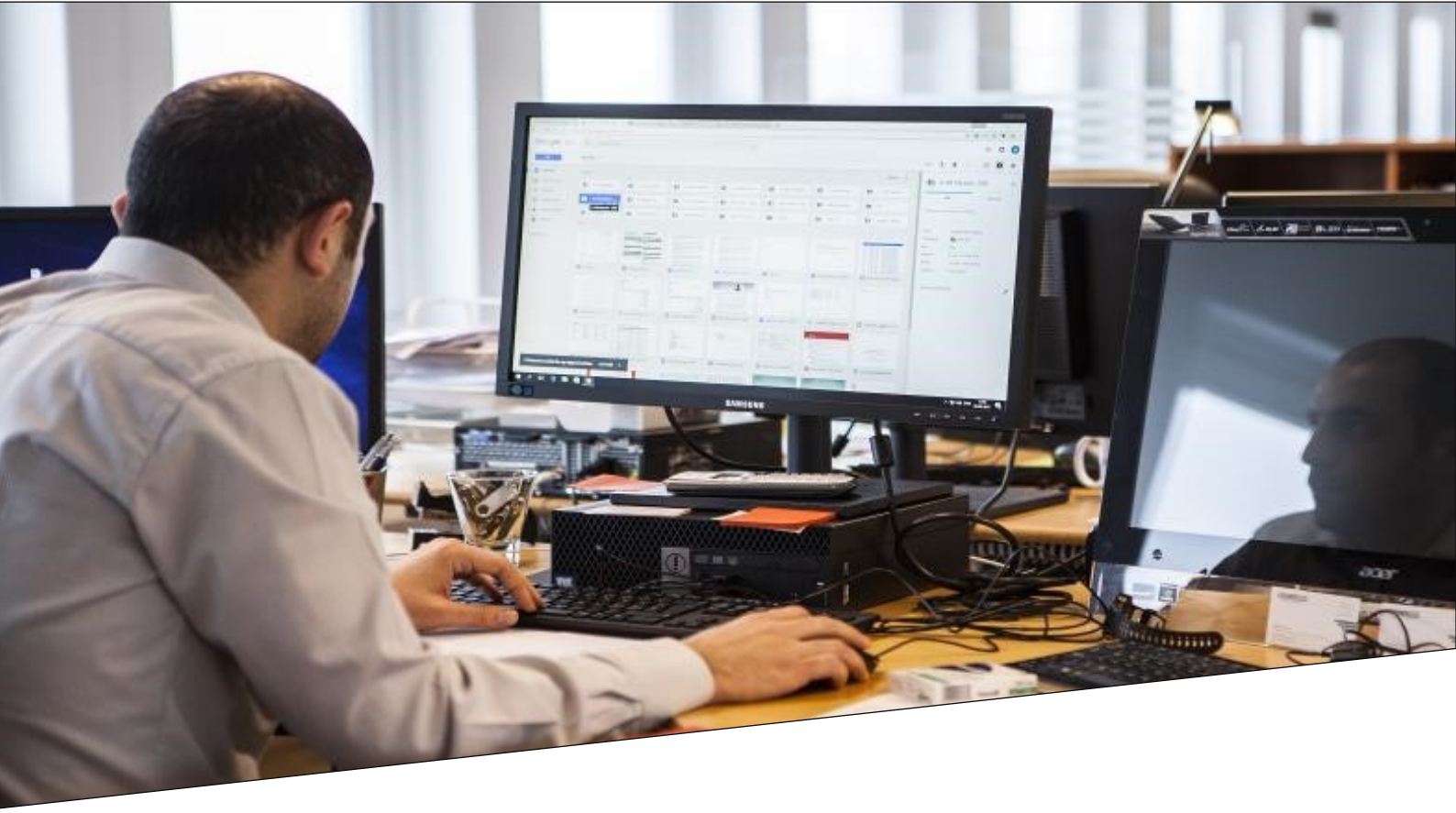
Many agencies can implement E2.050 using the Janusseal suite of applications from Janusnet. The Janusseal suite is a range of add-ons for Microsoft Office products. The Janusseal add-ons require end-users to assign security classifications to all the email messages they send and files they create. These 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 Victorian Government departments (and any entities to which the VPDSS applies)
- Demonstrates how the Janusseal suite can be used to comply with those requirements

Applicability

Does the Victorian Protective Data Security Standards (VPDSS) and Framework (VPDSF) apply to your organisation? The full answer is provided at https://ovic.vic.gov.au/resource/does-the-victorian-protective-data-security-framework-apply-to-your-organisation/ ; formally they apply if your organisation or body are declared by the Governor in Council to be subject to Part 4 of the Privacy and Data Protection Act 2014 (Vic) in the Government Gazette, or to be declared as 'public entities' under the Public Administration Act 2004 (Vic).



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 Victorian Government advocates use of protective markings on information via element E2.050 to satisfy requirement #2 of the VPDSS. It further defines the protective markings to be used by Victorian Government entities in the Practitioner Guide: Protective Markings document.

As espoused in that document.

> *Everyone who works with public sector information has an obligation to respect the information that they create, access and use, and are personally accountable for safeguarding this material. In order to do this, all persons need to have an understanding of the security value of public sector information, and the security measures designed to protect the confidentiality, integrity and availability of public sector information.*

The document further details the benefits of protective markings:

> *Consistent use of protective markings, coupled with the adoption of appropriate security measures, enhances Victorian Government's ability to conduct business in a secure and effective manner.*
>
> *Protective markings act as an important visual signal to anyone accessing or using the material, informing the minimum-security obligations that need to accompany public sector information.*
>
> *Protective markings offer an easily identifiable way for information users (visually) and for systems (such as an entity's email gateway) to identify and manage the handling and control of information at different 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 VIC

This is covered in detail in OVIC's Practitioner Guide: Protective Markings. Therein Victorian Government describes its approach to classifying and labelling sensitive information and is generally aligned with the Commonwealth system. Consistent classification and labelling allow sensitive information to be securely shared across Australian jurisdictions, with confidence that the information will be handled and protected according to its sensitivity.

There are three main components of a protective marking: security classification, information management markers and caveats. Specific definitions of each protective marking are set out in the table below. (This table does not list caveats or information management markers, which may be used in conjunction with security classifications – in accordance with the OVIC Practitioner Guide.)

Protective Marking	Business Impact Level	Description
UNOFFICIAL	0	An optional marking that is used (particularly with email messages) to indicate that the information has no relation to official activities, such as personal correspondence.
OFFICIAL	1	Applied to public sector information that requires some form of protection, or compromise of this information may cause minor harm/damage to government operations, organisations and/or individuals.
OFFICIAL: Sensitive	2	Applied to public sector information where secrecy provisions or enactments apply to the content, or where disclosure of the material may be limited or prohibited under legislation. This indicates compromise of the confidentiality of the information may cause limited harm/damage to government operations, organisations and/or individuals.
PROTECTED	3	Applied to public sector information where compromise of the confidentiality of the information may cause major harm/damage to government operations, organisations and/or individuals.
SECRET	4	Applied to public sector information where compromise of the confidentiality of the information may cause serious harm/damage to government operations, organisations and/or individuals.

PROTECTED and SECRET are the only two true security classifications used in Victoria; the lower sensitivity protective markings can be thought of as pseudo-classifications.

Information Management Markers can be added to the protective marking for anything OFFICIAL and above. They are used to reflect 'rights properties' for particular content and can inform access restrictions. They are not mandatory. The three commonly recognised IMMs in Victoria are:

- Legislative Secrecy
- Personal Privacy, and
- Legal Privilege

Caveats indicate extra special security requirements for public sector information in addition to the confidentiality requirements of the security classification, further restricting access to the material. Victoria generally

recognises the national level caveats of the Commonwealth, as well as its own Cabinet-In-Confidence caveat that can be used with information at a security classification of either PROTECTED or SECRET.

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.

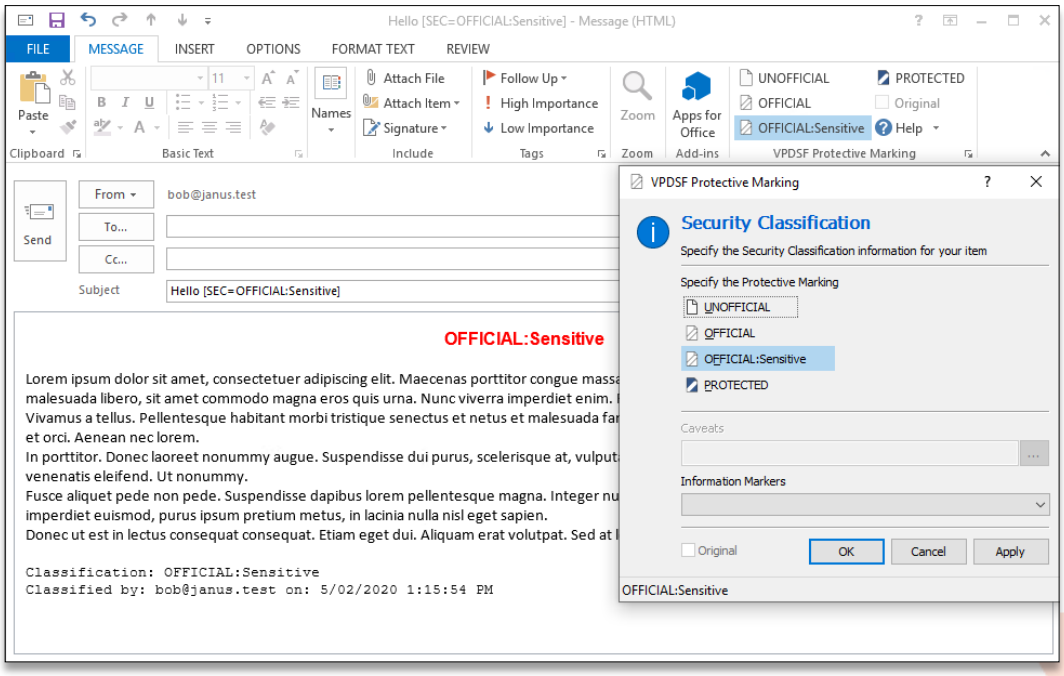


Figure 1: Selecting a VIC classification using Janusseal while composing a message

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 those defined in the OVIC Practitioners Guide for Protective Markings.

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.

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

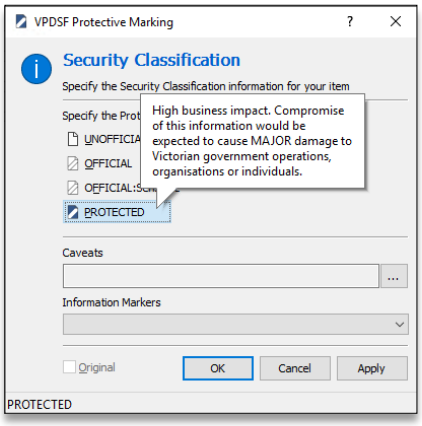


Figure 2: Janusseal pop-up forcing classification prior to sending.

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.

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 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 title of the message dialog box
- a subject line marking
- a marking at the start of the message body (body prepend marking)

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

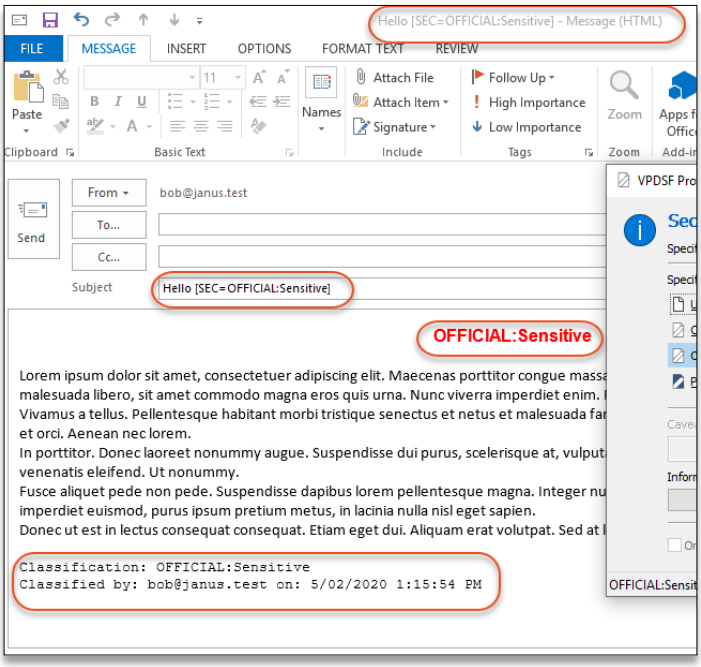


Figure 4: recipient's view of a protectively marked email

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 (when a message is sent, when a reply or forward message's classification is downgraded, 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.

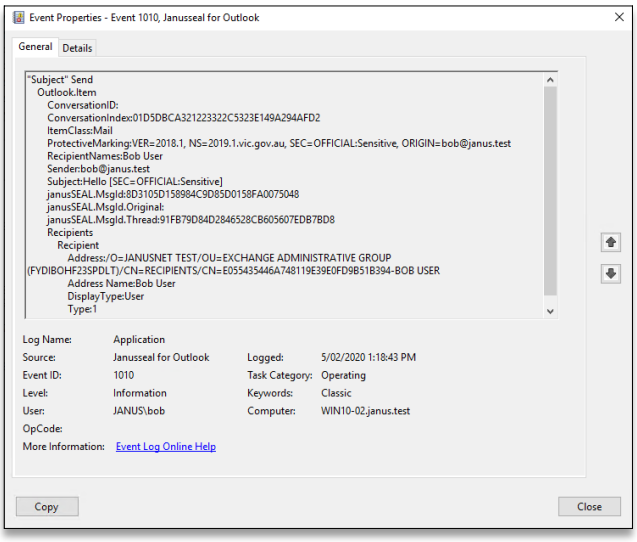
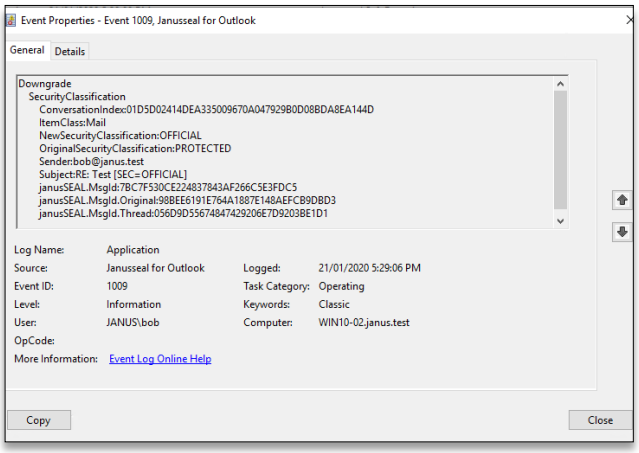


Figure 5: A record in the computer's event log shows the details of a classified message being sent.

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

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 VPDSS 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

- Victorian Protective Data Security Standards V2.0 (VPDSS 2.0) and Implementation Guidance
  - https://ovic.vic.gov.au/data-protection/standards/
  - https://ovic.vic.gov.au/wp-content/uploads/2019/10/VPDSS-V2.0-Standards-and-Objectives_web-version.docx
  - https://ovic.vic.gov.au/wp-content/uploads/2019/10/VPDSS-V2.0-Implementation-Guidance_web-version.docx
- Practitioner Guide Protective Markings V2.0
  - https://ovic.vic.gov.au/resource/practitioner-guide-protective-markings-v2-0/