Compliance with the South Australian Protective Security Framework (Information Classification System)

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 South Australian Protective Security Framework incorporates relevant South Australian security policies and provides tailored guidance and other resources for all South Australian public sector agencies. Part of the Framework is the Information Security Policy which aims to ensure all South Australian Government agencies protect their information assets from compromise.

A deeper component of the Information Security Policy is the South Australian Information Classification System. All South Australian Government agencies "…must use the system when assessing the confidentiality, integrity and availability of their information assets to ensure appropriate classification, protective markings and handling requirements are assigned."

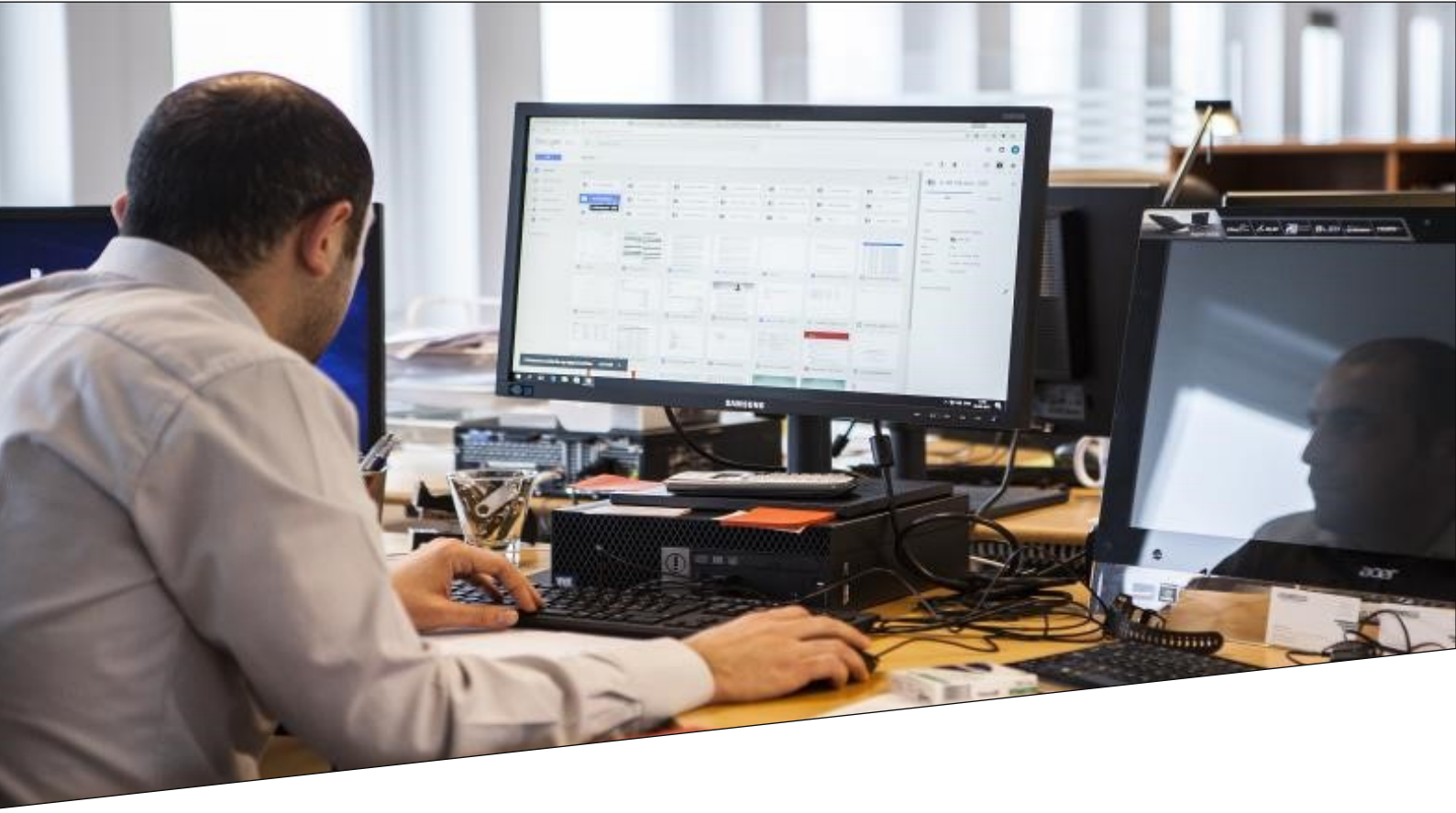
Many agencies can implement this requirement using the Janusseal suite of applications from Janusnet. The Janusseal suite is a range of add-ons for Microsoft Office products. The Janusseal add-ons require end-users to assign security classifications to all the email messages they send and files they 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 South Australian Government agencies
- Demonstrates how the Janusseal suite can be used to comply with those requirements

Applicability

The South Australian Information Classification System (ICS) applies to all organisations which are a South Australian public sector agency (as defined in the Public Sector Act 2009) or which are generally subject to the direction of a Minister of the Crown.



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 South Australian Government advocates use of protective markings on information in the South Australian Information Classification System (SAICS) Overview document.

As espoused in that document.

Information produced within the South Australian Government creates an official records [sic] of government actions and decisions. Official records must be appropriately protected to prevent damage from intentional and accidental threats. Assessing the business impact or 'damage' that may occur from compromise of official information enables agencies to apply the appropriate classification.

Classification enables agencies to protect their information in a consistent, organised and appropriate way.

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 SA

This is covered in detail in the SAICS Overview document. Therein the South Australian Government describes its approach to classifying and labelling sensitive information. Its Information Classification System (ICS) is based upon the Commonwealth Government's sensitive and classified information requirements under the Protective Security Policy Framework (PSPF), with some modifications to suit the South Australian context.

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 on the following page. (This table does not list caveats or information management markers, which may be used in conjunction with security classifications – in accordance with the SAICS Overview document.)

Classifications

Protective Marking	Business Impact Level	Description
UNOFFICIAL	0	UNOFFICIAL can be used for non-work-related information (including emails). Use of the protective marking is optional.
OFFICIAL	1	OFFICIAL describes routine information created or processed by the South Australian public sector with a low business impact. Use of the protective marking is optional, but recommended.
OFFICIAL: Sensitive	2	OFFICIAL: Sensitive identifies sensitive, but not security classified information. It is a single dissemination limiting marker (DLM) which indicates that compromise of the information may result in limited damage to an individual, organisation or government generally. Use of the protective marking is mandatory.
PROTECTED	3	PROTECTED is a security classification which indicates that compromise of the information may result in damage to the state or national interests, organisations or individuals. Use of the protective marking is mandatory.
SECRET	4	SECRET is a security classification which indicates compromise of the information may result in serious damage to the state or national interests, organisations or individuals. Use of the protective marking is mandatory.
TOP SECRET	5	TOP SECRET is a security classification which indicates compromise of the information may result in exceptionally grave damage to the state or national interests, organisations or individuals. Use of the protective marking is mandatory.

Information Management Markers

The ICS provides agencies with optional information management markers (IMMs) which can be used to help identify information which may have legislative or professional restrictions. They are not mandatory. The IMMs are not classifications and must only be used in addition to an appropriate classification of OFFICIAL:Sensitive or higher. IMMs do not provide any greater level of protection than the classification and are intended for information management purposes where disclosure of the content would breach specific legislative or professional restrictions.

The recognised IMMs in South Australia are:

- Legislative Secrecy
- Personal Privacy
- Legal Privilege
- Medical in Confidence

Caveats

A caveat is a further indication that the information contained has additional special protections and/or handling requirements beyond those indicated by the classification. Types of caveats which may be encountered in South Australian government include sensitive compartment information (codewords), foreign government markings, special handling instructions or releasability caveats; these caveats generally align with the national level caveats of the Commonwealth. South Australia does have its own SA Cabinet caveat that can be used with information at a security classification of OFFICIAL:Sensitive and above.

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, such as those defined in the SAICS Overview document.

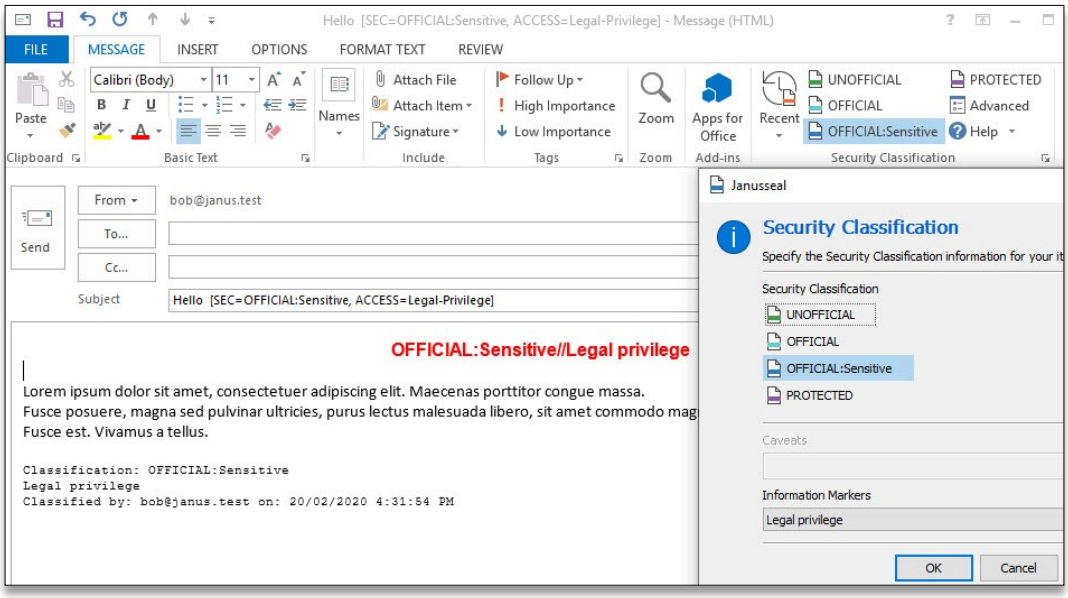


Figure 1: Selecting a SA classification using Janusseal while composing a message

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.

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

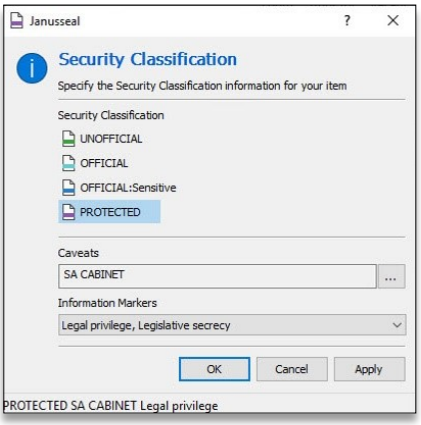


Figure 2: Janusseal pop-up forcing classification prior to sending

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, 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 an body append 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

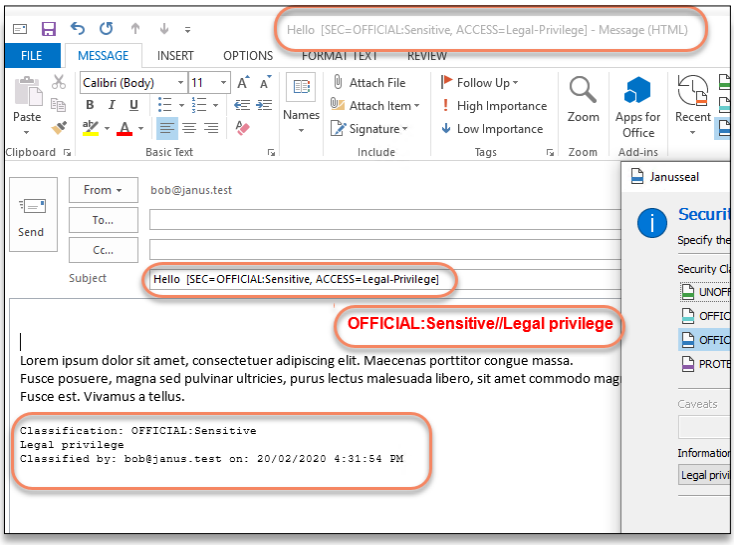


Figure 4: recipient's view of a protectively marked email

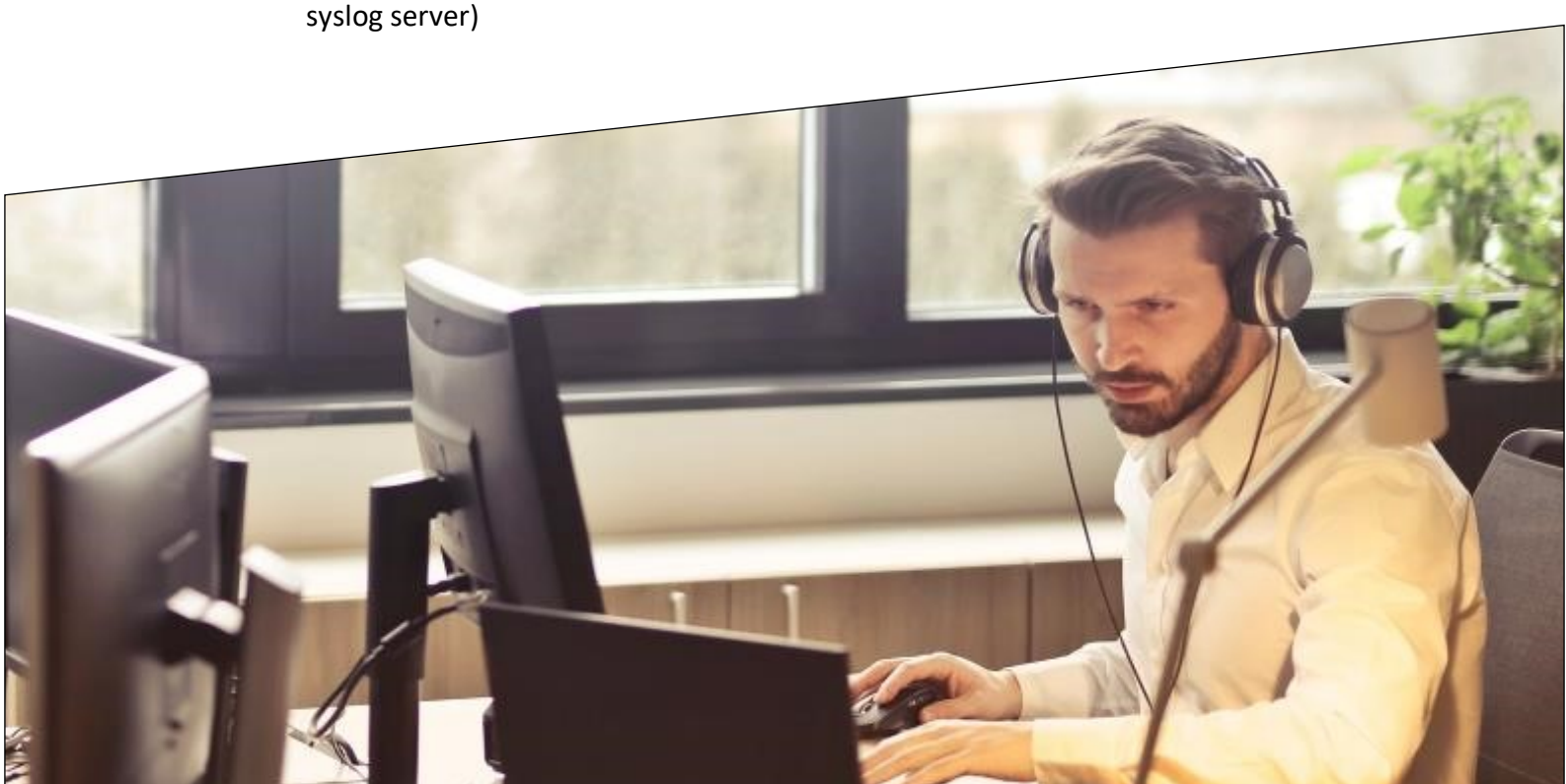
The message display window also shows the security classification of the message. The reader remains aware of the message's classification, even though the marking at the beginning of the message may have scrolled out of view.

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 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.

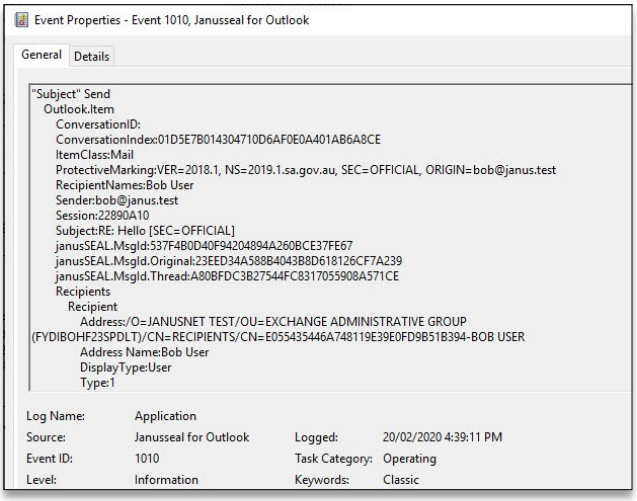
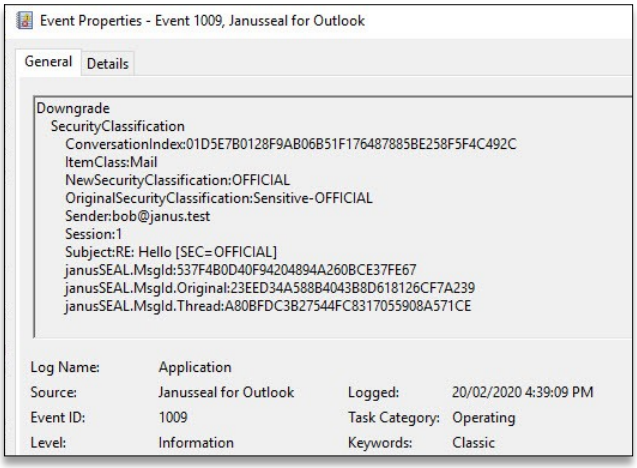


Figure 5: A record in the computer's event log shows the details of a classified message being sent



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.

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

- South Australian Protective Security Framework
  https://www.dpc.sa.gov.au/responsibilities/protective-security-framework
- Information Security
  https://www.dpc.sa.gov.au/responsibilities/protective-security-framework/information-security
- South Australian Information Classification System
  https://www.dpc.sa.gov.au/responsibilities/protective-security-framework/information-security/south-australian-information-classification-system
- South Australian Information Classification System overview