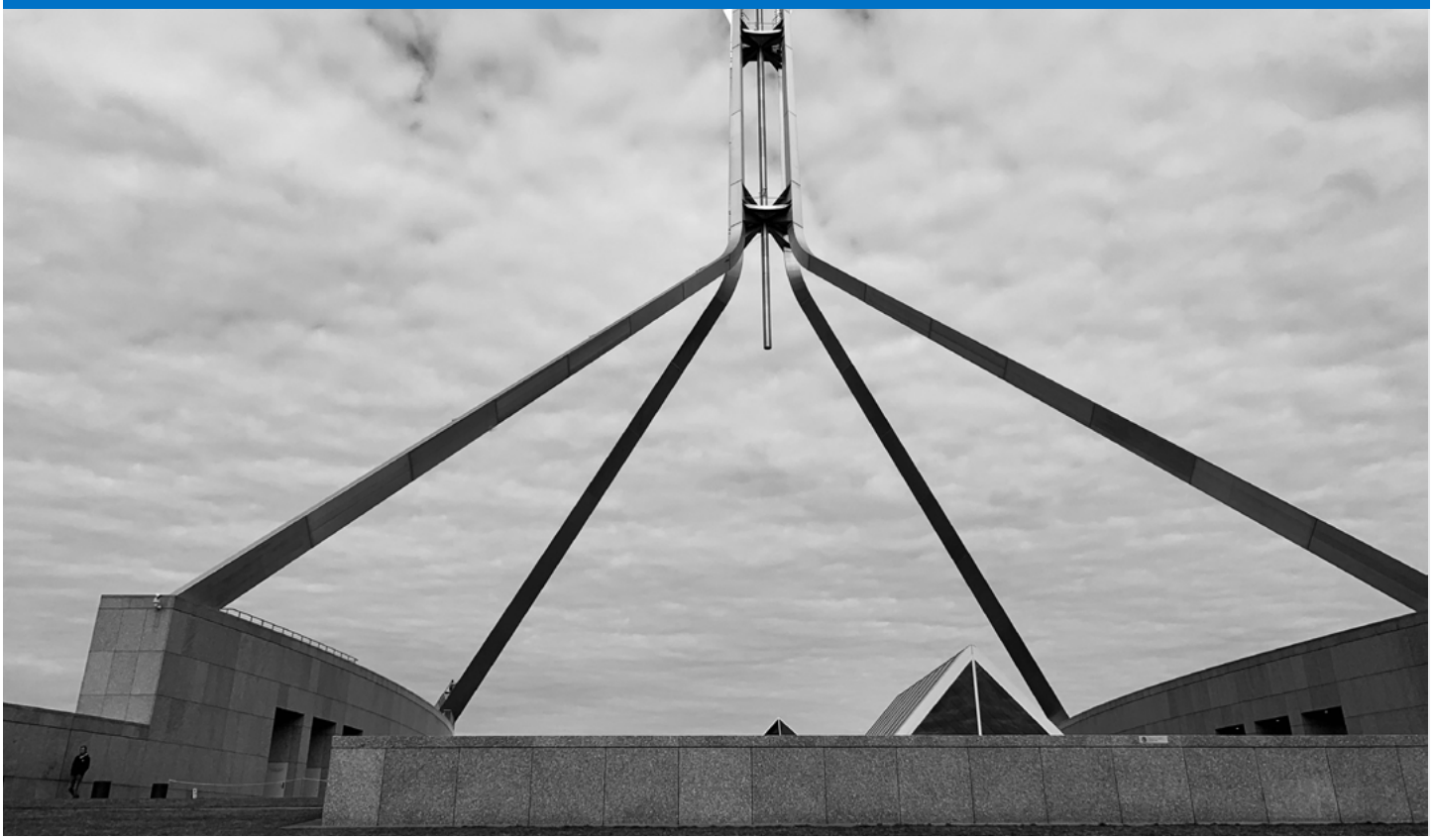
clearswift
by HelpSystems

GUIDE *(Cybersecurity)*



Controlling
Classified Information

Clearswift's adaptive data loss prevention (DLP) solutions allow organizations to implement simple and flexible controls to secure business communication channels. These controls have the specific objective of reducing data loss incidents and assist compliance with legislative requirements such as the Australian Government's Protective Security Policy Framework (PSPF).

For Australian Government agencies and commercial organizations required to comply with the Australian Signals Directorate (ASD) and Information Security Manual (ISM), Clearswift's solutions address several controls around email, data protection and enforcement of the PSPF.

One of the mandatory requirements of PSPF states 'Agencies must implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats), which match their value, importance and sensitivity.'

In October 2018, the Government updated the PSPF and gave agencies one year to adopt the new classification labelling scheme. While not a legal requirement, agencies that do not adopt the mandatory requirements and put in the appropriate data protection controls can be prevented from transacting with federal organizations.

Information Security Classification Systems

Security labelling and classification software applications from vendors such as Janusnet or Titus, provide agencies and commercial organizations with an easy-to-use and PSPF-compliant solution for marking documents and emails with their relevant classification level.

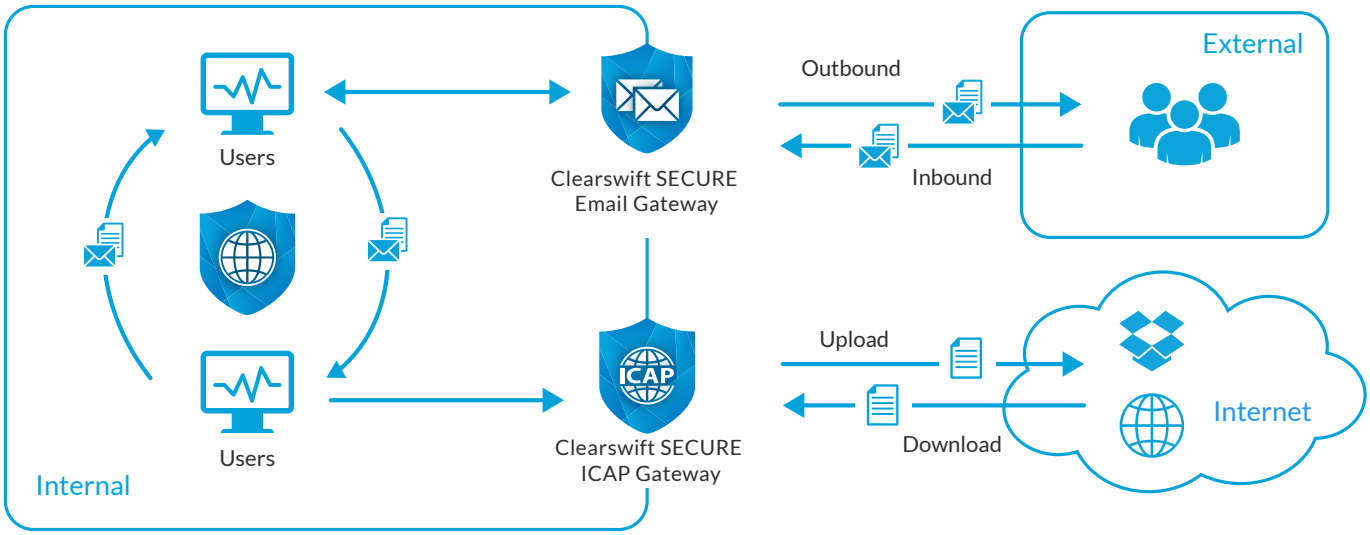
The use of security protective markings is an effective means to maintain data confidentiality and prevent data leakage. It is a method for users and systems to determine how to treat sensitive information when it is communicated internally or to third party organizations.

It is a mandatory requirement of the PSPF that agencies adopt a risk management approach to cover all areas of protective security activity across their organization. The Australian Government and Department of Defence now requires some of its supply chains to adhere to the standards of the ISM and attain membership of the Defence Industry Security Program (DISP). For some, this requires the application of protective marking controls, including the ability to block outbound or inbound emails with a protective marking higher than the sensitivity or classification than the receiving system is accredited for.

Irrespective of its obligations to adopt the PSPF, it is good security practice for organizations to implement an information classification system to reduce the risk of inadvertent or intentional data loss.

Enabling everyone engaged in information handling to categorize sensitive information in emails, documents, and other files, significantly improves information security. If Government contractors use the same classification scheme as the contracting agency, they can ensure material is controlled and marked to the same degree of diligence that the Government would apply to its own processes.

In this guide, we demonstrate how Clearswift's Secure Email Gateway and Secure ICAP Gateway work together with classification tools, from vendors such as Janusnet or Titus, to provide a combined information classification and DLP solution that is both easy to use and secure.

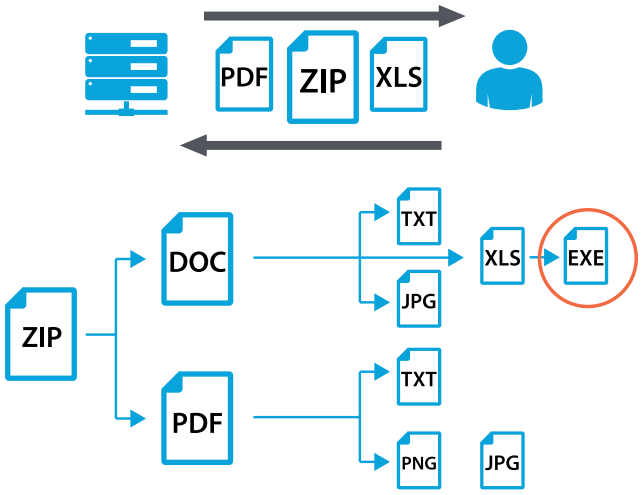


Clearswift's Adaptive DLP Solutions

Preventing information with a higher classification being transferred to a lower classified system, is a critical requirement of the PSPF and ISM.

Clearswift's Secure Email Gateway and Secure ICAP Gateway **automatically enforce policies** for classified, unmarked or inappropriately marked emails and documents covered in the ISM controls. The policies can be applied to internal and external email and uploads or downloads from the web (webmail, OneDrive, Dropbox etc).

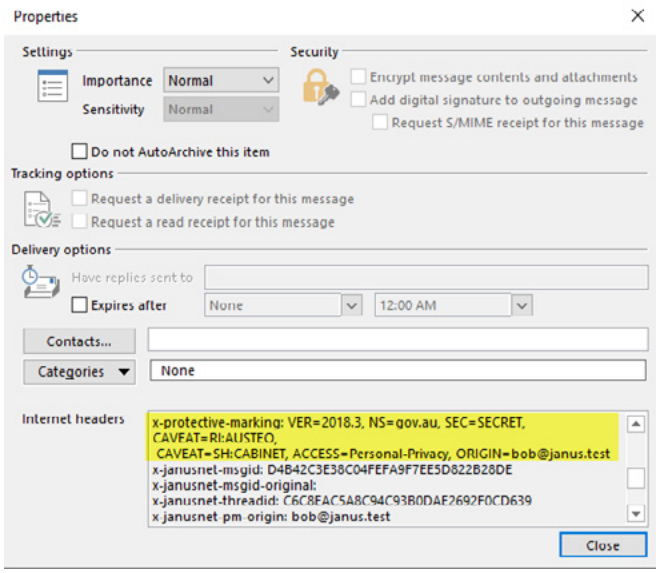
Central to all Clearswift solutions is a Deep Content Inspection (DCI) engine that inspects content and applies the appropriate security policy. In this case the DCI can check the classification markings in the body of the email or attached document. It also looks at the metadata, such as document properties and revision history.

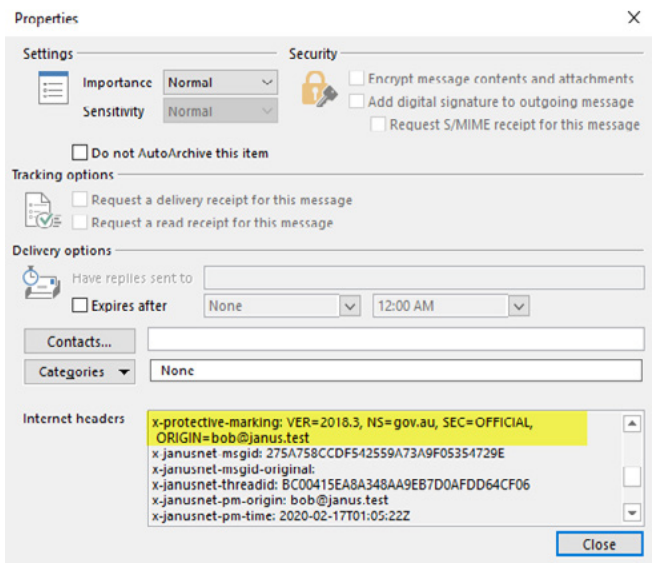


As illustrated below, compliance with the PSPF requires that x-headers (metadata tags and values) are inserted into emails. This, together with the ISM controls, ensures that information is correctly handled according to its classification.

Under the Email Protective Marking Standard (EPMS), the DCI engine looks for an OFFICIAL email (EMPS2018.3).

And similarly, with SECRET and AUSTEO.





Flexible and Granular Policy Controls

New documents, spreadsheets, or presentations are sometimes created from existing files. This creates a risk that a highly classified document is modified and reclassified at a lower level without the original information being removed from its history.

Clearswift's DCI engine inspects the hidden metadata and applies the appropriate classification policy or redacts the document history, removing the previously classified information and ensuring compliance. Other policy actions can include blocking, notifying an end user or manager or encryption.
In addition to classification-based policies, the Secure Email Gateway and Secure ICAP Gateway also apply policies based on user-specified rules such as Personal Identifiable Information (PII), and user-specified structured data such as customer numbers or intellectual property markers.

Advanced features including Optical Character Recognition (OCR) and Anti-Steganography technology allow for images and scanned documents to be inspected and sanitized, ensuring that the risk of data loss through these files types is also minimized.

" The flexibility and granularity of Clearswift's policy framework and the capabilities of the DCI engine provides additional compliance over what is possible in Office 365 and Azure Information Protection. In short, Clearswift ensures the correct classifications are correctly applied in the subject line, body, attachment and metadata of a message or file transfer."

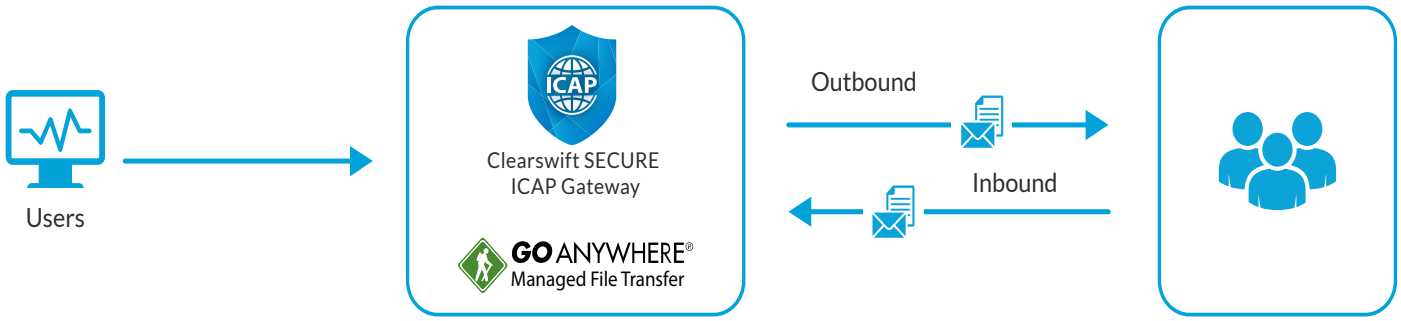
Kym Welsby, Regional Director, APAC

Additional Hygiene Features

Clearswift's Secure Email Gateway and Secure ICAP Gateway provide standard hygiene protection including anti-spam controls, anti-virus options and can identify and control certain file types, for example, executable or script files embedded within compressed file formats. Clearswift's unique Structural Sanitization feature removes active content from emails or documents, protecting against advance threats that traditional anti-virus or sandbox technologies cannot detect.

Cross Domain Secure File Transfers

Paired with our GoAnywhere Managed File Transfer (MFT) solution, Clearswift's Secure ICAP Gateway provides a layer of deep content inspection for secure file transfer cross domain solutions. GoAnywhere MFT enables the automation of file transfers with a maximum level of security, ensuring the sender is in complete control of both the file and the system the transfer is shared to and from. The files transferred are subject to policies enforced by the DCI engine, enabling the application of data classification policies.



Summary

Irrespective of compliance obligations, it is good security practice for organizations to implement and enforce information classification systems to reduce the risk of inadvertent or intentional data loss.

The combination of Clearswift and classification labelling solutions provide organizations with the ability to:

1. Provide the simple and powerful enforcement of classification policies
2. Control sensitive and classified information communicated internally, to trusted partners or leaving the organization through multiple channels
3. Ensure compliance with ISM and PSPF.

For more information, visit www.clearswift.com

" Clearswift's unique Deep Content Inspection engine looks beyond what other solutions can inspect, giving greater assurance that classified information is being treated correctly, and identifying threats concealed within complex file structures. Our clients find it provides a depth of protection for a broader range of formats that Office 365 and Azure Information Protection cannot"

Kym Welsby, Regional Director, APAC