FORTRA™

SOLUTION BRIEF (FORTRA)

Email Protective Marking Standards

Introduction

The Australian Government Email Protective Marking Standard (EPMS) is a set of requirements that organizations must follow in order to protect sensitive and classified information that is sent or received by email. The EPMS was updated on 30 January 2023, and the new requirements went into effect on 1 July 2023.

What has changed?

The new Email Protective Marking Standard introduces a number of changes from the previous standard, including:

- **New security classifications:** The new standard introduces three new security classifications: Protected, Secret, and Top Secret. These classifications replace the previous classifications of Confidential, Secret, and Top Secret.
- **New caveat requirements:** The new standard requires organizations to mark email with a caveat if the email contains information that is subject to export controls, is protected by intellectual property rights, or is otherwise subject to special handling requirements.
- **New requirements for handling, storing, and disposing of email:** The new standard includes new requirements for how organizations must handle, store, and dispose of email containing sensitive or classified information.
- **New penalties for non-compliance:** The new standard includes new penalties for organizations that fail to comply with the requirements. Organizations that fail to comply with the law may be fined up to $10 million.

What is Sensitive or Classified Information?

The EPMS defines sensitive or classified information as information that, if disclosed, could have a negative impact on the national security, economic interests, or public safety of Australia. Sensitive or classified information can include the following:

- Information about government policies or programs
- Information about military or intelligence operations
- Information about trade secrets or other confidential business information
- Information about personal or financial information

How to Mark Email

The EPMS requires all email that contains sensitive or classified information to be marked with the appropriate security classification. The security classifications are as follows:

- **Protected:** This classification is used for information that should be kept confidential.
- **Secret:** This classification is used for information that is important to the national security of Australia.
- **Top Secret:** This classification is used for information that is vital to the national security of Australia.

The email must also be marked with a caveat, if necessary, to indicate any additional special protections that are required. For example, if the email contains information that is subject to export controls, the email must be marked with a caveat that indicates this.

How to Handle, Store, and Dispose of Email

The EPMS also requires organizations to handle, store, and dispose of email containing sensitive or classified information in a secure manner. This means that the email must be stored on a secure system, transferred only through secure channels, and disposed of in a secure manner.

Organizations must also have a process in place for reviewing and approving the security classifications of email. This process should ensure that all email that contains sensitive or classified information is properly marked.

Organizations must also have a process in place for monitoring and auditing the handling, storage, and disposal of email containing sensitive or classified information. This process should ensure that the email is being handled, stored, and disposed of in accordance with the EPMS law.

When will it be implemented?

The new email protective marking standard will be implemented on 1 July 2023. This means that organizations must be compliant with the new standard by this date.

What should organizations do now?

Organizations that handle sensitive or classified information must take steps to ensure that they are compliant with the new email protective marking standard. These steps include:

- Reviewing their email policies and procedures to ensure that they are consistent with the new EPMS requirements.
- Training their employees on the new EPMS requirements.
- Implementing technical solutions to help them comply with the new requirements, such as email encryption and content filtering.

How Fortra’s Data Classification Suite can help?

Fortra has a wide range of cybersecurity solutions that can help organizations achieve the EPMS compliance. In particular, DCS can help organizations to achieve EPMS compliance by automating many of the tasks that are required to comply with the standard.

Fortra’s Data Classification Suite (DCS) can help to:

- **Identify sensitive and classified information:** DCS can help organizations to identify sensitive and classified information by automatically scanning documents, emails, and other files for keywords and patterns that are associated with sensitive or classified information.
- **Classify sensitive and classified information:** DCS can help organizations to classify sensitive and classified information by assigning the appropriate security classification to each piece of information.
- **Protect sensitive and classified information:** DCS can help organizations to protect sensitive and classified information by encrypting it using Fortra’s Vera that provides a secure collaboration capability.
- **Track the handling of sensitive and classified information:** DCS can help organizations to track the handling of sensitive and classified information by recording who has labelled the content, who accessed it and when it was accessed, and where it was sent or stored.
- DCS has created user-friendly classification tools that clearly and accurately classify emails, documents and other files with user-selected, system-suggested or automatically applied settings, based on your data security policies.
- DCS has released tailored solutions for Australian government agencies and contractors, which can assist agencies looking to comply with the new standard and ease the transition from previous versions of the standard.
- Not only does the DCS solution meet the new standards, but it is also interoperable with previous versions of the standard, allowing organisations to transition either gradually or immediately.

Conclusion

The new email protective marking standard is an important step in protecting sensitive and classified information in Australia. The new requirements will help to ensure that this information is properly marked, handled, stored, and disposed of. Organizations that fail to comply with the email protective marking standard could face significant penalties.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We’re creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We’re the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.