TOLL

Secure Digital Exchange
Powered by egress

Secure Email Document Classifier

All organisations, irrespective of their business sector or type, hold and distribute sensitive information. One of the biggest challenges any organisation faces when considering their data security strategy is to understand the types of sensitive data their employees handle and applying the correct levels of data protection.

The benefits

- Integrated MS Office Add-in for Word, Excel and PowerPoint with dynamically configurable classification labels
- Classification policies can be closely integrated into Secure Digital Exchange encryption policies to enforce and simplify the encryption process
- Fully configurable end-user experience including the ability to enforce selection of classification for any new or existing documents
- Header and footer classification information is fully customisable based on corporate requirements including text and branding
- Perform classification of email and office documents at the desktop or at the email gateway
- Assign dynamic policies based on individual users or groups, or apply organisation wide
- Maintain detailed auditing and tracking of information as it enters and leaves your organisation
- Integrate with existing DLP and content filtering tools

Contact:

Justin Cybul
National Business Development Manager

T: +61 3 9676 1250
M: +61 413 018 409
E: SDX@tollgroup.com
W: www.tollgroup.com/secure-digital-exchange

Promote data security awareness

Many organisations perform detailed analysis of all data flowing internally and outside their network boundary to try to create an appropriate risk assessment. A key part of this is training and end-user education so that all employees take responsibility for the data they hold and share. Being able to visually identify and mark data with appropriate classification can greatly improve an organisation's ability to control data flow and prevent data loss.

Integrated data classification

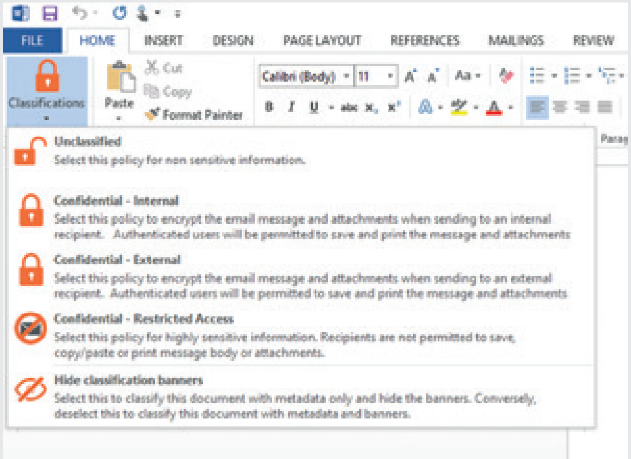
Secure Digital Exchange – powered by Egress – includes functionality that enables users and systems to add visual and system identifiers to MS Office documents, assisting with the identification and protection of sensitive content. Policies to classify MS Office content can be centrally deployed and enforced, enabling greater protection and tracking of personally identifiable information (PII) and other sensitive content. This functionality compliments Secure Digital Exchange's other capabilities for marking and securing email.

Automatically classify and encrypt data

The Secure Digital Exchange client and gateway apps can automatically detect classified content and apply policy-driven encryption appropriate to the classification. This integration simplifies end-user encryption and provides higher levels of Data Loss Prevention (DLP).

Automatic classification and encryption policies can be applied using the following criteria:

- Detection of keywords and metadata embedded within email message body and attachments including: Word (.doc, .docx), Excel (.xls, .xlsx), PowerPoint (.ppt, .pptx) and PDF
- Automatically encrypt based on content, classification and recipient addresses to enforce security between trusted entities



Unclassified
Select this policy for non sensitive information.

Confidential - Internal
Select this policy to encrypt the email message and attachments when sending to an internal recipient. Authenticated users will be permitted to save and print the message and attachments

Confidential - External
Select this policy to encrypt the email message and attachments when sending to an external recipient. Authenticated users will be permitted to save and print the message and attachments

Confidential - Restricted Access
Select this policy for highly sensitive information. Recipients are not permitted to save, copy/paste or print message body or attachments.

Hide classification banners
Select this to classify this document with metadata only and hide the banners. Conversely, deselect this to classify this document with metadata and banners.

User education and behaviour

Combined with Secure Email and Secure Managed File Transfer encryption technology, Secure Digital Exchange classification functionality can educate employees, promote security awareness and change behaviour. Users can be forced to classify content at the point of creation, when updating existing documents and when distributing it via email.

It is also possible to force compliance with information security standards such as ISO27001, and interact with users via customisable dialogs and prompts.

Visual identifiers

Secure Email and Document Classifier can apply visual identifiers (headers and footers) to Word, Excel and PowerPoint documents by default. The headers and footers are fully customisable, including content and branding to match your corporate policies and identity.

Metadata

In addition to visual identifiers the Secure Email and Document Classifier can add metadata tags and attributes to classified documents. This meta information can be used for tracking and be detected by DLP or other content inspection tools, as well as being used by the Secure Digital Exchange Gateway for message-level encryption.

Compliance

Secure Email and Document Classifier helps organisations to meet data protection and compliance regulations, as well as increasing end-user awareness and education. However, if required, these identifiers can be removed, with content still classified via the underlying metadata. Advice on how and when to classify data can be displayed to the user upon any interaction with content, including when protective marking should be applied.

About Secure Digital Exchange

Toll is already renowned as a world-class integrated logistics provider and is pleased to be enhancing its offerings in the digital space with its Secure Digital Exchange for email, documents, web forms, digital workspaces and mailrooms – for both internal and external communications in a completely secure environment.

Our new product suite is powered by Egress©, the world leader in encryption platforms, which today enables over 1,000 global organisations and is certified by the UK Government and NATO.

Taking a holistic approach to information security, the solution enables users to securely share and collaborate on sensitive data. Using patented key management, the platform utilises a unique community-based licensing model that consists of paying subscribers and designated recipients, who are able to share information securely with one another using a single global identity.

Toll is delighted to present Secure Digital Exchange – powered by Egress© – to our clients in Australia and New Zealand.

Egress© Certifications

UK Government

NATO IACD