# ICT Security Bulletin

June 2020
Vol.4

# DOCUMENT SECURITY

The average office can generate hundreds of new documents each month, but not all of them need to be safeguarded in the same way. Some documents might be public facing, such as sales brochures, while others might involve proprietary company information that should not be shared outside authorised personnel. Mishandling of sensitive information and human error often result in data breaches and if documents are not properly marked or protected, it can be hard for organisations to restrict access or how and where they are shared. Because of these possibilities in today's world, the issue of document security should be a top concern. One excellent tool within Office 365 to help you classify information automatically and enact protections based upon those classification is using sensitivity labels.

## Information Rights Management & Document Classification

Information protection is one of the three pillars of modern IT security.You can protect your corporate data using Office 365 Data Loss Prevention (DLP) and Office 365 Message Encryption. Sensitivity labels from the Microsoft Information Protection framework let you classify and protect your organization's data, while making sure that user productivity and their ability to collaborate is not hindered. When a label is applied, the content is protected based on the label applied. Access rights typically include viewing and editing privileges, i.e. some users might be allowed to view a document but not modify it. Others might have full rights, including editing privileges. Users might also have to provide passwords to access the documents. This can theoretically prevent unauthorized persons from accessing documents at an employee's workstation. Rights management safeguards your email and documents, and helps you securely share this data with your colleagues. This
is enhanced through encrypting the document or email.

| Sensitivity Label | Encryption | IRM | Expiry | Stamp |
|---|---|---|---|---|
| Internal Use Only | N/A | N/A | Optional | Footer (black) |
| Confidential | Enforced | View, Reply, Reply All, Do not forward, copy or print | Not set to expire | Diagonal (Red) |
| Highly Confidential | Enforced | View, Reply, Reply All, Do not forward, copy or print | Set to expire. Sender defines days | Diagonal (Red) |
| Private & Confidential | Enforced | View, Reply, Reply All, do not forward, copy or print | Set to expire within number of hours | Diagonal (Red) |
| Embargoed | Enforced | View, Reply, Reply All, do not forward, copy or print | Set to expire after a number of days | Diagonal (Red) |

The following gives a brief description of each sensitivity label

**Internal Use Only:** For Internal Delta Data. The data is encrypted and contains a header and footer marked: Delta Internal Use Only.
- **Confidential:** For Confidential Delta Data. The data is encrypted and contains, Watermark marked: Confidential - For Delta Internal Use Only and Footer marked: Confidential - For Delta Internal Use Only.
- **Private and Confidential:** For Strictly Private and Confidential Delta Data (Internal and External). The data is encrypted.
- **Embargoed:** For sensitive Delta Data ( Internal and External). The data is encrypted.

## Benefits of Implementing Sensitivity Labels in Office 365

After a sensitivity label is applied to an email or document, any configured protection settings for that label are enforced on the content. With a sensitivity label, you can:
- Encrypt email only or both email and documents. You can choose which users or group have permissions to perform which actions and for how long.

For example:-
- One can choose to make the document a "View Only"
- Another option "do not Forward, do not Copy, do not Print"
- Mark the content when you use Office apps, by adding watermarks, headers, or footers to email or documents that have the label applied. Watermarks can be applied to documents but not email.
- Retention Settings - A document or email can be set a life span. One can expire a document depending again on the sensitivity levels of the document. The higher the sensitivity the higher the chances of expiring the document. When a document or email is expired it automatically disappears from the recipient's computer.
- Classify content without using any protection settings - You can also simply assign a classification to content (like a sticker) that persists and roams with the content as it is used and shared. You can use this classification to generate usage reports and see activity data for your sensitive content.

## Steps to follow when applying sensitivity labels

**1.** Select New Mail / New Document
**2.** From the Home Tab, select Sensitivity on the Ribbon
**3.** Select the Sensitivity Label to apply to your email or document.

**NOTE:** If selection is for Public label, follow:
**1.** From the popup, Select Permissions to give
**2.** Then from the popup in your Outlook Mail, select Users, Groups, or Organizations to share data with.
**3.** Then select Expiration date for data access, if it has no expiration leave it blank
**4.** Save your document or send your email.

For more

information

contact your

IT Support

You can also contact IT Security

department

on:

itsecu@delta.co.zw

Or Ext 33211

33233

**Sources:** https://www.shredall.co.uk/blog/clean-desk-policy

https://www.csoonline.com/article/3335122/the-clean-desk-test.html

https://thedefenceworks.com/blog/top-5-security-awareness-topics-for-2020/

https://shrewsbury.happyfox.com/kb/article/57-march-cyber-security-newsletter-clean-desk-and-security/

*We are Delta Corporation - Brighter Together*

Delta Corporation
LIMITED

# ICT Security Bulletin

June 2020
Vol.4

# DOCUMENT SECURITY

For more information contact your IT Support

You can also contact IT Security department on: itsecu@delta.co.zw Or Ext 33211 33233

### Steps to follow when encrypting on Office 365

**1.** Select the New Email
**2.** Choose Options tab, select Encrypt and pick the encryption Do Not Forward
**3.** Finish composing your email and then choose Send

Alternatively
**1.** Select New Email
**2.** Choose Options tab, select Permissions and pick Do Not Forward
**3.** Finish composing your email and then choose Send

NOTE: Do Not Forward restriction means the recipient can read the message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies.

### Conclusion

Sensitivity labels for Delta have been customized and only apply to Office 365 users. One needs to authenticate with their email address to activate the use of the labels.

*Acknowledging Critical Data Is the First Step!*

**Sources:** https://www.shredall.co.uk/blog/clean-desk-policy
https://www.csoonline.com/article/3335122/the-clean-desk-test.html
https://thedefenceworks.com/blog/top-5-security-awareness-topics-for-2020/
https://shrewsbury.happyfox.com/kb/article/57-march-cyber-security-newsletter-clean-desk-and-security/