Secure Email Encryption

Version	1
Name of responsible (ratifying) committee	Simon Weech
Date ratified	TBC
Updated	06th February 2019
Review date	January 2020 (unless requirements change)
Electronic location	Director Documents
Related Documents	Data Protection: An Introduction

In the case of hard copies of this policy the content can only be assured to be accurate on the date of issue marked on the document.

For assurance that the most up to date policy is being used, staff should refer to the version held on the intranet

What is encryption, and how does it work in Office 365?

At a high level, encryption is the process of encoding data (referred to as plaintext) into ciphertext that cannot be used by people or computers unless and until the ciphertext is decrypted. Decryption requires an encryption key that only authorized users have. Encryption helps ensure that only authorized recipients can decrypt content, such as email messages and attachment files.

Encryption by itself does not prevent content, such as files, email messages, calendar entries, and so on, from getting into the wrong hands. Encryption is part of a larger information protection strategy for our organization. By using encryption, you can help ensure that only those who should be able to use encrypted data are able to.

You can have multiple layers of encryption in place at the same time. For example, you can encrypt email messages and also the communication channels through which your email flows. With Office 365, your data is encrypted at rest and in transit, using several strong encryption protocols, and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES).

Here's how email encryption typically works:

- A message is encrypted, or transformed from plain text into unreadable ciphertext, either on the sender's machine, or by a central server while the message is in transit.
- The message remains in ciphertext while it's in transit in order to protect it from being read in case the message is intercepted.
- Once the message is received by the recipient, the message is transformed back into readable plain text in one of two ways:
    - The recipient's machine uses a key to decrypt the message, or
    - A central server decrypts the message on behalf of the recipient, after validating the recipient's identity.

Send an encrypted message using Outlook for PC

A message that is encrypted by Office 365 Message Encryption is delivered to a recipient’s inbox just like any other email message. If the recipient has Outlook 2013 or 2016 and an Office 365 email account, they'll see an alert about the item's restricted permissions in the Reading pane. After opening the message, the recipient can view the message just like any other.

Note: Microsoft recently released the **encrypt-only** policy in Outlook for PC versions 2019 and Office 365. That means messages that have the new encrypt-only policy applied can be read directly in Outlook on the web, in Outlook for iOS and Android, and now Outlook for PC versions 2019 and Office 365. Other customers will see a message with a link. That link will take Office 365 users to Outlook on the web to read the message. Users with other email accounts will be prompted to obtain a one-time passcode and read the message in a browser window.

If the recipient is using another email client or email account, such as Gmail or Yahoo, they'll see a link that lets them either sign in to read the email message or request a one-time passcode to view the message in a web browser.

There are two primary ways to send encrypted messages.

We currently have a defined rule to automatically encrypt messages that meet certain criteria. Presently if you add the word ‘Secure’ somewhere in the subject line the system will automatically apply

If you want to encrypt a message that doesn't meet a pre-defined rule you can apply a variety of different encryption rules before you send the message. To send an encrypted message from Outlook 2013 or 2016, or Outlook 2016 for Mac, select **Options** > **Permissions**, then select the protection option you need. You can also send an encrypted message by selecting the **Protect** button in Outlook on the web.

View and reply to an encrypted message for Office 365 recipients using Outlook for PC

You can read messages encrypted with the do-not-forward policy or custom protection templates in Outlook 2013 and Outlook 2016 for PC, Outlook 2016 for Mac, Outlook on the web, Outlook for iOS, and Outlook for Android, Outlook on the web and in Outlook for iOS and Android, and Outlook for PC in the Monthly Targeted Channel. Office 365 users on Semi Annual Channel will be taken to Outlook on the web to read the message. Users with other email accounts will be prompted to obtain a one-time passcode and read the message in a browser window.

To reply to an encrypted message

1. Choose **Reply** or **Reply All**.
2. On the page that appears, type a reply and choose **Send**. An encrypted copy of your reply message is sent to you.

View and reply to an encrypted message without Office 365 using Outlook for PC

If you're not using Outlook with Office 365, your encrypted message will contain a link in the message body.

1. Select Read the message.
2. Select sign in with a one-time passcode.
3. Once you receive the passcode in an email message, make a note of the passcode, then return to the web page where you requested the passcode and enter the passcode, and select CONTINUE.

Tip: Each passcode expires after 15 minutes. If that happens, or if you can’t open the message for any reason, start over by opening the attachment again and following the steps.