Bureau of Information Technology Solutions
A Division of DAS

Workforce Enablement
Office Message Encryption (OME)

State of Connecticut Executive Branch: Office Message Encryption (OME) FAQs

i. What is Microsoft O365 Message Encryption?

Microsoft O365 Message Encryption allows State of Connecticut Executive Branch email senders to encrypt messages to any email recipient. Recipients of encrypted messages using this

service can then use their email service credentials or a pass code to read and reply to the encrypted message. Recipients with Gmail, Yahoo!, Hotmail/Outlook, and Office 365 accounts can authenticate using those credentials in lieu of a passcode. If the recipients are using Hotmail/Outlook or Office 365 and an Outlook or Outlook Online client then the message is automatically decrypted in their inbox.

ii. **Why would I need to encrypt an email**?

Although your O365 emails are encrypted while in your mailbox, the information within them is in plain text during their transit to the recipient and potentially within the recipient's mail system. To protect data that may not be public in nature (e.g., networking architecture documentation, certain

financial information, personal information, etc.), the use of encryption during transit is a viable alternative to ensure the data's security. This feature provides an additional security provision for those business needs where it is necessary or desired.

iii. What email client do I need to use in order to create an Office 365 Message Encryption encrypted message? What applications are supported for sending protected messages?

You can create protected messages from Outlook 2016, Outlook 2019, Outlook Microsoft 365 App (aka: Office 365 ProPlus) for Windows and Mac, and from Outlook on the web.

iv. How do I send an encrypted email?

To send an encrypted message from Outlook on Windows, in the new message window, within the Subject field add [Secure] before or after the subject of your email. Note: [Secure] must be in square brackets (not case sensitive). Or in the new message window, click "Options" -> "Encrypt" and then select Encrypt-Only or Do Not Forward. Please review the Sending Document Here.

v. What encryption options are available?

Encrypt-Only: The Encrypt option encrypts email to recipients, where they can then read the message, respond to it, forward the message, or download attachments unencrypted. Recipients with Gmail and Yahoo! Accounts can authenticate using those services in leu of a passcode. Recipients with O365 accounts outside of our tenant are decrypted automatically. This includes Outlook, MSN, Live, and Hotmail. Recipients with a wsu.edu email are decrypted automatically.

Do Not Forward: Encrypt and Prevent Forwarding. Your message stays encrypted within Microsoft O365 and cannot be copied or forwarded. Microsoft Office attachments such as Word, Excel, PDF, or PowerPoint files remain encrypted even after they are downloaded. Other attachments, such as image files, can be downloaded without encryption.

IMPORTANT: Messages sent internally to “ct.gov” to “ct.gov” do not run through the DLP Policy, and do not get sent encrypted. If a message is sent with [Secure] in the subject to “ct.gov” to “ct.gov”, the message will not be sent encrypted – however, if an external recipient is on the message as well, that will be sent encrypted.

vi. How do I open an encrypted email?

Outlook on a desktop or Browser: If you're using a Microsoft 365 email account in Outlook 2016/2019 or Outlook on the web, you shouldn't need to do anything special to read your message. Outlook mobile app: If you have a Microsoft 365 account and you're using the Outlook mobile app, the message should just open. If you are reading the encrypted email from another platform, please refer to the One-Time Passcode Document to review or the Single Sign-On Document (for use with Yahoo/Gmail).

If you have recipients that experience “This site can not be displayed” - please read this document.

vii. Is there a size limit for messages you can send with Office 365 Message Encryption?

Yes. The maximum message size you can send with Office 365 Message Encryption, including attachments, is 39 MB.

viii. What file types are supported as attachments in protected emails? Do attachments inherit protection policies associated with protected emails?

You can attach any file type to an email protected by Office 365 Message Encryption and that message is protected by encryption while being sent and received by the recipient, including the attachments. That protection does not extend to protecting the attachment after it is downloaded from the encrypted email, unless the attachment is of a supported file type.

The supported file types for protection outside of Office 365 Message Encryption service are applied only on the file formats mentioned in File types supported by the Azure Information Protection client. Office 365 Message Encryption does not support the 97-2003 versions of the following Office programs: Word (.doc), Excel (.xls), and PowerPoint (.ppt).

If a file format is supported, such as a Word, Excel, or PowerPoint file, the file is always protected, even after the attachment has been downloaded by the recipient. For example, say an attachment is protected by Do Not Forward. The original recipient downloads the file, creates a message to a new recipient and attaches the file. When the new recipient receives the file, the recipient will not be able to open the protected file. We has chosen to encrypt PDF documents. By default, PDF documents are not encrypted.

ix. Are OneDrive attachments supported?

Not yet. OneDrive attachments are not supported, and end-users can't encrypt a mail that contains a cloud OneDrive attachment. Send the attachment as a regular attachment and not a cloud link.

x. Am I able to print or download or forward an Encrypted Message?

Yes, we have made a few changes to allow for this now. In most instances, you can print/download/forward the message. It is possible that you may receive a message that the sender does not want forwarded, and in that case – you cannot forward/print/download the message.

xi. What type of data is being caught by DLP policy and sending out encrypted?

Currently, the DLP policy is forcing encryption if a Social Security Number, Drug Enforcement Number, or HIPPA Terms are scanned and found. We worked with the State of Connecticut Security Team to implement this policy. However, this policy can be modified – if modifications are needed we will work with the Security Team and implement off-hours.