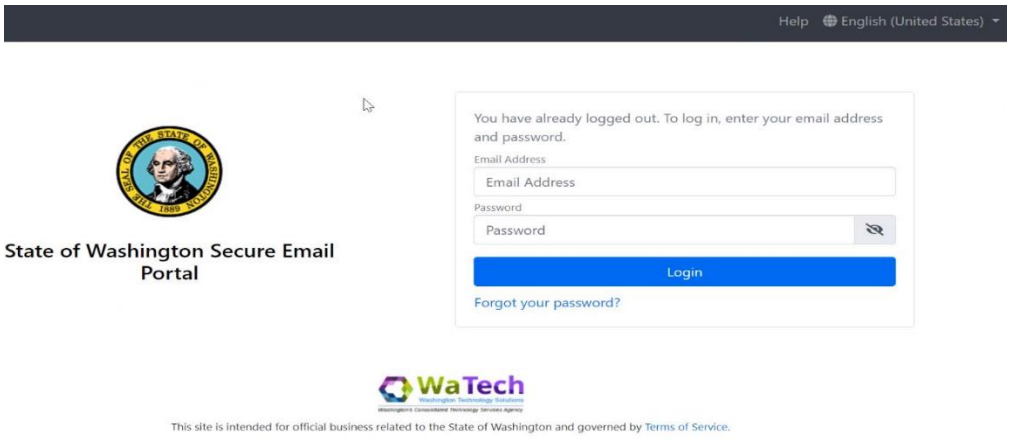
FAQ E-mail Encryption-WA State Partners

FOR PROVIDERS NOT USING OFFICE 365

Background

The State of WA will have all email moved to Exchange Online in Microsoft Office 365 by the end of 2021. As part of the contractual agreement with counties and subcontractors, transporting client records containing confidential information outside a secure area in email must be encrypted. The old email encryption service provided by WaTech in the screenshot below will be decommissioned by WaTech in Nov/Dec 2021. This solution using Trustwave and Echowrx is a third-party software as a service (SaaS) product purchased by WaTech for the State of WA and partners to interact with the state. Once all agencies in the State of Washington have been migrated to Exchange Online in the cloud, then WaTech will be decommissioning this service since the new cloud-based Microsoft email service has its own email encryption.



Questions and Answers:

1. **Our agency is not currently using office 365. Are there options available for us to continue with our current system after the state secure encrypted e-mail system ends?**
   If you are not using email encryption with Office 365 check with your IT provider to find out what email encryption you may be using or is available to you. If you are not using anything, below are some examples of email encryption providers that can be used in addition to Office 365. We are in conversations with Echowrx/Trustwave about the possibility of having DSHS contract for secure email, but there are complexities with the timeframe, contracting, support, and cost.

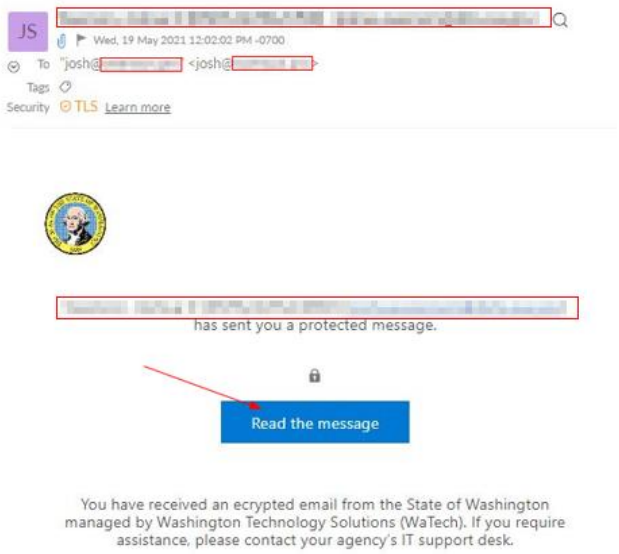
   - *Zix Secure Email https://zix.com/products/email-encryption*
   - *Barracuda Secure Email https://www.barracuda.com/landing/upgradefrommxlogic/secure-email-delivery*

2. **When looking for e-mail encryption solutions what should we be requesting?**
   The requirements of the contract specify that email encryption must be used but doesn't specify the level of encryption.
   E-mail solutions must ensure encryption of data in transit as well as encryption of data at rest. Solutions which provide "End to end" encryption of at least 256 MB provide the most secure

encryption. Solutions which encrypt "data in transit" using transport layer security (TLS); however, will satisfy the DSHS encryption requirement.

3. **We use Gmail. Is the confidential setting in Gmail sufficient to meet the DSHS encryption standards?**
   Because Gmail uses transport layer security (TLS) by default, then that should satisfy the requirements of utilizing email encryption in transit. Using the confidential setting in Gmail would just be an extra layer of security and can also be used.

4. **If receiving Office 365 encrypted e-mails from the state (or other partners such as the County) what steps may be needed to read and respond to e-mails? What can we expect?**
   If receiving an encrypted email from the state to a non-Microsoft account, you should expect to see an email like the screenshot below that has a link. After clicking to "Read the message", it will ask to send a one-time passcode that gets sent by email. Then, it will let you view the encrypted email and respond.



5. **When will the parallel WA state secure access encrypted e-mail no longer be active?**
   WaTech is our central service email provider and they are planning on bringing down the old secure email portal in December 29, 2022. DSHS is in conversation with EchoWrx/Trustwave about the possibility contracting for secure email, but there are complexities with the timeframe, contracting, support, and cost. We will provide updates as we learn more.

6. **How can I save critical e-mails which may be lost when the state secure system shuts down?**
   The old encrypted email portal saves email for 30 days before purging the email. If you need to save an email or document before the service is decommissioned, you can try saving the email to your local workstation, copying it in a word document, or printing a PDF. There are multiple methods of doing this.

7. **If the case manager has not encrypted an e-mail, what are our options to respond if the content requires encryption?**
   If you are receiving the document with [DSHS Secure] in the subject line, then you should be good and will be able to respond with TLS encryption in transit. You might need to look into whether or not your email provider uses transport layer security (TLS) by default when sending messages. If so, then it should be safe to send the email because it will be using email encryption in transit.

   If you do not have a secure e-mail service and a case manager sends you a non-encrypted e-mail, but you need to respond with confidential data, you can request that the case manager to send you a new e-mail with [Secure] in the subject line. Doing this will initiate Microsoft encryption e-mail that will encrypt all replies/forwards/CC within that e-mail chain.

8. **Can I add (cc) someone else to an encrypted e-mail chain initiated by a case manager?**
   If [Secure] is in the subject line, the e-mail is encrypted using Microsoft email encryption, which follows the email and attachments, so only the people in the To and CC fields will be able to read everything. The sender can CC someone, but you might have issues if you try forwarding the encrypted email to someone not originally on the email chain.

   E-mails initiated by a case manager with [DSHS Secure] in the subject will only guarantee TLS encryption sent from DSHS. If you CC or forward the e-mail on, it will not guarantee encryption.

9. **How long will secure emails be available to review?**
   At the moment, the encrypted emails will be held until the sender's (DSHS staff) account is disabled and unsynchronized. There is no 30-day limit like the old email system. This is a tenant-wide setting for the State of WA, but each county or partner Office 365 tenant could be configured differently.

10. **Is there a way for me to save critical e-mails that exceed the 30-day settings set by the state office 365 encryption system?**
    Yes, critical emails that are encrypted using M365 can be saved more than 30 days. The new Microsoft email encryption will allow you to access the e-mail and it's attachments until the sender's account is disabled and unsynchronized.

11. **Is using a one-time pass code the only way to read/accept encrypted messages or is there a larger scale solution that agencies could use to read/view encrypted emails?**
    Using a one-time pass code is the Microsoft method of reading an encrypted email to a non-Microsoft account. There are a few ways around this. One option is to migrate to Office 365 or sign up with a free Outlook.com account. Any encrypted email from Microsoft to Microsoft will be transparent and not require a one-time passcode. A second option would be to have the DSHS sender of the email use [DSHS Secure] in the email subject, which has been configured to remove Microsoft encryption and force TLS (transport layer security) encryption.