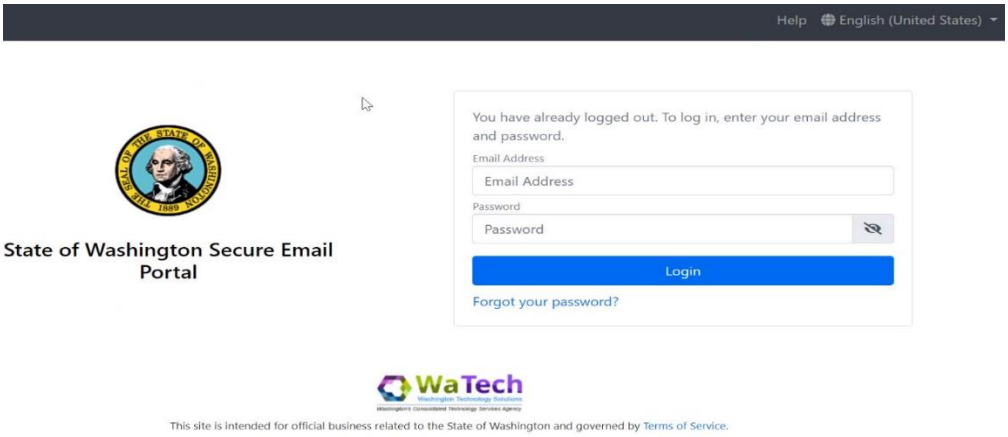
FAQ E-mail Encryption-WA State Partners

FOR PROVIDERS NOT USING OFFICE 365

Background

The State of WA will have all email moved to Exchange Online in Microsoft Office 365 by June of 2022. 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 Dec 2022. 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.



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 WaTech about the possibility of having DSHS take on the contract, 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*

- *Another option is to send the email with transport layer security (TLS). This is an alternative method of sending email encryption in transit. Companies like Google (Gmail) have this enabled by default.*

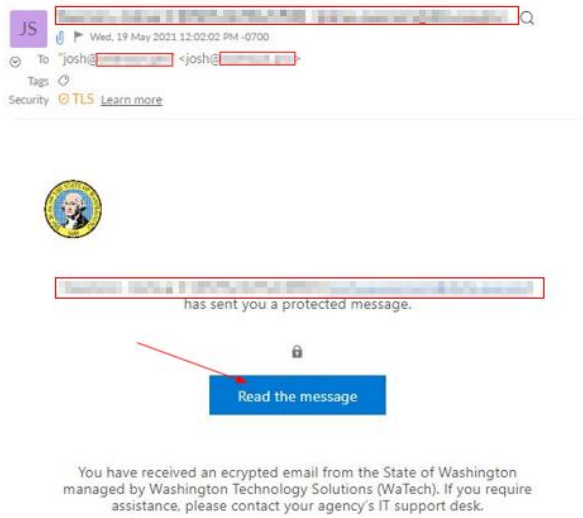
2. ***When looking for e-mail encryption solutions what should we be requesting?***

   The majority of the email encryption providers available should meet your needs and comply with the security requirements. The requirements of the contract specify that email encryption must be used but doesn't specify the level of encryption.

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. The alternative method of receiving an encrypted email using TLS will have the text [DSHS Secure] in the subject line and you can reply like a normal email without visiting a separate website.



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 Dec 2022. We are in conversations with WaTech about the possibility of having DSHS take on the contract, but there are complexities with the timeframe, contracting, support, and cost.

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?**

   DSHS staff should be defaulting to sending email with Microsoft email encryption using [secure] in the subject. If the recipient does not have Microsoft authentication, then DSHS staff should be using [DSHS Secure] in the subject line, which will remove Microsoft encryption and force transport layer security (TLS) encryption in transit. If DSHS staff or a case manager sends an email with no encryption at all and nothing is in the subject line, then I would assume the email is not encrypted, unless you are able to verify that your email provider is using TLS encryption. Companies like Google and Yahoo use this by default. You can respond to the email if you know that your email provider uses TLS or if you are able to utilize your own email encryption solution to initiate an email to send to DSHS.

8. **Can I add (cc) someone else to an encrypted e-mail chain initiated by a case manager?**

   If the message is being sent using Microsoft email encryption with [secure], then no, this is not possible by Microsoft design. Microsoft email encryption 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. The solution is to have the sender resend the message and include all the people who need to read the message. You can also initiate a new encrypted email and copy the content, but only if it does not include an attachment since email encryption with Microsoft follows attachments. An alternative method is having the DSHS staff send an email with [DSHS Secure] in the

subject line, which will remove the Microsoft email encryption and force TLS encryption in transit. In this case, the message and attachment can be forwarded as needed.

9. **How will e-mails sent by the case manager appear and how long will they be available to review?**

   At the moment, the encrypted emails will be held at Microsoft forever. 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 Office 365 can be saved more than 30 days. The new Microsoft email encryption will allow you to save them for as long as your retention policies allow.

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.