Policy & Standard Background

Name: Policy 310 – Statewide Migration to Enterprise Cloud Email Services

Purpose of Action: This policy establishes the expectation for state agencies to use the state's centrally managed, cloud-based shared email service, and to migrate data off on-premises email systems to the cloud service by 6/30/2022.

What is the business case for the policy/standard?

The on-premises hardware and software that supports legacy shared services email and archive systems will be out of support by 6/30/2022 and replacing it would be a major capital expense. WaTech has established a cloud-based shared email service that is more robust, more secure, and more cost-effective than the old on-premises system. Many agencies are in process of migrating email data to the new service, but some are lagging even though WaTech has procured the licenses needed to serve the entire shared email user community. Delaying the migration beyond 6/30/2022 creates excessive cost and greatly increases statewide risk to maintain and safeguard the obsolete on-premises email system.

What are the key objectives of the policy/standard?

1. Formalizes the long-standing statewide strategy to standardize on a single common email system and aligns that strategy with the state's direction to move to cloud services.
2. Directs agencies in the actions they must take to join the cloud-based shared email service and establishes a deadline of 7/31/2021 to give agencies and WaTech time to migrate data.
3. Reduces costs by directing agencies to use the licenses allocated to them from a single enterprise pool managed in the shared tenant. This ensures agencies do not pay for more licenses than needed, can move to the new service without delay, and that all agencies have the licenses required to properly secure the environment. It also clarifies that agencies are only required to use email and associated directory services even though licensing gives them the option to use all Microsoft 365 products and services provisioned in the shared tenant.
4. Establishes a deadline of 6/30/2022 to complete migrating email data to the new cloud email service. This is necessary to avoid excessive costs and to mitigate risks associated with maintaining obsolete hardware and software for the old on-premises shared services email.
5. Affirms that agencies are not authorized to operate separate Microsoft 365 environments without an approved waiver from the OCIO. The state's standard identity management infrastructure is Enterprise Active Directory (EAD). EAD is now linked to Azure Active Directory in a hybrid EAD/AAD federated model to manage user IDs and email services in the state's shared Microsoft 365 tenant. Only one such hybrid is technically possible, so agencies with separate tenants create an unnecessarily complex, expensive, and potentially risky environment for all state agencies.

How does policy/standard promote or support alignment with strategies?

The policy supports and promotes alignment with the state's strategies for:

- Adopting cloud solutions and migrating existing systems to cloud services.
- Adopting shared services for common business solutions.
- Reducing unnecessary operational complexities and costs.
- Modernizing IT infrastructure to promote business innovation.
- Protecting the state's IT assets by improving security and resilience of IT systems.
- Advancing efficient and accountable government.

What are the implementation considerations?

- The policy memorializes what has been statewide strategy for several years. The deadlines have been communicated by multiple methods and in multiple forums. This is not 'new news' to agencies. Putting policy in place now is critical because time is getting short to be off the legacy, on-premises email system before it becomes unsupportable.
- Some agencies may not be able to prioritize resources to meet the required timeline. They can apply for a waiver, but that means the state will incur increased risk and significant costs to keep the legacy email system operating beyond end-of-life, until all agencies are off.
- Like all cloud services, the Microsoft 365 offering is constantly evolving, and some services are more mature than others. Only email and associated directory services are mandated by this policy, but some agencies are still reluctant to join the service because other M365 products do not yet meet their needs.
- Some agencies are resistant to giving up the high level of control they enjoy with a private M365 tenant. But not moving to the state's shared tenant has complex, expensive and potentially risky implications for the rest of the enterprise.

How will we know if the policy is successful?

The policy is successful if all agencies have joined the state's enterprise M365 tenant for shared cloud email services, and the legacy email infrastructure is retired by 6/30/2022. Migration status is published regularly at the M365 Enterprise Shared Tenant Migration project page.

Policy 310 – Statewide Migration to Enterprise Cloud Email Services

Purpose

This policy establishes the expectation for state agencies to use the state's centrally managed, enterprise cloud email services, and to migrate off on-premises email by 6/30/2022. This is in support of the state's strategies for licensing and operational cost reduction, infrastructure modernization, improved security and resilience, and the advancement of efficient and accountable government.

Policy Statement

1. Agencies must use the state's cloud-based, centrally managed shared email service provisioned within the state's designated Microsoft 365 (M365) Enterprise Shared Tenant.
2. Agencies must register their email domain names and synchronize enterprise active directory (EAD) user accounts with Azure Active Directory (AAD) in the Enterprise Shared Tenant by 07/31/2021. (see 183.20.10 Identity Management User Authentication Standard, and 185.10 Enterprise Service: Enterprise Business Processes for Internal Identity Management)
3. Agencies must use the Microsoft 365 licenses assigned to them in the Enterprise Shared Tenant but are only required to use email and associated enabling directory services.
4. Agencies must complete migrating email and email archive data off on-premises systems to the M365 shared email service by 06/30/2022.
    4.1. An agency may use an alternative email archive product if the solution is compliant with all state policies and standards, works fully in an M365 shared tenant environment, and all data is migrated off the Washington State Electronic Records Vault Service (WaSERV) by 06/30/2022.
5. Agencies are not authorized to establish or operate a separate agency-owned Microsoft 365 tenant without an approved waiver.
    5.1. Any agency with an established agency-owned Microsoft 365 tenant must submit a waiver request by 7/31/2021, following the instructions in Policy 103 Technology Policy & Standard Waiver Request.

This policy does not apply to institutions of higher education.

For questions or to request a waiver, please contact the OCIO Policy and Waiver Mailbox.

SUNSET REVIEW DATE: 5/13/2024
ADOPTION DATE: 5/13/2021
APPROVAL DATE: 6/8/2021

Policy 310 – Statewide Migration to Enterprise Cloud Email Services (Agency Feedback)

POLICY SECTION	AGENCY FEEDBACK	DISPOSITION
Full Policy	**Virginia Tomlinson (CWU):** Does this apply to higher ed?	No changes. It does not apply to higher ed. See the clarifying statement at the end of the policy.
	Matt Oram (DFW): Concerned about mandating M365 when current agencies are running into technical issues and limitations, such as agencies blocking others from doing timely eDiscovery searches; unindexed items and search; potential to see data between agencies; agencies still don't agree on retention labels and point of ongoing friction; B2B administration changes made without agencies awareness; Exchange migration issues not being discussed transparently. Need to step back and look at the issues where the architecture is failing us before putting ourselves in a policy corner, especially for large agencies. Must have candid conversations about the limitations.	Microsoft continues to evolve the product, adding features and addressing customer concerns. For example, the blocking issue was recently resolved when Microsoft increased the number of simultaneous tenant-wide searches. Other concerns are addressed by modifying policy to clarify it is *limited to email*, noting that the state's current standard is delivered via M365. Note too that agencies are not required to use M365 licensed products or features to archive data – alternative products may be used at agency discretion.
	Thomas Heichelbech (DOL): DOL supports the policy. Should data security be included?	No action needed. Data security is addressed in 141.10 Securing Information Technology Assets Standards.
	Christie Fredrickson (ECY): Policy is specific to agency requirements but nothing about expectations for WaTech role in supporting the policy.	No action needed. WaTech's responsibilities are spelled out in the Terms of Service (TOS) with operational details documented in the Tenant Handbook. 185.10 Enterprise Service: Enterprise Business Process for Internal Identity Management, enumerates WaTech's responsibilities for managing identity and single sign on services, maintaining security boundaries between agencies, delegating administration duties, and

		administering the enterprise shared tenant.
	Chris Lamb (OFM): We should not define solutions in a policy but rather required goals. Requiring M365 shared tenant is a solution. Policy should require agencies reside in an enterprise shared tenant for (list benefits). Create a standard that mandates the M365 shared tenant.	Understand the position of the commenter but at this time, no change is being made. There are linkages to the product in terms of the enterprise licensing that would be difficult to separate out. We will continue to evaluate this over time.
	Chris Lamb (OFM): Concerned about strict mandates and not being able to pivot easily. Many technical issues remain in the shared tenant, mostly involving public records and privacy. This mandate could put us in legal jeopardy. We should keep our eyes on the potential need to pivot. Should build policies and standards to highest level of agility possible. Take a "slow-step" and then gradually grow as more things are finalized.	See note above on Matt Oram comments re: records and technical issues. Because of the 5-year term of the enterprise agreement, the implications of active directory, the hard deadline of 6/30/2022 to avoid substantial investment in on-premises assets, and the momentum of agencies, there doesn't seem to be a good business case to delay.
	Lara Pate (WSDOT): Is this related just to M365, not Azure?	This policy only addresses the state's shared e-mail services licensed in the shared M365 tenant. Contact WaTech to inquire about licensing optional Azure SaaS and PaaS services or if an agency's Azure IaaS tenant requires access to the state's hybrid Enterprise Active Directory / Azure Active Directory (EAD/AAD).
	Lara Pate (WSDOT): Any requirements or dependencies related to connectivity to SGN or EAD?	An agency must be part of the state's Enterprise Active Directory (EAD) to register users in the shared M365 tenant and use e-mail services. 183.20.10 Identity Management User Authentication Standards, requires agencies that are connected to the State Government Network (SGN) to join the state's EAD.

	Karen Yandle (DOC): No questions or comments.	No action needed.
	Brian Thomas (OAH): Understood. No suggestions.	No action needed.
1. State agencies must use the state's centrally managed Microsoft 365 Enterprise Shared Tenant and are not authorized to establish or operate a separate agency-owned Microsoft 365 tenant without an approved waiver.	**Christie Fredrickson (ECY):** ECY infers they are covered by their existing waiver, approved through 6/30/22.	No action needed. The referenced Ecology waiver is narrow in scope and is not affected by this policy.
1.1 Any agency with an established agency-owned Microsoft 365 tenant must submit a waiver request by 12/31/2021, following the instructions in Policy 103 Technology Policy & Standard Waiver Request.	**Christie Fredrickson (ECY):** Is there a driver for the 2021 date vs. 12/31/2022?	Date for waivers is changed to 7/31/21 to coincide with Section 2 date to register domains and accounts in the shared tenant.
2. Agencies must register their domain names and synchronize user accounts in the Enterprise Shared Tenant by 06/30/2021.	**Lara Pate (WSDOT):** Is the date correct? Seems like registering in the tenant would come after the waiver deadline not a year prior.	Date is changed to 7/31/21. Note date also changed in 1.1 so that waiver date and account registration date are the same and give an additional 30 days.
3. Agencies must use the Microsoft 365 licenses assigned to them in the Enterprise Shared Tenant.	No comments on section 3.	No action needed.
4. Agencies must use email services provided to them in the Enterprise Shared Tenant. 4.1. Agencies must migrate email and archive data to the Enterprise Shared Tenant by 06/30/2022. 4.2. An agency may use an alternative archive product if necessary, to meet unique business	No comments on section 4.	No action needed.

requirements as long as the solution is compliant with all state policies and standards, the solution works fully in a shared tenant environment, and all data is migrated off of the Washington State Electronic Records Vault Service (WaSERV) by 06/30/2022.		
5. Agencies must use the security services provided to them in the Enterprise Shared Tenant as the primary means to secure state data.		Policy Statements 5, 5.1 and 5.2 will be removed and addressed in a future security policy. It should be noted that the state's shared identity infrastructure is an Enterprise Active Directory/Azure Active Directory (EAD/AAD) hybrid, so all identity and security policies and standards apply to the shared tenant. This includes 183.20.10 Identity Management User Authentication Standards, 185.10 Enterprise Service: Enterprise Business Processes for Internal Identity Management, and 141.10 Securing Information Technology Assets Standards.
5.1. Required security services in the Enterprise Shared Tenant include, but are not limited to: 5.1.1.Identity management; 5.1.2.Access management; 5.1.3.Cloud application security; 5.1.4.Endpoint protection.	**Christie Fredrickson (ECY):** Will the G5 license cover these costs? There are currently security tools in the shared tenant that are not available to agencies. Does this mean they will be made available?	Microsoft 365 G5 licenses include the Microsoft security tools used in the shared tenant. Questions regarding status and availability of new service features should be addressed to the WaTech service owner and the tenant governance committee.
5.2. Agencies wishing to supplement the required security services with additional products or services must request and receive written	**Vel Rajagopal (COMM):** Recommend adoption but have concerns because MS Endpoint Protection is not good enough. COMM uses both MS and ESET. Perhaps with business case OCS could approve for 3 years without revisit. Understand setting MS as the minimum,	See statement for Section 5.

approval from the State Office of Cybersecurity.	but hope OCS approves exceptions to supplement MS tools because they are not good enough.	
	Phil Davis (DFI): DFI supports policy. Expect agencies invested in 3rd party security products will challenge section 5.2	See statement for Section 5.
	Christie Fredrickson (ECY): What is the reason for this requirement?	See statement for Section 5.
This policy does not apply to institutions of higher education.		No action needed.