WaTech
Washington Technology Solutions

TERMS OF SERVICE FOR
ENTERPRISE SHARED TENANT

(Updated:12/15/2022)

This Service is subject to and governed by the Customer's separately signed Master Services Agreement (MSA) or Customer Service Agreement (CSA) as applicable with Consolidated Technology Services (CTS), calling itself Washington Technology Solutions or "WaTech" for short. The reference to WaTech means the same as Consolidated Technology Services. This Agreement is entered between you and CTS for the provision of the Washington Enterprise Shared Tenant. For the purposes of this agreement "You", "Your" and "Customer" are used interchangeably and mean the entity to which WaTech is providing service.

A. Service description

A tenant is a cloud computing architecture that allows multiple customers to share computing resources in the cloud. The Enterprise Shared Tenant is the Microsoft provided Office 365 software as a service (SaaS) managed (global tenant administration) by WaTech on behalf of state agencies.

A directory is the Azure Active Directory service. Each directory has one or more domains. A directory can have many subscriptions associated with it, but only one tenant.

A domain or accepted domain is a Domain Name Server (DNS) zone for which a tenant has proven ownership (by creating an arbitrarily named DNS record as requested by Microsoft). It represents the possible domain suffixes (or namespace) which directory objects can use.

1. Included features and functions from Microsoft in the Government Community Cloud Office 365 SaaS include the following (this is not an exhaustive list of the MS O365 SaaS functionality) –

- **Email** –Exchange Online provides customers with access to email, calendars, contacts and tasks for many endpoint devices. Users connect to Exchange Online via the Microsoft Outlook desktop client or Outlook with a web browser.
- **Exchange Online Archive** – **Exchange Online Archiving** offers users advanced archiving capabilities with the **archive** mailbox feature. An **archive** mailbox is a specialized mailbox that appears alongside the users' primary mailbox folders in Outlook or Outlook Web App.
- **Exchange Online Protection (EOP)** – Provides advanced security and reliability for protecting information. EOP eliminates threats before they reach the corporate firewall with multi-layered, real-time, anti-spam and multi-engine, anti-malware protection. It protects the state's IP reputation by using separate outbound delivery pools for email.

- **Exchange Message Encryption** – An online service built on Microsoft Azure Rights Management (Azure RMS) which is part of Azure Information Protection (AIP). This includes encryption, identity and authorization policies to help secure email. Encrypt messages by using rights management templates, the Do Not Forward option and the encrypt-only option. Provides encryption of email messages between people in the Tenant and outside the Tenant.
- **Mobile Email Access** – Access email anywhere, anytime via a mobile device.
- **Teams** – Connects people on their PC or mobile devices as part of their everyday productivity experience. Teams provides presence, instant messaging, collaboration, conferencing, voice, and video.
- **Teams Telephony** – The Microsoft phone system in Teams is an available option. Microsoft Conferencing includes Audio Conferencing and a local access number. There is also Toll-Free Audio-Conferencing access option. Additional details about this service are available on the WaTech website.
- **SharePoint** – Create sites to share documents and information with colleagues, partners, and customers.
- **OneDrive** – File hosting and synchronization for users use.
- **Power BI Pro** – Enable business analytics from hundreds of data sources and visualize data with live dashboards and reports.
- **Dynamics 365** – Enterprise resource planning (ERP) and customer relationship management (CRM) tools.
- **Power Apps** – Quickly build and share low code apps.

2. Prerequisites to receive the Washington Enterprise Shared Tenant service from WaTech:

- Membership in the Enterprise Active Directory (EAD).
- Register Customer's name and secondary names in the Enterprise Shared Tenant.
- Register Customer's name in the Exchange hybrid connector.
- Synchronize user IDs in the Enterprise Shared Tenant.
- Purchase or receive from WaTech, appropriate Microsoft Office 365 licenses based on Customer's business requirements.
- Register licenses in the Enterprise Shared Tenant.
- Recommend purchasing Microsoft Premier Support.
- Accept WaTech Terms of Service (TOS).

3. Recommended services in support of Office 365:

- Microsoft Identity Manager (MIM) - Helps agencies manage users, credentials, policies and access within your organization. With MIM, an organization can simplify

identity lifecycle management with automated workflows, business rules and easy integration with heterogeneous platforms across the datacenter. MIM enables the organization to have the right users and access rights for Active Directory for on-premises apps, and Azure AD Connect can then make available in Azure AD for Office 365 and cloud-hosted apps.

Common MIM scenarios include:

- Automatic identity and group provisioning based on business policy and workflow-driven provisioning.
- Integration of the contents of directories with HR systems and other sources of authority.
- Synchronizing identities between directories, databases and on-premises applications through common APIs and protocols, Microsoft-delivered connectors and partner-delivered connectors.

- MIM requires the correct Enterprise Mobility Security (EMS) E3 or E5 license from Microsoft.
- Intune Mobile Device Management (MDM) – Microsoft Intune is a cloud-based service in the enterprise mobility management (EMM) space that helps enable your workforce to be productive while keeping your corporate data protected. Similar to other Azure services, Microsoft Intune is available in the Azure portal and can:
  - Manage the mobile devices and PCs your workforce uses to access company data.
  - Manage the mobile apps your workforce uses.
  - Protect your company information by helping to control the way your workforce accesses and shares it.
  - Ensure devices and apps are compliant with company security requirements.
- Modern Public Folders – Public Folders in the on-premises Exchange 2010 environment have been migrated to Office 365 Modern Public Folders. eDiscovery searches for Modern Public Folders will be provided by WaTech.

B. Availability/Accessibility

The Enterprise Shared Tenant is the Microsoft O365 software as a service (SaaS) running in the Microsoft Government Community Cloud, managed (global tenant administration) by WaTech on behalf of state agencies. WaTech works with Microsoft to sustain the Tenant service availability 24-hours, 7-days-a-week, 365-days-a-year (24x7x365). Microsoft publishes uptime data for M365 since 2017 in quarterly increments. These uptimes range from 99.97% to 99.99% per quarter.

1. WaTech will coordinate emergency maintenance activities (global tenant administration) with customers as soon as practicable (typically within 30 minutes) once a need for emergency maintenance is recognized.

2. This is a Microsoft provided SaaS and as such WaTech shall not be liable for any damages resulting from any service interruptions, downtimes, or any other factor beyond WaTech's control.
3. Planned maintenance events: Planned maintenance is regular Microsoft-initiated service updates to the infrastructure and software applications. Planned maintenance notifications inform customers about service work that might affect the functionality of a Microsoft service. Per Microsoft, customers are notified no later than five days in advance of all planned maintenance through Message Center on the Microsoft 365 admin center. Microsoft typically plans maintenance for times when service usage is historically at its lowest based on regional time zones. Customers determine and control which of their staff have access to Microsoft's Message Center to see these alerts.
4. Unplanned downtime: Unplanned service incidents occur when one of the services is unavailable or unresponsive due to a failure within the Microsoft managed environment. Customers are notified of known service incidents through Service health located on the Microsoft 365 admin center. Microsoft posts anticipated "next update" timelines and these are outside the control of WaTech. Customers determine and control which of their staff have access to Microsoft's admin center to see these incidents. Additionally, WaTech actively monitors the Microsoft Service Health Dashboard on the Microsoft 365 admin center and will send out service notifications on highly used services based on this information.

Additionally, when connected to the State Government Network, this service leverages several underlying WaTech services such Managed Firewall, Network Core, Transport and Connectivity and as such is subject to the specific terms and conditions of these services as provided in the links below:

- Managed Firewall
- Network Core
- WaTech's Transport

In addition to the above-mentioned underlying WaTech services, Office 365 relies on the internet as the transport mechanism from WaTech's network to Office 365. As such, WaTech cannot provide service level guarantees as service performance depends on other factors such as customer equipment, how the internet is performing and Microsoft's efforts to maintain the performance and integrity of its service. You may occasionally experience delays in utilizing Office 365.

5. **Change management**

   All changes performed by WaTech are managed to promote or provide stability and minimize the impact to its customers. All changes to the service are implemented in accordance with the WaTech Change Management Process Guide. Customers can view the Change Notifications Calendar and also subscribe to service notifications.

6. **Incident management**

WaTech follows the Information Technology Service Library (ITIL) best practices including but not limited to Incident Management.

The WaTech Support Center has multiple telephone lines to respond to customer calls. If all lines are busy, the incoming calls are sequenced and answered in order. If technicians are away from the phone, the caller may choose to leave a voicemail message. A technician will automatically be paged and will return the call. The Customer will receive a trouble ticket log number when an incident is reported.

Please also see our contact us page for more information and contact options.

7. **Security management**

   WaTech provides a security system infrastructure that reasonably protects WaTech and its Customers from unauthorized external access to or broadcast on the internet of Customer's intellectual property, proprietary and confidential data. WaTech shall ensure the security infrastructure is configured and maintained in compliance with OCIO IT Security Policy and Standards as well as the WaTech Information Technology Service Management Operations Manual Standards and Procedures.

   WaTech will configure and maintain WaTech resources to protect against commonly known attack vectors in accordance with OCIO policy standard 141.10 and industry standards, guidelines and best practices.

8. **Reporting service outages and incidents**

   In the event of an outage, WaTech will notify Customer via an alert email message as well as post an alert on our System Status webpage. The Customer may report any known outages to the WaTech Support Center. Note: WaTech is not responsible or able to monitor outages within the Customer's environment.

C. Charges

The Tenant service rate is found on the WaTech website:

watech.wa.gov/solutions/it-services/Enterprise-Shared-Tenant.

D. Responsibilities

- **WaTech responsibilities:**
  1. WaTech shall furnish the necessary personnel, equipment, material and/or services to maintain the performance of this service.
  2. Management and configuration access to WaTech infrastructure is only granted to authorized WaTech personnel and contractors.
  3. WaTech will coordinate service governance via the Enterprise Active Directory Steering Committee (EAD). Topics that need to escalate beyond this group shall leverage the Technology Management Council and/or the Business Management Council.

4. WaTech will be the “Customer of Record” for the Enterprise Shared Tenant Contracts and will be responsible for coordination and management of contracted service providers.
5. WaTech will comply with state of Washington OCIO IT Security Policy and Standards.
6. WaTech will secure the service against known security risks. Any observed security breaches or suspicious activity will be reported to the Customer.
7. WaTech shall ensure the WaTech controlled portions of the environment comply with the specific security control frameworks communicated to WaTech pursuant to Customer Responsibilities subsection 15 below.
8. WaTech will report any suspected security vulnerabilities to Customer if it impacts their data or customer use of the environment.
9. WaTech will assist Customers with any required third-party audits.

- **Customer responsibilities**

1. Customers will adhere to security best practices for the applicable industry and comply with the most-current version of the Office of the Chief Information Officer (OCIO) Standard 141.10, Securing Information Technology Assets.
2. Customer agrees to complete and have an approved Network and Security Design Review(s) on file with the Office of Cybersecurity (OCS) before Customer applications and other applicable resources to include third-party hardware, software and services are integrated with (and connected to) the Tenant service.
3. Customer agrees to comply with WaTech policies, standards and best practices for developing and integrating applications and other applicable resources including third-party hardware, software and services with the Tenant service at all times.
4. Customer agrees that customer shall utilize the Enterprise Shared Tenant service to engage only its authorized servers, cloud services and networks. Any attempt to utilize the Enterprise Shared Tenant service to access unauthorized servers, cloud services and networks is strictly prohibited and may result in the termination of service(s).
5. Customer agrees that applications and other applicable resources to include third-party hardware, software and services will be configured and maintained in a manner that is compliant with regulatory and industry standards, guidelines and best practices before, during and after integration with the Tenant service.
6. Customer agrees to review any changes to applications and other applicable resources to include third-party hardware, software and services that are integrated with and could affect the Tenant service prior to making such changes. If recommended, customer agrees to complete and have approved Network and Security Design Review(s) on file with the Office of Cybersecurity (OCS) prior to making such changes.

7. Customer will be liable for charges, infractions or legal actions resulting in their failure to adhere to third party Terms of Service.
8. Customer will provide technical resources for troubleshooting assistance as needed to expedite service recovery.
9. Customer will provide contact information for use by the WaTech Support Team.
10. Customers will review their contact information at least annually and make appropriate updates.
11. Customer will designate at least one primary and one alternate technical resource (the "Customer Technical Contact") authorized to execute the following responsibilities:
    - Customer Technical Contact(s) will have the training and expertise required to support the customer's solution.
    - Customer Technical Contact(s) will submit requests to set up, change or remove a solution for their agency by submitting a request to the WaTech Support Team.
    - Customer Technical Contact(s) will be the "central Point of Contact" for questions and concerns relating to the customer's solution.
    - Customer Technical Contact(s) will report service problems, disruptions and concerns to the WaTech Support Center.
    - Customer Technical Contact(s) will work in collaboration with WaTech to setup, install, configure and maintain the Customer's solution.
12. Customer will configure and maintain appropriate local policy settings and security controls for the level of data transmitted, stored and accessed in accordance with the Customer's needs, such as defined internet use policy, as well as regulatory and industry standards, guidelines and best practices
13. Customers are responsible for working with their cloud service provider to determine appropriate firewall rulesets when accessing this service from the Customer's networks.
14. Customer will configure and maintain Customer resources to protect against commonly known attack vectors in accordance with regulatory and industry standards, guidelines and best practices.
15. Customers are responsible to identify and communicate requirements for compliance with specific security control frameworks associated with Category 4 data types (such as but not limited to HIPAA, PCI, IRS Publication 1075, CJIS). Charges may apply for implementation of additional controls where required.
16. Customer is accountable and responsible for proper licensing, contracts and records/data management for any third-party vendor provided service(s) that customers acquire that are connected to the Shared Tenant service.

17. Customers shall participate in WaTech governance meetings in order to provide timely feedback regarding maintenance and configuration changes being considered. Customer agrees and accepts that lack of participation may result in customer's concerns not being addressed.

E. Prohibited uses

Customer shall not use the Enterprise Shared Tenant to:

- Store any content that is obscene, pornographic, libelous, invasive of privacy rights, and advocates violence, bigotry, or bias based on race, color, religion, ancestry, national origin, gender orientation, or physical or mental disability, unless part of an investigation.
- Store any data to which customer does not have prior authorization to access.
- Alter, tamper or otherwise modify the service, software and/or equipment used to provide the service.
- Interfere with or disrupt the service(s), or the servers or networks connected to the service(s), or disobey any requirements, procedures, policies or regulations of the networks' connection to the service, including without limitation, engaging in unauthorized computer or network trespass, obstructing or bypassing computer identification procedures or scanning or probing another computer.
- Damage, disable, overburden or impair any services or any network connected to the services or interfere with any other party's use and enjoyment of the services.
- Gain unauthorized access to any services, other accounts, computer systems or networks connected to any services through hacking, password mining or any other means.
- Provide, or attempt to provide, access or use of the service, servers or system to any entity or third party not previously disclosed by customer and authorized in writing by WaTech.
- Obtain or attempt to obtain any materials or information through any means not intentionally made available by WaTech through the service.
- Access or attempt to access the Tenant after termination or expiration of this agreement.
- Use the service for means other than performing a purpose reasonably related to customer's business.
- Upload, post, email, otherwise transmit, or post links to any material that contains software viruses, worms, Trojan horses, time bombs, trap doors or any other computer code, files or programs or repetitive requests for information designed to interrupt, destroy or limit the functionality of any customer computer software or hardware, telecommunications equipment, or customer data or to diminish the quality of, interfere with the performance of or impair the functionality of the service.

F. Security

1. Customer agrees to engage the Office of Cybersecurity (OCS) to perform a security design review as required by OCIO IT Security Standards 141.10 of the customer or customer provided third-party architecture, including but not limited to any and all changes to the architecture that could compromise the security of the Customer or WaTech's systems.
2. Customer further agrees to assume full responsibility for the on-going secure and compliant operation for their portion of the environment as required by OCIO 141.10. This includes restricting access to state assets by policy, rules, filters and/or other reasonable methods including agreements with contractors or other third parties. The filtering shall be documented showing the real customer address(es), the address(es) of the state server(s), and the services (telnet, FTP, WWW, etc.) allowed. In so doing, customers agree to comply with all applicable Washington State IT Security Policy and Standards and shall ensure that each contractor or third-party vendor complies with all applicable security policies and standards.
3. Customer shall ensure that remote clients and servers are secured to the highest minimum level appropriate for the sensitivity of the data being transferred, manipulated or accessed.
4. Customer acknowledges that WaTech is obligated to report any suspected security vulnerabilities to the Washington State Auditor's Office (SAO). Customer acknowledges that the SAO may audit without any advance notice.
5. Customer acknowledges and accepts WaTech's right to suspend service without prior notice upon detection, confirmation or notification of any unauthorized access, malicious traffic caused by infection or abuse deemed harmful to the State Government Network. If unauthorized access, malicious traffic caused by infection or abuse occurs, WaTech and customer will attempt to resolve security issues to the satisfaction of WaTech and customer. If no satisfactory resolution of security issues is identified, WaTech reserves the right to terminate service to customer.
6. WaTech provides a security system infrastructure that reasonably protects its customers from unauthorized external access to or broadcast on the internet of the customer's intellectual property, proprietary and confidential data. In the event that WaTech becomes aware of a breach of the security of the system involving customer information maintained but not owned by WaTech, WaTech shall immediately notify the Customer that owns the information. Breach of the security of the system means unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of information maintained by the Customer.

G. Support

1. Customer Helpdesk

Customers are responsible to provide Tier I support to its users. This includes support for first contact with users who are experiencing an issue. Customer-provided support

will include workstation/client PC support. At a minimum, the following is a summary of the Tier 1 support and troubleshooting activities that the Customer will perform:

- Creating and deleting User ID.
- Profile setup on workstations.
- Distribution Lists: Setup, additions, deletions.
- User support including OWA and mobile devices.
- Troubleshooting/problems with client installation or profile, and mobile devices.
- Network connectivity including connectivity to the Shared Tenant Environment and VPN access.
- Email issues including receiving, sending, and lost or deleted email.
- Assisting users with junk mail and quarantine.
- Performance/slowness issues.
- Offline Storage Table (OST) file issues.

2. Customer Responsibilities

The Customer is responsible for the following support activities:

- Management, processing and response to litigation and public disclosure requests, legal holds, and search of Customer records stored in the Shared Tenant environment.
- Product training pertaining to use of products and services in the Shared Tenant environment.
- Ensure that email traffic directed to the WA App Relay is appropriately verified and formatted, to ensure that it does not cause an impact to the Shared Tenant environment.
- Analyzing and correcting any issues with email directed to WA App Relay. This may include taking appropriate measures to throttle the flow of messages from the device or application to the WA App Relay.
- In the event of an unintended and uncontrolled message flood caused by infection or compromise of a workstation or server, it is the Customer's responsibility to immediately remove the device from the network, change the Active Directory credentials for the compromised account, and re-image or otherwise make certain the workstation or server has been completely cleared of infection.

3. WaTech Support Center

Should the Customer be unable to resolve the problem after completing Tier I trouble shooting activities, the Customer Helpdesk will escalate the matter to either the WaTech Support Center **or** Microsoft, depending on the issue.

For Service-related issues within the Shared Tenant, Customers shall open tickets with Microsoft via portal.office.com Example of service-related issues: Users can't access Microsoft Teams, Unable to access Exchange Online. Agencies are encouraged to check the M365 Service Health dashboard via the M365 Admin Center.

Customers who have a Microsoft Unified Support contract can open Sev A through Sev C cases directly with Microsoft for service-related issues within the Shared Tenant via the M365 Admin Center at portal.office.com.

For configuration related issues or requests for change to the Shared Tenant, Customers should open tickets with WaTech Support Center via support@watech.wa.gov or by calling **1-855-WaTech1 (1.855.928.3241).** Examples of configuration related issues: emails going to Quarantine, permissions to services, licensing issues, Intune scope issues.

WaTech Support Center, available 24x7 via our phone (email is not monitored 24x7), is the single point of contact for WaTech related customer requests, problem reporting, escalation, and notification. Regardless of severity or impact, all incidents that fall outside of normal operating parameters will be reported and handled according to established procedures.

Contact the Support Center if an escalation is needed or to check the status on incidents and requests. Support Center staff will contact the technician working the request to have them contact you. We also follow up with an email to the technician and manager. Tier 2 & 3 resources are on call 24x7x365 via the WaTech Support Center phone numbers/phone tree 360-586-1000 or 855-Watech1 (855-928-3241). A visual detailed map of the phone tree is available on our website.

H. Termination

Termination of services under this TOS by WaTech shall be communicated in writing, no less than eighteen (18) months prior to provide the Customer with adequate lead-time to migrate to an alternative service without loss of service to the Customer.

1. WaTech Contacts

WaTech Support Center has multiple options to respond to customers inquiries.