Office 365
Dedicated and ITAR-support Plans

ITAR-support Service Description

FedRAMP and ITAR Solutions for Enterprises

Applies to: *Office 365 ITAR-support Plan – Legacy 2013 Platform Release*

Topic Last Modified: *12-Oct-2015*

The Office 365 suite provides online services for enterprise messaging, the collaborative sharing, management, discovery, and presentation of content, and communications features involving instant messaging (IM), presence, conferencing, and telephony solutions. Microsoft offers several versions of the suite to meet the operational requirements of a diverse base of customers. The generally available Office 365 offerings are provided to a customer (or tenant) from within a virtualized operating environment on multi-tenant hardware. The Office 365 Dedicated offerings are premium enterprise cloud services provided to a single tenant on dedicated hardware.

The ITAR-support plan service offerings build upon the Office 365 Dedicated base by providing enhanced levels of security, privacy, and regulatory compliance. The offering is designed to meet the requirements of the following customer types:

- U.S. federal government agencies requiring certification of cloud services in accordance with the Federal Risk and Authorization Management Program (FedRAMP)
- U.S. Dept. of Defense agencies requiring certification of cloud services in accordance with DoD Cloud Computing Security Requirements Guide (SRG) for information of Impact Level 5 (L5)
- Commercial entities subject to International Traffic in Arms Regulations (ITAR)

The current version of the ITAR-support plan offering includes core services that provide Exchange Online, SharePoint Online, and Lync Online. Optional shared services provided only to ITAR-support plan customers (e.g., Secure Token Service to support federated authentication) in addition to shared services accessible via Internet connectivity (e.g., Exchange 2013 Availability Service) also are available.

Comprehensive descriptions of the features and functionality of the ITAR-support services are represented within the service description set for Office 365 Dedicated. A link to each service description and supplemental information related to each description are provided within ITAR-Support Plan Feature Differences. The balance of this document describes the following:

- Enhanced security features and functionality specific to the ITAR-support service offerings
- Expanded descriptions of the underlying data protection and connectivity protection aspects of Office 365 services
- Any implementation differences within the ITAR-support offering when compared to the Dedicated offering
- Federal regulatory compliance and support

Enhanced Security Features

The ITAR-support plan services utilize the data protection features and functionality of Office 365. Layered onto the platform are the private networking model of Office 365 Dedicated, the physical security controls to segregate each customer environment, and additional system resources that are provided only to ITAR-support plan customers.

Data Protection

The enhanced data protection features available within the Office 365 ITAR-support plan offering are described in this section. Included are descriptions of service-level and customer-controlled encryption.

Note that *customer data*, as defined in the enrollment agreement for Office 365 services, refers to all data that the customer places in the Office 365 service including both data created directly by users of the service and user-identifiable information generated through use of the service. *Customer content* refers to a specific subset of customer data, as defined in the Office 365 Asset Classification standard, and includes any content that has been directly created by users such as email body text and attachments, content uploaded to SharePoint Online, or IM and voice conversations.

Isolation of Customer Data

***Applies to**: Exchange Online, SharePoint Online, Lync Online*

Environment Isolation

The Office 365 data center environments for ITAR-support plan customers are segregated from the environments provided to Office 365 Dedicated plan customers and other Microsoft commercial online services. The isolation is achieved through a series of physical, logical, and network level controls which include the following:

- Securing of physical barriers using biometric devices and cameras
- Segregated data networking including a dedicated demarcation point
- Use of specific credentials and multi-factor authentication by Microsoft personnel requiring logical access to the production environment
- Hosting of all service infrastructure in Microsoft data centers located only within the United States

Per-Customer Isolation

Every ITAR-support plan customer receives their own set of dedicated server hardware for customer content storage. All customer-owned content processed by Office 365 services is stored on the dedicated hardware. Isolated customer access to the content is provided through the use of dedicated virtual local area networks (VLANs), network access controls, and a trust model that restricts user context to their isolated environment.

Note:

The default isolation model for customer data in an ITAR-support plan environment is the following:

- Blocked routing of mail messages to the Exchange Online Protection (EOP) shared service
- Blocked outbound initiated Internet access to Microsoft shared services (e.g., Office Online, Azure Rights Management, Azure Binary Large Object (BLOB) storage, and the Microsoft Federation Gateway used to support the Exchange 2013 Availability Service)

Outbound initiated access to Azure Rights Management, the Microsoft Federation Gateway, and the services to support Microsoft Click-to-Run are possible if your organization has approved the use of a bidirectional Internet connectivity method. Similarly, inbound initiated access that is provided via a bi-directional Internet connection approved by your organization can be used to allow specific types of external applications within your on-premises environment or other cloud systems to interact with an ITAR-support plan instance. See the ITAR-Support Plan Feature Differences section for more information.

Encryption at Rest

Applies to: *Exchange Online, SharePoint Online, Lync Online*

The encryption of data at rest applies to the protection of customer data held in disk storage associated with each of the Office 365 service offerings. Disk storage encryption is performed by the Microsoft BitLocker Drive Encryption feature of Windows Server 2008, later server releases, and later releases of client versions of the Windows operating system.

Bitlocker encrypts the entire volume of data including the operating system itself, the Windows registry, and temporary files by following the Advanced Encryption Standard (AES) specification which is implemented using a 256 bit encryption key. Servers within Microsoft data centers are equipped with a Trusted Platform Module (TPM) – a microchip built into the server used to store cryptographic information such as encryption keys. BitLocker uses the TPM to lock the encryption keys that protect the disk storage data.

During the startup process, the TPM releases the key that unlocks the encrypted partition only after comparing and confirming a hash of important operating system configuration values with a snapshot taken earlier. Because the keys needed to decrypt the disk data remain locked by the TPM of the server associated with the disks, an attacker cannot read the data by removing your hard disk and installing it in another computer.

Microsoft maintains FIPS 140-2 validation for the BitLocker cryptographic modules. Within FIPS 140 Validation, see the **BitLocker® Validated Cryptographic Modules** section.

Encryption in Transit

***Applies to**: Exchange Online, SharePoint Online, Lync Online*

The base level of encryption provided for private network connectivity between your on-premises environment and the Office 365 Dedicated data center involves the use of the Transport Level Security (TLS) protocol. The TLS protocol also is used for client connectivity to Office 365 ITAR-support services. All X.509 certificates are generated using the Secure Hash Algorithm 2 (SHA-2) 256 bit standard as the cryptographic hash function.

The ITAR-support plan allows the Federal Information Processing Standard (FIPS) 140-2 Level 1 standard of cryptography to be applied, if required, to meet your security requirements. Also, if required by your organization and supported by your network carrier, connections between your network and the Microsoft network can be encrypted by the carrier using validated FIPS 140-2 Level 1 algorithms. Validated FIPS 140-2 Level 1 cryptographic algorithms also are used for all private network connections between primary and secondary data centers within the Microsoft network. If your organization allows your workforce to access Office 365 services remotely over the Internet using a Web browser interface, the ITAR-support services also will accommodate FIPS 140-2 Level 1 encryption for these sessions.

Customer-Controlled Encryption – IRM & S/MIME

***Applies to**: Exchange Online, SharePoint Online*

The ITAR-support offering utilizes the customer-controlled encryption methods that are available for Office 365 Dedicated services. Included are Information Rights Management (IRM) supported by the Active Directory Rights Management technologies of Microsoft and S/MIME encryption to apply a digital signature to mail messaging.

AD RMS is a Windows Server security product that works in conjunction with Microsoft Active Directory authentication. The capabilities of AD RMS are employed by information protection applications such as Information Rights Management (IRM) to safeguard digital information from unauthorized use. The Azure Rights Management service also is available to Exchange Online as well as SharePoint Online; implementation considerations are described in the Platform section below. Within Exchange Online and SharePoint Online, end users and/or administrators are able to define the level of IRM protection used for access restrictions and data usage rights. The restrictions and rights can be applied to supported file types, transported mail messages, and unified messaging content. The protected content remains encrypted during transport between systems and while being held for consumption by an end-user.

The encryption processing of AD RMS utilizes Federal Information Processing Standard (FIPS) 140-2 level 1 validated modules. See FIPS Compliance Issues for RMS for additional information. Implementation options for the IRM feature are described in the Exchange Online Dedicated and SharePoint Online Dedicated service descriptions.

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a widely accepted method for sending digitally signed and encrypted messages. S/MIME assures the recipient that the message received is the original and untampered message initiated by the sender and that the message was sent by a verified sender. To do this, S/MIME provides cryptographic security services such as authentication, message integrity, and non-repudiation of origin (using digital signatures). It also helps enhance privacy and data security (using encryption) for electronic messaging.

S/MIME requires a certificate and publishing infrastructure that is often used in business-to-business and business-to-consumer situations. The user controls applying the cryptographic keys for each message sent. When S/MIME encryption has been applied to a message, email applications such as Outlook will search a trusted root certificate authority location to perform digital signing or verification of a signature.

An administrator for your Exchange Online environment can enable S/MIME-based security for your organization.

Support for Data Spillage Scenarios

***Applies to**: Exchange Online, SharePoint Online, Lync Online*

Office 365 has features to support you if your organization ever needs to manage data "spillage." An example of data spillage is the submission of government classified data into Office 365. Compliance and security officials with appropriate RBAC privileges within your organization can use eDiscovery to search for the message or document and hard-delete the content item.

Your organization must establish procedures to address data spillage incidents. Available tools within Office 365 and procedures to consider as part of your data spillage remediation plan can be found within How to control data spillage in Office 365 dedicated and ITAR.

Connectivity Protection

The enhanced connectivity features available with Office 365 ITAR-support plans are described in this section. Included are required and optional secure connectivity capabilities involving the use of the Internet and client authentication methods.

Trusted Internet Connection

***Applies to**: Exchange Online, SharePoint Online, Lync Online*

The default network configuration for Office 365 ITAR-support services is via the private network connection dedicated to communication between your data centers and the Microsoft data centers; access to your ITAR-support services via a direct Internet connection is blocked at the Microsoft data centers. Federal government customers that require the use of a Trusted Internet Connection (TIC) should work with the Office 365 ITAR-support plan deployment team to determine how the TIC implementation requirements can be accommodated within the service design for your specific ITAR-support plan.

Federated Authentication

***Applies to**: Exchange Online, SharePoint Online*

Within the isolated data center environment for ITAR-support plan customers is infrastructure to support federated authentication. The Secure Token Service (STS) provided by Microsoft for ITAR-support plan services is referred to as the Office 365 ITAR-support Federation Hub. The system is used to establish a federated relationship with an STS established within your on-premises environment. Federated authentication facilitates access management by requiring an access request to be confirmed by your authentication system before access is granted. Security Assertion Markup Language (SAML) tokens exchanged between the client, your STS, and the Federation Hub are used to either grant or deny access to the requested service and to apply additional access restrictions. The Federation Hub is an Active Directory Federation Services (AD FS) version 2.0 system configured as a shared service dedicated to, and utilized by, all ITAR-support plan customers.

> **Note:**
>
> Connectivity between your on-premises Secure Token Service (STS) and the Office 365 ITAR-support Federation Hub must be established via the Internet. Federal customers are able to use the Trusted Internet Connection infrastructure to securely provide Internet connectivity. Engineering resources within Microsoft can assist with providing implementation guidance. Contact your Microsoft Account Team for assistance.

Multi-Factor Authentication

***Applies to**: Exchange Online, SharePoint Online*

In accordance with Homeland Security Presidential Directive 12, the Office 365 ITAR-support offering allows federal agency customers to configure Exchange Online and SharePoint Online services to support multi-factor authentication (MFA) using FIPS 201-1 compliant Personal Identity Verification (PIV) smart cards or Department of Defense Common Access Card (CAC) smart cards. Customers can leverage PIV/CAC support to securely authenticate client connections that use the Microsoft Outlook and Outlook Web App (OWA) applications to access Exchange Online as described in the MFA section of the Exchange Online Dedicated Service Description.

MFA is implemented using federated authentication. See the Federated Authentication section above for additional information.

To utilize PIV or CAC smart cards, your organization must adhere to the following requirements:

- Meet all technical and infrastructure prerequisites to establish PIV/CAC services (e.g., issuing PIV/CAC cards to your staff, establishing trust and certificates for authentication against Office 365 services, and deployment of specific client modifications to support PIV); additional details for specific customer implementation scenarios will be provided by Microsoft.
- Implement and support all customer-side configuration and security changes that are required to deploy and use PIV/CAC.
- Address all client-side authentication issues that arise during production use of PIV/CAC.
- Manage, remediate, and support the public key infrastructure (PKI) and card management functions for PIV/CAC.

The following limitations apply to the use of PIV in your environment:

- PIV is only available to U.S. government agencies and CAC is only available to Department of Defense agencies.
- Only the "premium" (full client) version of Outlook Web App is supported; the use of the "light" version of Outlook Web App with mobile devices is not supported.
- PIV/CAC support for is provided by SAML-based authentication via a federated trust involving a Security Token Service (STS) product such as Active Directory Federation Services (AD FS) or a compatible third-party product approved by Microsoft.

ITAR-Support Plan Feature Differences

The ITAR-support plan offering leverages the data center release of Office 365 Dedicated. The online versions of Exchange, SharePoint, and Lync provided with the offering are all the based upon the 2013 version of each server application. The administrative and user-level features of the Dedicated and ITAR-support plan releases are fundamentally similar; however, implementation differences exist in several areas. As indicated in the introduction, comprehensive descriptions of the features and functionality of Exchange Online, SharePoint Online, Lync Online, and platform related services are provided within the service description set for Office 365 Dedicated. Implementation differences for the ITAR-support release are highlighted in the service descriptions; additional detail is provided within this section.

Exchange Online

In comparison to the Exchange Online Dedicated ANSI platform offering, the following service, feature, and tool characteristics apply to the ITAR-support plan version of Exchange Online:

Exchange Online Protection – Microsoft Exchange Online Protection (EOP) is a cloud-based email filtering service that helps protect your organization against spam and malware. The service also includes features to safeguard your organization from messaging-policy violations. EOP is available to all Exchange Online Dedicated and ITAR-support plan customers at no additional charge. By default, EOP is not enabled for a Dedicated or ITAR-support plan environment. EOP accepts and transmits mail messages via the Internet. Connectivity between Exchange Online and EOP is via private data connectivity maintained by Microsoft. If your organization chooses to not utilize EOP, your instance of Exchange Online will only scan mail messages for malware and process all offending messages.

Office Online – With Exchange Online, the Office Online shared service is used by Outlook Web App (OWA) to render Microsoft Office and Adobe Acrobat PDF attachments. By default, Office Online is not enabled for an ITAR-support plan environment due to the requirement for Internet connectivity between the two services. Blocked access to Office Online will require your client systems to download all OWA attachments for rendering by an application on the client.

Calendar Free/Busy Sharing – The Exchange 2013 Availability Service can be used with Exchange Online to share user schedule availability data on-demand between your ITAR-support plan environment and mail servers within (a) on-premises forests in your environment, (b) ancillary forests associated with your organization, and/or (c) forests within the multi-tenant version of Exchange Online. To interact with Exchange Online, the remote forest must use an Exchange Server 2010 or Exchange Server 2013 system with Internet access to support connectivity with the Microsoft Federation Gateway (MFG). In addition, an Internet connectivity implementation approved by your organization between your Exchange Online environment and the MFG also must be established. The actual sharing of calendar data involves the delivery of the data via either your private network connection (between your on-premises Exchange servers and Exchange Online) or via the Internet (between systems outside of your on-premises environment and Exchange Online).

Office 365 Message Encryption – If your organization has a need to forward protected Exchange Online messages to external recipients, the Office 365 Message Encryption (OME) service can be used in conjunction with Microsoft Exchange Online Protection (EOP) and Azure Rights Management. As an admin, you can set up transport rules that define the conditions for message encryption. When a user sends a message that matches a rule, encryption is applied automatically. To view encrypted messages, recipients can either get a one-time passcode, sign in with a Microsoft account, or sign in with an Office 365 account that is external to your service instance. Recipients also can send encrypted replies. An Office 365 subscription is not needed to view encrypted messages or to send encrypted replies.

At this time, only the commercial version of Azure Rights Management is available to support the OME service when used with an ITAR-support plan offering. Note that Internet connectivity is required between your Exchange Online service instance and Azure Rights Management. To establish your OME implementation, contact your Service Delivery Manager to request assistance.

SharePoint Online

In comparison to the SharePoint Online Dedicated legacy platform offering, the following service, feature, and tool characteristics apply to the ITAR-support plan version of SharePoint Online:

Office Online – Within the ITAR-support environment, dedicated servers are used to provide a localized implementation of Office Online to support the rendering of Microsoft Office and Adobe Acrobat PDF content held within SharePoint Online. Internet connectivity is not required for the localized instance of the Office Online service.

Content Storage – The ITAR-support plan offerings of SharePoint Online and the companion OneDrive for Business service do not utilize Microsoft Azure to hold data. All files created, modified, and viewed by these systems are held within local SQL server storage contained within the physical boundaries of the Microsoft data centers reserved for ITAR-support plan customers.

External Application Access - Inbound initiated access provided via a bi-directional Internet connection approved by your organization can be used to allow specific types of external applications within your on-premises environment or within other cloud systems to interact with an ITAR-support plan of SharePoint Online – see the SharePoint Online Dedicated Service Description for more information regarding either option.

Lync Online

Within the Lync Online Dedicated legacy platform offering, the following service, feature, and tool characteristics apply to the ITAR-support plan version of Lync Online:

Enterprise Voice & Dial-in Conferencing – The Enterprise Voice and Dial-in Conferencing features provided with the Lync Online Dedicated offering are not available as a standard offering for the ITAR-support release. To introduce enhanced voice services into your environment, contact your Microsoft Account Team for solution assessment assistance.

Exchange Online Unified Messaging Support for On-Premises IP-PBX – An on-premises Lync Server, Skype for Business Server, or third-party IP-PBX system established and maintained by your organization can be configured to utilize the unified messaging services of the Exchange Online service provided with your ITAR-support offering. To comply with security requirements, connectivity between your on-premises environment and the ITAR-support environment endpoints must be via the private data network established between the two locations.

Platform

The Platform services provided within the ITAR-support plan offering include the following:

Core Services	Ancillary Services
Identity	Change Management
Provisioning	Support
Network	Service Continuity Management

In comparison to the legacy platform offerings of Office 365 Dedicated, the following service, feature, and tool characteristics apply to the ITAR-support plan version of Platform services:

Azure Rights Management – The Azure Rights Management shared service is only available for use with Exchange Online. All client systems as well as Exchange Online must use bi-directional Internet connectivity to communicate with Azure Rights Management. An Internet implementation approved by your organization to support Azure Rights Management is required. See Azure Rights Management for more information.

At this time, only the commercial version of Azure Rights Management is available as a file and message encryption service for ITAR-support plan customers; a similar service provided within the Azure Government cloud services environment is not currently available. For information regarding the availability of new Azure Rights Management services, contact your Microsoft Account Team representative.

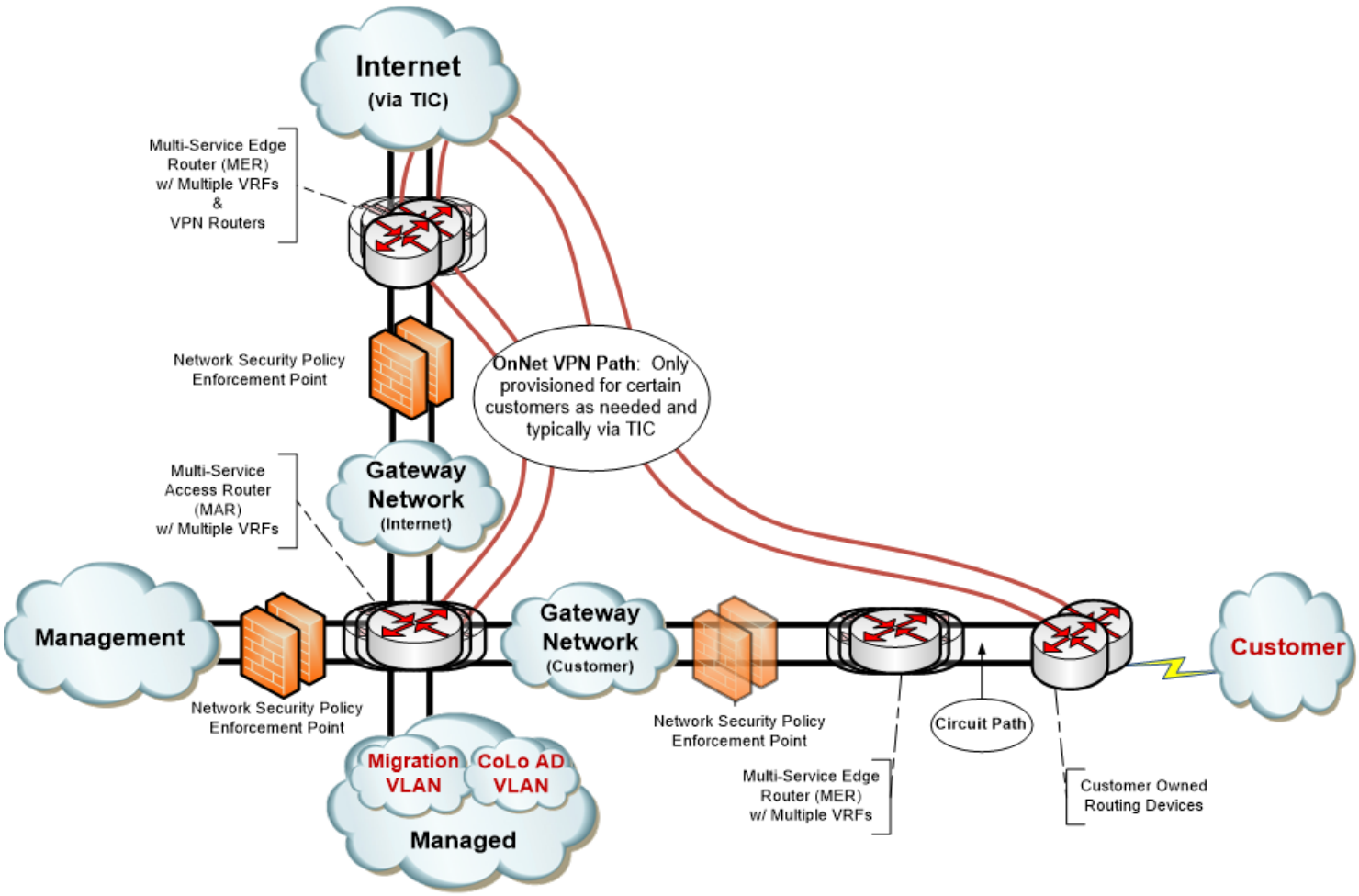
Volume Licensing of Microsoft Office Client Applications – Office 365 ProPlus is the version of Office that is available as an optional volume licensing offering for your Office 365 plan. As described in the Identity & Provisioning Service Description for the legacy platform releases, the delivery of Office ProPlus relies upon the use of the Click-to-Run (C2R) streaming and virtualization technology provided by Microsoft. To utilize C2R, all clients must have Internet access, a multi-tenant "Quick Start" instance of an Office 365 tenant must be created, and the synchronization of on-premises Active Directory user objects to Azure Active Directory must be established. Your Microsoft Service Delivery Manager can assist with establishing your Office 365 tenant. If your organization chooses to not utilize the C2R service, contact your Microsoft Account Team to gain access to a Licensing Specialist for assistance with obtaining a .msi copy of the Office applications you require and the licensing keys for each application.

Private Networking Implementation – The private networking framework for an ITAR-support implementation leverages the networking model for Office 365 Dedicated. In the Network Service Description for the legacy platform releases of Office 365 Dedicated, the following changes apply:

- Within the **Customer-Owned Private Network Connection** section, the description regarding the use of a third-party *edge site* does not apply. For an ITAR-support plan networking implementation, private networking connections terminate within the Microsoft data center that provides your ITAR-support plan services.
- Federal government customers must arrange to configure and confirm FIPS 140-2 encryption for all private networking or Internet IPsec VPN connections used between your on-premises facilities and Microsoft data centers.
- For ITAR-support plan network services, it is strongly recommended that private networking is implemented to connect to Microsoft data centers. If Internet IPsec VPN connections are used, the following should be considered:

    - Federal agencies seeking to use Office 365 ITAR-support plan services should contact their authorizing official to determine whether a TIC or other secure connection mechanism is required and to identify any additional restrictions to consider.
    - Federal agencies must decide whether to mandate that the site-to-site VPN is routed through a TIC zone.
    - Federal agencies must provision either an MPLS circuit or VPN with a licensed TIC access provider (TICAP).

- The Microsoft network architecture and security zone components for an ITAR-support plan implementation are represented in the diagram shown below. When referencing the Network Service Description for the legacy platform releases of Office 365 Dedicated, the illustration below replaces the management network diagram in the service description. The Trusted Internet Connection (TIC) shown in the implementation is applicable only to federal government customers. Microsoft does not deploy the TIC equipment or networking facilities. All federal agencies that utilize the TIC architecture must ensure that an appropriate TIC implementation is established and maintained for the customer connection to the Gateway Network/Internet (GN/I) edge router demarcation point in the Microsoft data network. Similarly, your organization must arrange to establish network connectivity between your on-premises environment and Gateway Network/Customer (GN/C) edge router demarcation point in the Microsoft data network.



Private Networking Implementation – ITAR-support Plan Legacy Platform Release

Ancillary Services – Change Management, Support, and Service Continuity Management services for the ITAR-support plan offering are the same set of services provided for Office 365 Dedicated as described in their respective legacy platform service description. All Microsoft personnel involved in change, support, and service continuity functions that are required to directly access customer content as part of their functional role will be personnel that have been subject to requirements described in the Personnel and Background Checks section.

Support personnel with a need to transfer data (e.g., logs or files with sensitive data) will utilize the Secure Files Store (SFS) system to facilitate the data transfer. The SFS resides within the ITAR-support plans security boundary. A SFS system is assigned to each ITAR-support plan customer. The system requires a separate set of authentication credentials to gain access. Support personnel engaged in issue resolution will make your support staff aware of the procedures involved to access the SFS system.

Federal Regulatory Compliance and Support

The Office 365 ITAR-support plan complies with the Federal Information Security Management Act (FISMA) of 2002 regulations which cover the hosting of services. The FISMA regulation are a certification defined within the Federal Risk and Authorization Management Program (FedRAMP) program. The ITAR-support plan also provides support for customers with data that must be handled according to International Traffic in Arms Regulations (ITAR).

FISMA and FedRAMP Compliance

***Applies to**: Exchange Online, SharePoint Online, Lync Online*

In accordance with FISMA and FedRAMP requirements, Office 365 ITAR-support plans have been certified compliant with NIST 800-53 (Moderate) system-level requirements. Upon request, Federal agency customers will receive FedRAMP accreditation materials for the Office 365 ITAR-support plan as part of the onboarding process.

For US Department of Defense customers, Microsoft has prepared DoD SRG L5 templates for the Office 365 ITAR-support offering. Copies of the templates will be made available to DoD customers upon request to support accreditation review.

International Traffic in Arms Regulations (ITAR) – Commercial Agencies

***Applies to**: Exchange Online, SharePoint Online, Lync Online*

The Office 365 ITAR-support plan is designed to meet the need of commercial agencies that handle ITAR-controlled information through the following security and screening features:

- All ITAR-support plan customers receive their own dedicated service hardware which is managed to the same FedRAMP-compliant standards as federal agency customers.
- All ITAR-support plan customer have their Office 365 service infrastructure hosted in U.S. data centers.
- Physical, logical, and network access controls ensure that only properly screened Microsoft support and operational personnel have access to the Office 365 production systems for ITAR-support plans.
- Screening standards include validation of U.S. citizenship of all Microsoft support and operational staff before access is granted to Office 365 production systems for ITAR-support plans.

Personnel and Background Checks

***Applies to**: Exchange Online, SharePoint Online, Lync Online*

For the Office 365 ITAR-support plan offering, Microsoft ensures that personnel with access to *customer content* are U.S. citizens in accordance with International Traffic in Arms Regulations (ITAR) which restricts access to ITAR-controlled content to "U.S. Persons" or "U.S. Citizens." In addition, all customer content is processed and stored in Microsoft data centers that are located only in the United States.

All Microsoft personnel who have access to *customer data* that are hosted in Office 365 ITAR-support plan environments undergo the background checks and screenings described in the following table:

Microsoft Personnel Screening and Background Checks	Description
US Citizenship	Verification of US citizenship.
Employment History Check	Verification of seven (7) year employment history.
Education Verification	Verification of highest degree attained.
Social Security Number (SSN) Search	Verification that the provided SSN is valid.
Criminal History Check	A seven (7) year criminal record check for felony and misdemeanor offenses at the state, county, and local level and at the federal level.
Office of Foreign Assets Control List (OFAC)	Validation against the Department of Treasury list of groups with whom U.S. persons are not allowed to engage in trade or financial transactions.
Bureau of Industry and Security List (BIS)	Validation against the Department of Commerce list of individuals and entities barred from engaging in export activities.
Office of Defense Trade Controls Debarred Persons List (DDTC)	Validation against the Department of State list of individuals and entities barred from engaging in export activities related to the defense industry.
Fingerprinting Check	Fingerprint background check against FBI databases.

Selected background checks will be repeated on a recurring basis for Microsoft personnel that have access to customer-owned data.

The information contained in this document represents the current view of Microsoft Corporation on the topics described as of the date of publication. Because Microsoft must respond to changing market conditions, the content of this document should not be interpreted to be a commitment on the part of Microsoft. The accuracy of any information presented after the date of publication cannot be guaranteed by Microsoft. The Information is provided for marketing purposes only and cannot be incorporated within, or attached to, any type of agreement.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.