Infrastructure Processes and Storage Options

Common Questions from the Institutional Review Board

To assist with questions from the Institutional Review Board (IRB) regarding information security, the Office of the Chief Information Officer (OCIO) Infrastructure Risk Management team has developed this document outlining common processes and storage options available to OCIO and Managed IT Services (MITS) (it.osu.edu/MITS) partners.

The OCIO adheres to the university's Information Security Control Requirements (ISCR) (cybersecurity.osu.edu/ISCR) as much as possible. The ISCR is primarily based on the NIST SP 800-53 security standard and the CPI-RISC Information Risk Framework.

Endpoint Management

OCIO-managed endpoints are enrolled in device management tools. These tools are used to monitor and detect software versions and security threats such as viruses and malware. They are also used to apply updates, patches, and various policies designed to keep endpoints as secure as possible.

OCIO-managed endpoints are encrypted using industry standard tools which vary depending on operating system.

For remote access, only managed devices are granted access to connect to our Cisco virtual private network (VPN). Users without a managed device are provided with an alternative, secure process to access university data from an offsite location. Additionally, the OCIO has deployed Always On VPN to connect users to VPN without requiring any action from the end user.

The OCIO participates in Enterprise Security's data loss prevention (DLP) and vulnerability management programs. Additionally, several tools provide logging of security events related to managed endpoints.

Microsoft 365 Email (Exchange Online)

The university is currently using Microsoft 365 Email for faculty, staff, and students allowing for the use of Outlook Mobile, Outlook for Desktop (Mac and Windows) and Outlook for the web.

Email encryption at Ohio State is done for external domains only via a third-party product called ZixCorp. All email that is transported internally between current Ohio State users is considered encrypted and will not pass through ZixCorp.

Currently, research-related data (CUI, ITAR, EAR) is not permitted on Ohio State’s M365 tenant. With that in mind, Ohio State offers an on-premises Exchange environment specifically for research correspondence with authorized persons. Any export-controlled data sent through this system is done so using the university approved encryption system, ZixCorp.

Microsoft uses Transport Layer Security (TLS1.2) to encrypt the connection session between two servers. Encryption at rest for Exchange Online is performed at Microsoft data centers via BitLocker Drive (AES-256) encryption.

Microsoft 365 utilizes Exchange Online Protection (EOP) cloud-based filtering against spam and malware.

Account management for Microsoft 365 applications and services is handled by Azure AD.

Microsoft provides several audit logging and reporting features that are available through the Microsoft 365 Security & Compliance Center (protection.office.com), Microsoft 365 Security Center (security.microsoft.com), Microsoft 365 Compliance Center (compliance.microsoft.com), and Microsoft 365 Admin Center (admin.microsoft.com). These centers allow administrators to access security-related alerts, search through content, and review audit, usage, and activity logs.

Storage on OCIO Servers

The data will be stored on the OSU Isilon which is hosted at the State of Ohio Computing Center (SOCC). The SOCC is a Tier II data center based on the Uptime Institute’s Tier Standards. The data center offers defense in depth through comprehensive physical and environmental security controls, including the following key controls:

- 24/7 onsite security staff
- Closed-circuit television (CCTV) recording and monitoring
- Secured physical access (staffed entry points, badge access, locked cages, etc.)

- Escorted visitor access
- Multi-factor authentication (MFA) for authorized access to secure areas

In addition to these physical security measures, many additional security controls have been implemented for the in-scope systems. These include:

- Managed and restricted user access
- Multi-factor authentication (MFA)
- Audit logging
- Robust change management processes
- Data encryption (256-bit encryption via self-encrypting drives)
- Anti-virus scanning
- Realtime ransomware monitoring & prevention
- Filesystem event auditing

Storage in OneDrive for Business

OneDrive for Business, which utilizes SharePoint Online's underlying architecture, is Microsoft's enterprise cloud storage platform that enables users to access their files from any of their devices, including mobile and desktop devices as well as from web browsers.

OneDrive for Business also facilitates collaboration by allowing users to share files within or external to their organization as well as provides real-time coauthoring capabilities for productivity applications.

OneDrive is currently configured to allow for anonymous links. Anonymous links (aka public links, open links or anyone links) allow people to collaborate by sharing files and/or folders that do not require an account or authentication to access. With OneDrive, anonymous links also enable the ability to set link expiration dates and to password protect those links. Event and audit data of sharing link activities including type and use are logged within Office 365 and delivered to Splunk.

OCIO security measures include:

- Access management for OneDrive for Business is managed through Azure AD.
- Data loss prevention tools are in place.
- Encryption - For data processed and stored within OneDrive for Business, data is encrypted as it moves from the client to server as well as from server to server, internally. Data transmitted from the client to server is encrypted using TLS. Data are also fully encrypted at rest using disk- and file- level encryption. At the disk level, data

are encrypted using BitLocker (AES-256). Each file is also individually encrypted using AES-256 with its own unique encryption key.

- Logging - User activity is captured for OneDrive for Business within the unified audit log available through the Security and Compliance Center (protection.office.com). Additionally, OneDrive for Business allows end users to generate a downloadable sharing report which denotes shared content as well as to whom the content is shared.
- Data Storage and Architecture - Data is maintained within a user's OneDrive for Business repository, which is built on SharePoint Online Document Libraries. When a file is uploaded to OneDrive for Business (SharePoint Online), the uploaded content is disassembled and translated into application code, which is stored in multiple tables across multiple databases. On the backend, SharePoint Online utilizes SQL Server and Azure Storage for customer metadata storage and stores encrypted file content in Azure blobs. At-rest, data are stored in the following three (3) physically separate locations:
  - Azure blob stores – Customer content
  - SQL Server – includes smaller chunks of customer data, metadata to reassemble customer content, as well as maintains encrypted encryption keys used in the blob store encryption process (known as the Content Database)
  - Key store – Credentials for accessing storage containers and master key to the encrypted keys stored in the Content Database.

Physical Security – Microsoft 365

Microsoft 365 is physically hosted in fenced and non-descript Microsoft-managed datacenters ("Microsoft Datacenters") distributed across the globe. New customer tenants are provisioned in a geographical datacenter location according to the billing address configured with the customer's initial subscription, which, in the university's case, is based in the United States. Datacenter locations based in the United States are located in the following cities: Boydton, Cheyenne, Chicago, Des Moines, Quincy, San Antonio, Santa Clara, and San Jose.

A layered approach to physical security exists at datacenters with electronic card access control devices to restrict access to authorized personnel at perimeter doors along with additional security access technologies for rooms within the datacenter that contain critical computing equipment. These mechanisms include electronic card access control, keyed locks, man traps, and/or biometric devices. The datacenters are equipped with surveillance systems and are staffed and monitored on a 24x7 basis by security personnel, who conduct periodic inspections of datacenter areas as well as operate and monitor the surveillance systems. Surveillance records are maintained for a period of 90 days or as law within the local jurisdiction dictates.

A quarterly audit is performed to ensure only authorized individuals have access to secure facilities.