

DATA USE

OneDrive for Business and SharePoint Online

What Types of Information Can I Store on OneDrive for Business and SharePoint Online?

OneDrive for Business and SharePoint Online are Microsoft's cloud-based storage and collaboration solutions. This means that any information input or stored using these services is hosted in an off-campus, non-university-owned data center.

Florida State University (FSU) has a signed Business Associate's Agreement with Microsoft to reasonably safeguard personal information against inappropriate use and/or disclosure. Information Technology Services (ITS) has activated audit controls within OneDrive for Business and SharePoint Online to record select activity and provide forensic capabilities should unauthorized activity be detected. In addition, Microsoft uses an industry standard encryption solution to protect data between the user's device and the receiving server, internal server-to-server communications and Bitlocker disk and file storage encryption which meets the federal FIPS 140-2 requirements for encryption strength.

Before choosing to share and store information on OneDrive for Business or SharePoint Online, consider the sensitivity and protected nature of the information, including the following applicable university/state/federal policies, laws, Executive Orders, regulations, contractual obligations or other restrictions.

Usage Matrix

The following matrix identifies what types of data are approved for storage on FSU's OneDrive for Business and SharePoint Online.

Data Type	OneDrive for Business and SharePoint Online Approved Use	Additional Information
Family Educational Rights and Privacy Act (FERPA)	Yes	FSU Registrar's FERPA website
Health Insurance Portability and Accountability Act (HIPAA)	Yes	Microsoft Business Associates Agreement
Gramm-Leach-Bliley Act (GLB Act)	Encrypted GLB data classified as protected ¹	FSU Controller's Office
Payment Card Industry Data Security Standard (PCI DSS)	PCI DSS documentation not including primary account number, cardholder name, expiration date, full track data, CVV, PIN block	PCI Security Standards Council
Contractually-Restricted Research Information	Refer to contract for restrictions	FSU Office of Research
Human Subject Research (de-identified)	Yes	
Human Subject Research	Encrypted human subject research only ¹	FSU Office of Research – Human Subjects
International Traffic in Arms Regulations (ITAR)	No ²	FSU Office of Research – Export Controls Compliance Program
Export Administration Regulations (EAR)	No ²	FSU Office of Research – Export Controls Compliance Program
Federal Information Security Management Act (FISMA)	No ²	FSU Office of Research
Covered Defense Information (CDI) including Controlled Unclassified Information (CUI) and Controlled Technical Information (CTI)	No ²	FSU Office of Research
Social Security Number (SSN)	Must be encrypted when stored with name ¹	

¹Microsoft encrypts data in transit and at rest; however, units still have the option of encrypting information and controlling the possession of the encryption keys.

²Select end user configurations for OneDrive may have redirect options turned on to create file saves to OneDrive and the users local computing device. It is incumbent on these users to ensure they do not save restricted protected information to OneDrive or SPO in violation of legislated or contractual obligations concerning cloud storage restrictions.

Usage Detail

Family Educational Rights and Privacy Act (FERPA)

It is permissible to store FERPA information on OneDrive for Business and SharePoint Online, including grades, student transcripts, degree information, disciplinary records and class schedules.

Health Insurance Portability and Accountability Act (HIPAA)

Health Information Technology for Economic and Clinical Health (HITECH) Act

HIPAA Omnibus Final Rule

If a university unit is a “covered entity” or a “business associate” and stores "protected health information" as defined in 45 CFR § 160.103, then execution of the university’s volume licensing agreement includes execution of the HIPAA Business Associate Agreement (BAA), the full text of which is available at:

<http://www.microsoftvolumelicensing.com/userights/DocumentSearch.aspx?Mode=3&DocumentTypeId=52&Language=1>.

It is the responsibility of the FSU covered entity or business associate to review this agreement to ensure the service meets the currently enacted privacy and security provisions of HIPAA/HITECH/Omnibus Final Rule for the type of information stored on OneDrive for Business or SharePoint Online.

The Gramm-Leach-Bliley Act (GLB Act)

Officially known as the Financial Modernization Act of 1999, this act includes privacy provisions to protect consumer information held by financial institutions. Because of student loan activity conducted by the university, FSU is considered a financial institution under the GLB Act.

Contractual Agreements

Individuals responsible for maintaining contractual agreements with outside entities should review provisions that may restrict moving select information into a third party cloud storage environment such as OneDrive for Business or SharePoint Online.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a contractual agreement between the university and its merchant bank. The

agreement covers handling of credit card numbers, magnetic stripe contents, card verification code numbers and expiration dates. In addition to the standards outlined above for sensitive systems, PCI DSS requires extra security and has its own set of standards. Information classified as “Protected” per the latest version of PCI DSS must be encrypted when stored on OneDrive for Business or SharePoint Online. The encryption key used for this process may not be stored in OneDrive for Business or SharePoint Online. PCI DSS information not classified as “Public or Private” can be stored on OneDrive for Business or SharePoint Online in an unencrypted format.

Contractual Restrictions Governing Research

Externally-funded research and sponsored projects may contain contractual restrictions on the release of information that could include a prohibition on the use of cloud computing services or third party digital data storage. Failure to comply with the contractual restriction could result in breach of contract and, if the contract is federally funded, possible civil or criminal fines and penalties. Consult with the FSU Office of Research for further guidance.

Other Laws or Restrictions

Other laws or restrictions (e.g., human subjects, confidentiality, granters, export control) may prevent you from moving information into OneDrive for Business or SharePoint Online, including:

Human Subject Research

Allowed: De-identified human subject research and encrypted human subject research classified as “Protected”

Not Allowed: Unencrypted protected identifiable human subject research

International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR)

Not Allowed: Information containing research on things such as chemical and biological agents, satellite communications, certain software or technical information and work on formulas for explosives. In addition, using cloud computing servers or storing digital data on third party servers located in a foreign country are exports; if the information exported is controlled, the exporter (the person who transmitted the data) could face civil and/or criminal fines and penalties. Consult with the FSU Office of Research for further guidance.

Federal Information Security Management Act (FISMA)

Not Allowed: Any government information that is regulated by the Federal Information Management and Security Act, including VA, FDA and Medicare information. Consult with the FSU Office of Research for further guidance.

Controlled Defense Information (CDI)

Not Allowed: CDI (CUI and CTI) is governed by contract language and NSIT 800-171 control requirements. Further, there are restrictions limit the movement of CDI to only FedRAMP approved cloud vendor services. The current Microsoft Online Service agreement with FSU does not include FedRAMP approved services.

Social Security Numbers (SSNs)

Allowed: Encrypted SSNs with associated names

Not Allowed: Unencrypted SSNs with associated names

Personal use of OneDrive for Business and SharePoint Online

Faculty and staff who use OneDrive for Business or SharePoint Online for non-university business purposes must understand this information may be subject to searches by subpoena or other law enforcement demands for information as part of university operations. Users are recommended to obtain a personal [OneDrive](#) or SharePoint Online accounts to conduct non-university business.