



## What Types of Information Can I Store on OneDrive for Business?

OneDrive for Business is a Microsoft off-premise, cloud-based storage solution. This means that any information stored using this service is hosted in an off-campus, non-university-owned data center(s).

Florida State University (FSU) has a signed Business Associate's Agreement (BAA) with Microsoft to reasonably safeguard personal information against inappropriate use and/or disclosure. Users needing to store and/or share university information classified as "Protected" using OneDrive for Business must enable auditing. Use the instructions at the end of this document to turn on auditing. If an account is compromised, auditing allows a user or administrator to see when a file was created, when it was read, who edited the file and who searched for it.

Before choosing to share and store information on OneDrive for Business, 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.

# OneDrive for Business Usage Matrix

The following matrix identifies which types of data are approved for storage on FSU's OneDrive for Business.

<i>Data Type</i>	<i>OneDrive for Business Approved Use</i>	<i>Additional Information</i>
Family Educational Rights and Privacy Act (FERPA)	Yes	
Health Insurance Portability and Accountability Act (HIPAA)	Yes	<a href="#">Refer to the Microsoft Business Associates Agreement for details.</a>
Gramm-Leach-Bliley Act (GLB Act or GLBA)	Encrypted GLB data classified as protected	<a href="#">Contact the FSU Controller's Office for additional information.</a>
Payment Card Industry Data Security Standard (PCI DSS)	No Primary Account Number/Cardholder Name/Expiration Date/Full Track Data/CVV/PIN Block- All other PCI DSS related documentation is allowed	<a href="#">Refer to current PCI DSS requirements for additional guidance</a>
Contractually Restricted Research Information	Refer to Contract for Restrictions	<a href="#">Contact the FSU Office of Research for additional information.</a>
Human Subject Research (De-identified)	Yes	
Human Subject Research	Encrypted Human Subject Research only	<a href="#">Contact the FSU Office of Research for questions on storing human subject research or refer to data sharing agreements if applicable.</a>
The International Traffic in Arms Regulations (ITAR)	No	<a href="#">Contact the FSU Office of Research to confirm methods of storing ITAR information.</a>
Export Administration Regulations (EAR)	No	<a href="#">Contact the FSU Office of Research to confirm methods of storing EAR information.</a>
The Federal Information Security Management Act (FISMA)	No	<a href="#">Contact the FSU Office of Research to confirm methods of storing FISMA information.</a>
Social Security Number (SSN)	SSN must be encrypted when stored with name	Number in combination with an individual's name must be encrypted.

## Usage Detail

### Family Educational Rights and Privacy Act (FERPA)

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

### Health Insurance Portability and Accountability Act (HIPAA)/The 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 this [link](#). 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.

### 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. Student loan information, payment history and student financial aid information classified as “Protected” should not be stored on OneDrive for Business unless it is encrypted and the encryption key is not stored on OneDrive for Business.

### 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.

#### 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. The encryption key used for this process may not be stored in OneDrive for Business. PCI DSS information not classified as “Public or Private”

can be stored on OneDrive for Business 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. Please consult with the university Office of Research for further information.

## 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, including:

#### Human Subject Research

Allowed: De-identified human subject research.

Not Allowed: Unencrypted protected identifiable human subject research.

Allowed: Encrypted human subject research classified as “Protected.”

#### 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.

#### The 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.

#### Social Security Numbers (SSNs)

Not Allowed: Unencrypted SSNs with associated names.



Allowed: Encrypted SSNs with associated names.

## Personal use of OneDrive for Business

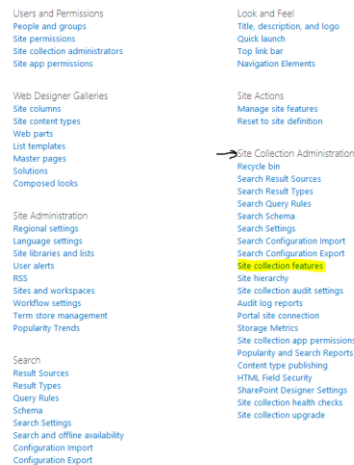
Faculty and staff who use OneDrive for Business for non-university business purposes must understand this information may be subject to searches by subpoena or other law enforcement demands for information as part of university operations. It is recommended users obtain a personal OneDrive account to conduct non-university business.

## Turn on OneDrive for Business Auditing

The most important reason to enable OneDrive for Business auditing is that it allows you to have a record of whom you have shared documents with. To turn on auditing, follow these simple steps:

1. Log in to Office 365 at: <https://outlook.com/fsu.edu>
2. Click the **Grid icon**  in the upper left-hand corner
3. Select **OneDrive**
4. Click the **Gear icon**  in the upper right-hand corner
5. Select **Site Settings**
6. Under the **Site Collection Administration** section, click **Site collection features**

### Site Settings



7. Scroll down to **Reporting** and click the **Activate** button on the right

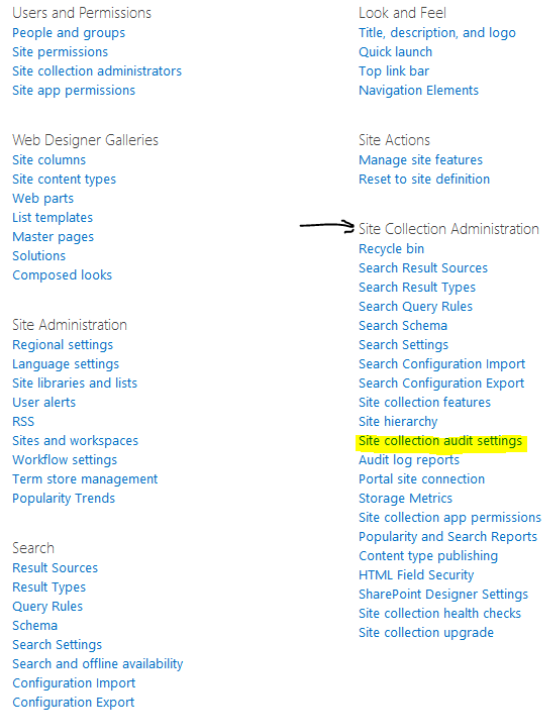


You will see a blue “**Activate**” button appear next to a Deactivate button to confirm your activation of the service.

8. Go back to the Site Settings page by clicking the **Gear Icon**  in the upper right-hand corner and click on “**Site Settings**.”

9. Under the **Site Collection Administration** section, click **Site collection audit settings** and specify which events to audit.

## Site Settings



10. Information Technology Services recommends you check all of the boxes to the right of the “**Documents and Items**” and “**Lists, Libraries, and Sites**”.

## 11. Click **OK**

### Configure Audit Settings

**Audit Log Trimming**  
Specify whether the audit log for this site should be automatically trimmed and optionally store all of the current audit data in a document library. The schedule for audit log trimming is configured by your server administrator. [Learn more about audit log trimming](#)

Automatically trim the audit log for this site?  
☒ Yes ☐ No

Optionally, specify the number of days of audit log data to retain:

If you'd like to keep audit data for longer than this, please specify a document library where we can store audit reports before trimming occurs:

**Documents and Items**  
Specify the events that should be audited for documents and items within this site collection.

**Specify the events to audit:**

- ☒ Editing items
- ☒ Checking out or checking in items
- ☒ Moving or copying items to another location in the site
- ☒ Deleting or restoring items

**Site Libraries and Sites**  
Specify the events that should be audited for lists, libraries, and sites within this site collection.

**Specify the events to audit:**

- ☒ Editing content types and columns
- ☒ Searching site content
- ☒ Editing users and permissions

12. To create an audit report, return to the **Site Settings** page

13. Under the **Site Collection Administration** section, click **Audit Log Reports**

## Site Settings

Users and Permissions  
People and groups  
Site permissions  
Site collection administrators  
Site app permissions

Web Designer Galleries  
Site columns  
Site content types  
Web parts  
List templates  
Master pages  
Solutions  
Composed looks

Site Administration  
Regional settings  
Language settings  
Site libraries and lists  
User alerts  
RSS  
Sites and workspaces  
Workflow settings  
Term store management  
Popularity Trends

Search  
Result Sources  
Result Types  
Query Rules  
Schema  
Search Settings  
Search and offline availability  
Configuration Import  
Configuration Export

Look and Feel  
Title, description, and logo  
Quick launch  
Top link bar  
Navigation Elements

Site Actions  
Manage site features  
Reset to site definition

Site Collection Administration  
Recycle bin  
Search Result Sources  
Search Result Types  
Search Query Rules  
Search Schema  
Search Settings  
Search Configuration Import  
Search Configuration Export  
Site collection features  
Site hierarchy  
Site collection audit settings  
**Audit log reports**  
Portal site connection  
Storage Metrics  
Site collection app permissions  
Popularity and Search Reports  
Content type publishing  
HTML Field Security  
SharePoint Designer Settings  
Site collection health checks  
Site collection upgrade