Stanford UNIVERSITY IT | Information Security Office

Position Paper

Position Title	Local Data Storage Use and Considerations
Position Audience	Stanford Faculty, Staff, and Students
Contact	Information Security Office
Position Release Date	2024-05-10
Last Update	Initial Posting

Problem Statement

With Google and Microsoft ending free and unlimited storage for higher education accounts, the university is applying a limit to the amount of data that can be stored at no cost on these platforms. As a result, individuals with significant storage needs may consider alternative options that Stanford has not vetted.

ISO Position

It is highly recommended that institutional files stored in your Stanford accounts remain in a Stanford-approved solution. Moving Stanford data to a personal storage account or purchasing local data storage significantly increases risk and is not a best practice.

- To explore a list of recommended Stanford storage solutions, visit University IT's Storage Recommendations website.
- For School of Medicine personnel, refer to USB external drives and encryption guideline: https://med.stanford.edu/irt/security/alldevices/external-drives.html

Storage guidance

Should you or your teams choose to use a storage solution that is not listed in the approved matrix, please consider Stanford's Administrative Guide Section 6.3.1 and Research Policy Handbook Section 1. 10 for specific requirements around the storage and management of Stanford data:

- To protect Stanford's sensitive data, the Stanford Administrative Guide guide section Section 6.3.1 Information Security (section 2) requires all individuals to comply with the University Minimum Security standards. The Stanford data classification for PHI is "High Risk PHI Data."
- The Risk Classifications website lists classifications of data allowed on a selection of commonly used Stanford University IT services. Individuals are advised to consult with the Information Security Office before using services that are not listed.
- Section 6.3.1 Information Security (section 4) states: "Any School or Department found to have violated this policy may be held accountable for the financial penalties and remediation costs associated with a resulting information security incident."
- Research Policy Handbook Section 1. 10 (section 3) states: "Research computing systems must be overseen by a full-time information technology (IT) professional. The level of care required for research computing systems depends solely on the highest designated risk classification of any of the project data."

Dangers of external storage devices

Storing Stanford data on personal hardware, such as an external hard drive or other portable device, significantly increases risk.

In exceptional circumstances where you feel it is necessary to store university data on an external device, you should discuss this matter with your manager or supervisor. Additionally:

- Store only such data as there is an immediate need for and remove the data from the external device when this immediate need no longer exists.
- The media should be located in a physically secure location or locked room or securely tied down so that theft would be difficult.
- Ensure the media is encrypted to mitigate risks associated with loss or theft.
- Back up datasets frequently, including those not stored on a computer. Backing up your files protects your data against ransomware, accidental loss, and system failures. Ensure that the backup of the data exists in a secure environment.

Resources

Helpful information security websites:

- Protecting Sensitive Data at Stanford
- Secure Computing Practices
- Stanford Medicine Information Security Services
- Stanford Administrative Guide 6.3.1 Information Security
- Research Policy Handbook 1.10 Information Security