Stanford UNIVERSITY IT | Information Security Office

Position Paper

Position Title	[Title]
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

Moving Stanford data to a personal storage account or purchasing local data storage is not a recommended best practice.

Files stored in your Stanford accounts that are institutional and not personal (individual) should remain in a Stanford-approved solution. To explore a list of recommended Stanford storage solutions, visit University IT's Storage Recommendations website.

- To protect Stanford's sensitive data, individuals are required to comply with University Minimum Security standards. The Stanford data classification for PHI is "High Risk PHI Data." The Risk Classifications website lists approved Stanford services corresponding to each risk level.
- Individuals are advised to consult with the Information Security Office before using services that are not listed.

Storing Stanford data on personal hardware, such as an external hard drive, significantly increases risk. Any physical medium purchased to store university data should follow these safe computing practices.

- 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.
- Note that 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. (https://doresearch.stanford.edu/policies/research-policy-handbook/conduct-research/information-security)
- For more guidance on USB external drives and encryption, School of Medicine personnel refer to https://med.stanford.edu/irt/security/alldevices/external-drives.html

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