Protecting Research Data

Produced by the Information Security Office

What does it mean to protect data?

Maintain Research Integrity	Research findings aren’t called into question because of corrupted data
Ensure Research Confidentiality	Data is not exposed and test subjects are protected from risk of harm
Continuous Research Availability	University network is more reliable than personal or removable storage devices

The C.I.A. Triad

Confidentiality
Data are only accessed by those who should have access.

Integrity
Data are known to be accurate and uncorrupted.

Availability
Accurate, uncorrupted data are available to approved individuals when needed.

The C.I.A. triad is the unifying philosophy for all information security and cybersecurity policies and practices at Texas State University.

Data minimization

The concept of reducing the need for data beyond what you need to collect and collecting the least risky data points possible.

Keep data minimization in mind when planning research projects.

For example: an age range is less risky than collecting someone's specific age, which is less risky than collecting someone's exact date of birth.

Age range > Specific age > exact DOB

University Data Classification

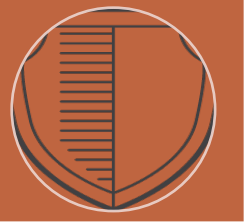
TXST uses a 3-tier data classification scheme established by **UPPS 04.01.11 & 02.08 a, b, c**

Confidential information is the highest-value and highest-risk. Disclosure poses risk of harm to data subjects and the university. **It must be protected from unauthorized disclosure.**

Confidential

Sensitive information can have attributes of both public and confidential information. **It must be protected from unauthorized disclosure.**

Sensitive



Public information, by its nature, is intended to be shared broadly and without restriction.

Public

Research Data Classification

The term “research data” can have wildly different meanings to different disciplines, and “research data” can present varying risks to data subjects, researchers, and the institution.

University policy classifies “unpublished research” as sensitive information, unless the data contain information that is classified as confidential. These blanket classifications convey a risk-averse stance that is intended to protect the confidentiality of the subject data.

Know Your Role

Information Resource **Owner**

Information Resource **Custodian**

Information Resource **User**

Principle of Least Privilege

The principle of least privilege refers to the concept that a user should be given the minimum levels of access – or permissions – needed to perform their job functions.

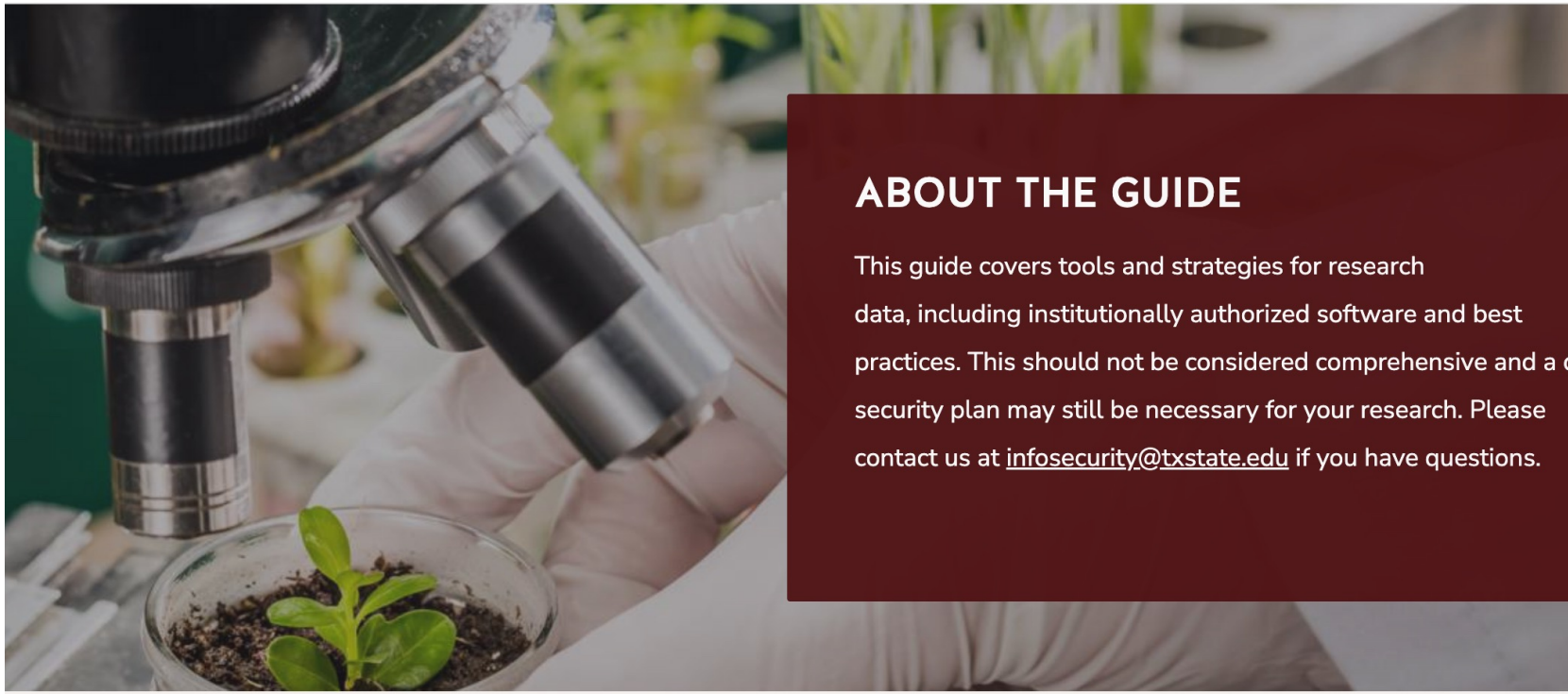
The principle of least privilege is a cybersecurity best practice, a fundamental step in protecting privileged access to high-value data and assets.

This model can be applied to applications, systems, or connected devices that require privileges or permissions to perform a job function.

Guidelines

Directions

Authorized Tools



https://infosecurity.txst.edu/work/research-guide.html

Preserving Research Data

Researchers, particularly project PIs, are responsible for ensuring that records related to their projects are retained for at least as long as is required by the university's Records Retention Schedule.

Depending on the data type, faculty sponsors of student projects may be required to assume retention responsibilities for their students' projects.

https://www.univarchives.txstate.edu/records/rm-rrs.html

Backup procedures

All researchers are strongly encouraged to ensure that important data are sufficiently and regularly backed up.

SharePoint, OneDrive, and restricted-access S:Drives have a high degree of redundancy on the back-end that will protect against data loss.

Institutional Support

- Funders and grantors may look favorably upon use of institutional resources by applicants
- Consider reviewing lineup of software, products, and services offered by TXST and including references in applications – many are provided at no cost
- Can consult with DoIT personnel to get more information as needed

Use Caution

- The ISO is less frequently consulted by ORSP pre/post award areas, but we are part of software authorization process in almost all cases.

- Receiving grant funds to procure something doesn’t bypass university compliance requirements.

- Procurement and related processes is often slow – can cause delays for time-sensitive projects

Getting ahead of the process

900+ Assessments last FY

The ISO required by policy and state law to review IT products and services before acquired

Review the Assessment page here:

https://infosecurity.txst.edu/services-tools/security-services/service-evaluation.html

Tips on using available tools

Know your data classification

Classification of data determines which tools are generally pre-authorized, which solutions are appropriate for which types of data, and what controls need to be in place.

Tips on using available tools

Find the sweet spot

For media like audio, video, images, and renders – capture only as high of a resolution as necessary, keeping in mind diminishing returns and challenges presented by ultra-large files.

For example - does an interview with a participant need to be recorded in 4k at 60fps if all the study needs is audio for transcription and coding?

Tips on using available tools

When in person…

Take advantage of on-campus bandwidth to conduct big file transfers.

Consider remoting into an office computer to download large files from Zoom or SecureTransfer before uploading them to SharePoint, OneDrive, or a restricted-access FileShare.

Non-university / personal projects

Endeavor to use university resources
Where it makes sense to do so (e.g., student projects, lit reviews, etc.)

Don’t use university resources for personal purposes.
Includes email, OneDrive, and university-owned computers and networks. Exposes data owner and university to unnecessary risks (TPIA, data breaches, data deletion, availability issues after graduating/separating)

University Policy

- 04.01.01 - Security of Texas State Information Resources
- 04.01.05 - Network Use Policy
- 04.01.07 - Appropriate Use of Information Resources
- 04.01.10 - Information Security incident Management
- 04.01.11 - Risk Management of Information Resources
- 05.01.02 - University Surplus Property
- 04.01.02 - Identity and Access Management
- 05.02.06 - Acquisition of Information Technology Products and Services

Resource List

One Time Link: https://onetimelink.txstate.edu/

Secure File Transfer: https://securetransfer.txstate.edu/login

WebFiles: https://webfiles.txstate.edu

TxState VPN: https://remoteaccess.txstate.edu

Remote Desktop: https://itac.txstate.edu/support/remote-desktop.html

UPPS: http://infosecurity.txstate.edu/policies/uni_std_guides.html

Data Classification Guide:

http://infosecurity.txstate.edu/policies/uni_std_guides/data_classification.html

Disposal of Surplus Property UPPS No. 05.01.02:

http://www.txstate.edu/effective/UPPS/upps-05-01-02.html

Additional Information

Texas State Websites

- Information Security - http://infosecurity.txstate.edu
- Disposal of University Surplus Property UPPS No. 05.01.02 http://www.txstate.edu/effective/UPPS/upps-05-01-02.html

Contact Us

Information Security Office	**ITAC**
512-245-HACK (4225)	512-245-ITAC (4822)
infosecurity@txstate.edu	itac@txstate.edu

Contact us to host an online training for your team!