

Protecting Sensitive Digital Research Data

Table of Contents

1. Introduction.....	1
2. Required Practices.....	1
3. Information for Technical Staff.....	3
4. About this Initiative	3
5. Revision History	4
6. Approvals.....	4

1. Introduction

UT System has issued [rules](#) for all researchers to ensure that [sensitive digital research data](#) is appropriately protected. Protecting this important data requires a commonsense approach to managing your computer systems. You need to be aware of common vulnerabilities and then take some not-too-extraordinary steps to shield those vulnerable areas. The university has many people and tools available to support you in making this happen so you can go about your business.

Why should you take the time to secure your digital data? It's part of being a responsible researcher, just like using appropriate protocols and protecting human subjects. Your reputation and your funding are on the line. If your data is compromised, your research could be called into question. Following the university's new rules for protecting sensitive digital research data will help ensure the security of the systems involved and will help safeguard the confidentiality and integrity of sensitive digital research data.

Essentially, you are responsible for:

- Classifying your digital research data appropriately.
- Based on the classification of data, protecting the systems where the data is stored and how you transmit that data. This includes controlling how it is accessed and by whom.

2. Required Practices

Apply these basic practices to all systems.

Protecting Sensitive Digital Research Data

Document Version: Approved

- Classify your digital research data according to the [Data Classification Standard](#). The guidelines define the three levels of data classification, show you examples of how data can be at risk, and discuss the consequences of a data theft or system compromise. **If you have Category-I data, you are responsible for implementing the appropriate steps from the [Minimum Security Standards for Systems](#).**
- Ensure that you have installed anti-virus, anti-spyware, and firewall software, available at no additional cost from [BevoWare](#). Set your operating systems, security programs, and all other applications to check for updates regularly.
- Use secure services and applications when you are on any network, including:
 - Application-level security, such as HTTPS, SSH, and secure FTP.
 - The VPN when connecting to campus resources from off-campus. This protects your data between the off-site area and the campus network.
 - If you are using wireless, use the new campus wireless network, restricted.utexas.edu, which encrypts your data on the wireless portion of the network.
- Be a good data steward of [Category-I research data](#).
 - Ensure your systems have the [Minimum Security Standards for Systems](#).
 - Never use social security numbers as identifiers and ensure that you comply with the university's SSN policy.
- Identify professional personnel to manage research servers and IT resources. These experienced individuals can help you successfully comply with the minimum standards, including implementing such important practices as encrypting data and backing it up regularly. Check with [your department's IT personnel](#) or ask about [centralized support from ITS](#).
- Restrict virtual access to your data by using [EID-based authentication](#) to access computer systems, databases, Web applications, and more. You can also contact ITS for [programming assistance](#) if you do not have programmers available in your area.
- Ensure physical security for your systems
 - Lock workstations and use password-protected screen savers.
 - In the office, lock up portable devices (including laptops, PDAs, etc.) and media containing Category-I data.
 - When transporting portable devices, do not leave them unattended.
 - Use [a whole-disk encryption program](#) so that data cannot be accessed if systems are stolen.
 - Consult the [University of Texas Police Department Crime Prevention Unit](#) about how to secure labs.

- For new employees, make use of the [background check form](#) provided by Human Resources.
- You take precautions with your data and those precautions should extend to the information you store on your Smartphone using a MicroSD card.
 - Activate the [encryption function](#) in Windows Mobile. This should prevent any other phone from being able to see the files on your storage card.

3. Information for Technical Staff

Technical staff play an important role in protecting sensitive digital research data. The Information Security Office has tools and services that can help you support the researchers in your area implement the security practices that are essential on our campus.

Familiarize yourself with the [Information Resources Use and Security Policy](#). This document outlines requirements for many aspects of security systems. The policy also includes many supporting documents that provide specific details.

To see specific requirements and recommendations for systems storing Category-I, -II, and -III data, please see the [Minimum Security Standards for Systems](#).

The [Server Hardening Checklists](#) provide specific steps you should take to secure your servers. They reference the requirement in the Minimum Security Standards for Systems, provide notes about information specific to the university, and link to the Center for Internet Security documents for the relevant operating system.

E-mail the Information Security Office at security@utexas.edu if you have any questions or need more information.

4. About this Initiative

In response to data thefts at many universities, including The University of Texas at Austin, the UT System issued *Business Procedure Memorandum 75, Protecting the Confidentiality and Integrity of Digital Research Data*, in April, 2006, to protect the integrity of research at the university. The university is currently working on incorporating this standard into the Handbook of Operating Procedures.

President Powers has delegated responsibility for implementing BPM 75 to the Vice President for Research. The steering committee for the implementation includes representatives from these offices:

- Vice President for Research
- Chief Information Officer
- Vice President for Institutional Relations and Legal Affairs

[Memos from President Powers to Chancellor Yudof and to the Deans, Department Chairs, Directors of organized research units, and Researchers, regarding the university's plan to implement BPM 75.](#)

Protecting Sensitive Digital Research Data

Document Version: Approved

If you have questions about the information in this Web site or concerns about a particular system, please e-mail the Information Security Office at security@utexas.edu. For questions about research projects, please contact the [Office of the Vice President for Research](#).

(Effective April 12, 2007, UT System consolidated several Business Procedure Memoranda (53, 66, and 75) into a single policy with a new numbering scheme. The controlling document for this initiative is now [UTS 165](#).)

5. Revision History

Version	Date	New	Original
Protecting Sensitive Digital Research Data.docx	7/11/2011	Converted web page to PDF.	

6. Approvals

Name	Role	Members	Date
Cam Beasley	Information Security Officer		06/03/2006