ISO Information Security Office

The University of Texas at El Paso

Information Security Office

Protection of Sensitive Digital Research Data

Contents

Introduction.. 3

Required Practices.. 3

Information for Technical Staff.. 5

Revision History.. 5

Introduction

The University of Texas at El Paso has issued requirements 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 is 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 rules for *Protecting Sensitive Digital Research Data*[1] will help ensure the security of the systems involved and will help safeguard the confidentiality and integrity of sensitive digital research data.

Required Practices

Apply these practices to all systems.

Classify your digital research data according to the Standard 9: Data Classification Standard. The standards define the three levels of data classification and shows examples for each of the three levels, as well as alternate methodology for classifying data. Consequences of data theft or system compromise for Confidential data include but are not limited to potential long-term loss of research funding from granting agencies; long-term loss of reputation (published research called into question due to data being unreliable); unauthorized tampering of research data; increase in regulatory requirements (long-term loss of critical campus or departmental service); and individuals put a risk for identity theft.

Any system containing Confidential or Controlled data must have a security assessment performed by the ISO. Please contact security@utep.edu to schedule the assessment.

[1] Adapted, in whole or in part, from “Protecting Sensitive Digital Research Data” (https://security.utexas.edu/policies/sensitive_research), with permission from ITS, The University of Texas at Austin, Austin, Texas 78710-1110

If you have Confidential and/or Controlled data, you are responsible for implementing the appropriate steps from the Minimum Security Standards for Systems.

- Ensure that anti-virus and firewall software is installed, enabled and configured to update signatures at least daily.
- Set 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 Virtual Private Network (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 campus wireless network, on the wireless portion of the network. Please be sure to log in through VPN to insure that your data is encrypted when communicating to your server.
- Be a good data steward of confidential research data.
  - Ensure systems comply with the Minimum Security Standards for Systems.
  - Never use social security numbers as identifiers and ensure that you comply with the University's Standard 13: Use and Protection of Social Security Numbers, as well as federal and state law.
- 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 Enterprise Computing.
- Monitor and maintain documentation on the integrity of that Digital Research Data (i.e., that the Data has not been altered by either intent or accident).
- Ensure appropriate backup and retention of that Digital Research Data.
- Restrict virtual access to data by using Miners credentials for authentication to access computer systems, databases, Web applications, and more. This includes controlling and documenting how it is accessed and by whom.
- Ensure physical security for systems are in place:
  - Lock workstations and use password-protected screen savers.
  - In the office, lock windows, file cabinets and office doors.
  - When transporting portable device, do not leave them unattended.

  - Use whole-disk encryption so that data to preclude unauthorized access should the device be lost or stolen.
  - Secure labs.
  - Consult the UTEP Police Department Crime Prevention Unit about how to secure labs.

- As precautions are taken to protect data, so should those precautions be extended to the information stored on smartphones and other devices.
  - Activate the encryption function on supported version of Apple iOS, Blackberry OS and Android.

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 UTEP 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 seek specific requirements and recommendation for systems storing Confidential, Controlled, or Published data, please refer to the Minimum Security Standards for Systems.

The Server Hardening Checklists provide specific steps to take to secure the 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.

Email the Information Security Office at security@utep.edu if you have any questions or need additional information.

Revision History

First Draft:	February 4, 2008
Revised:	May 23, 2017 (update content and links as necessary)
Approved:	May 23, 2017
	Gerard D. Cochrane Jr., Chief Information Security Officer