Top Information Security Concerns for Researchers

Last reviewed: June 2017

Related Resources:

- **Top Information Security Concerns for Campus Executives & Data Stewards**
- **Top Information Security Concerns for HR Leaders & Process Participants - Protecting Your HR Assets**

Top Information Security Concerns for Researchers: *Protecting Your Intellectual Assets*

For the purpose of this resource, the term research includes any work done as part of a grant, contract, or independent agreement unless specifically noted.

Do Researchers know:

1. What/Where is my research data?

a. Do I know what comprises the data created by my research activity? Do I have an accurate inventory of it?
b. Who owns the data created by my research activity? As a grantee, do I collect, store, process, transmit or use information on behalf of a federal agency (e.g., Veterans Administration (VA), Health and Human Services (HHS))?
c. Does my research data reside in institutional / departmental data centers? Does my research reside in personally owned devices?
d. Will my research data be transmitted over a wired, wireless, or cellular network? (i.e., what methods are being used to encrypt or otherwise protect the data in transit?)
e. Will my research data be stored on a portable device or removable media? Where will the device or media be stored and used?
f. Is my research data being backed up? By whom? To what location and how often? How are the backup copies secured? Are the backup copies encrypted?

RESOURCES

- Asset and Data Management - Information Security Guide chapter
- Information Security Governance - an EDUCAUSE resource

Top of page

2. How sensitive is my research data?

a. Am I familiar with my institution's data classification policy? Have I classified my research according to confidentiality and integrity requirements?
b. Does my research include information that can be used to distinguish or track an individual's identity such as name, Social Security Number, or biometric information as well as information that could be used in conjunction with other data elements to reasonably infer the identity of a subject such as a combination of gender, race, date of birth, geographic indicators, or other descriptors?
c. Is my research activity subject to the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), to Federal Information Security Management Act (FISMA) or other regulatory controls? If so, what are my responsibilities?
d. Is my research activity subject to Export Administration Regulations (EAR) or International Traffic in Arms Regulations (ITAR)? If so, what are my responsibilities?
e. How do export controls affect my research activity? How do I comply with the regulations?

RESOURCES

- Data Classification Toolkit
- Risk Management Framework
- Guidelines for Data De-Identification or Anonymization

Top of page

3. Why should I care?

a. What are the expectations of my granting agencies/sponsors regarding the release of data that include confidential or sensitive information (e.g., personally identifiable information (PII), medical history of human subjects, or locations of endangered species)?
b. How can I as Researcher fulfill the expectation to share with other researchers, through the process of Peer Review, data, samples, and other research supporting materials within legal constraints and in accordance with applicable standards for protecting privacy rights and confidentiality of subjects?
c. Am I aware of the potential threats to my research data? Some lurking examples:

- Tampering or theft of intellectual property or government-sponsored/secret research
- Alteration, damage, or loss of sensitive research data
- Unauthorized access or use of sensitive research data
- Improper disposal of digital media containing sensitive research data
- Sharing passwords and/or system access codes
- Unauthorized release of sensitive research data or product information, on or off the campus

d. Am I aware of the civil and criminal penalties for the unlawful export and disclosure of export-controlled information?

RESOURCES

- National Institute of Health (NIH) Data Sharing Policy
- National Science Foundation (NSF) Data Sharing Policy & Data Management Plan Requirements
- National Science Foundation Data Management and Sharing Frequently Asked Questions (FAQs)

Top of page

4. What are my legal and contractual obligations?

Research and research data may be impacted by the following regulations:
a. Family Educational Rights and Privacy Act, 20 U. S. C. § 1232g
b. Health Insurance Portability and Accountability Act (HIPAA)
c. Personal Data Privacy and Security Act
d. FDA 21 CFR Part 11 Electronic Record; Electronic Signatures; Final Rule
e. Higher Education Opportunity Act of 2008 (HEOA)
f. Federal Information Security Management Act (FISMA)
g. International Traffic in Arms Regulations 2011 (ITAR)
h. Export Administration Regulations (EAR)
i. NIST 800-171
j. State Security Incident Notification Laws

RESOURCES

- Compliance Management - Information Security Guide chapter
- Higher Education Compliance Alliance Compliance Matrix
- An Introduction to NIST Special Publication 800-171 for Higher Education Institutions

Top of page

5. Who's responsible for securing my research data?

a. Who is accountable for protecting the confidentiality and integrity of research data at my institution?
b. Who is accountable for protecting the confidentiality and integrity of research data in a collaborative environment that may belong to other institution or agency?
c. Do I know who is my institution's Chief Information Security Officer (CISO/ISO)? Do I know his/her role and responsibilities regarding my research data?
d. Am I including an information security budget (i.e., technology, services, and staff) in my grant applications to ensure I have enough funds to properly secure the data? Who can assist me with technology options and cost?
e. If regulatory compliance (e.g., FISMA) is required, is my institution's CISO involved early in the grant application process? Are the requirements for compliance (i.e., what it would take to become compliant) clearly understood?
f. Does my research require a Technology Control Plan (TCP), Sensitive Data Control Plan, or written plans documenting the procedures that will be utilized to protect my research data?
g. Do I need to conduct annual reviews of technology control plans for sensitive research projects? Myself or in collaboration with my CISO?
h. Does any data residing on removable media require confidentiality? If so, how is this data being encrypted? What steps are being taken to ensure that the data is recoverable in the event that an encryption key is lost or forgotten?
i. Do I know whether my research data is being targeted for attack/unauthorized access? Do my research team and system administration know? Who can assist me with finding out?
j. Are my system administrators appropriately trained to secure my data? Do they rely on professional IT support staff to properly manage and encrypt the systems hosting my research data?

RESOURCES

- Security Program Development - Information Security Guide chapter
- Confidential Data Handling Blueprint

Top of page

6. Who has access to my research data?

a. Who approves access to research data and who provides the access? Is it granted based on a documented process or ad-hoc?
b. How is remote access to research data by external collaborators managed?
c. Does my research data have export control or foreign national access restrictions? If so, how am I managing local and remote access to that data by foreign nationals??
d. If my research data reside in personally-owned devices, what rights does my institution have to those devices (e.g., electronic (e)discovery)?

RESOURCES

- Identity and Access Management - Information Security Guide chapter
- Organizational Security Awareness - Information Security Guide chapter

Top of page

7. Is my research data safe in the cloud?

a. Are free cloud storage services truly free? Are they suitable for research data? What are the risks and the costs
b. Does my institution have any preferred cloud service providers? How does the third-party safeguard customer data?
c. Do contractual provisions and/or licensing agreements warrant data safeguards?
d. Does the cloud service provider store data outside of my country?
e. Does the cloud service provider have a reasonable mechanism for retrieving data once I no longer require their services or they go out of business?

RESOURCES

- Cloud Computing Security
- Cloud Data Storage Solutions
- Vendor and Third-Party Management - Information Security Guide chapter

Top of page

8. What if I travel?

a. What devices do I need to be concerned about? (e.g., laptop, smartphone, mobile storage devices/thumb drives, etc.) Should I use my laptop or get an institutional loaner?
b. What data should I be concerned about taking with me? Trade secrets, proprietary information export-controlled technical data or information?
c. Does my research involve export-controlled data?
d. Does full disk encryption provide enough protection? Can I decline to provide the password if asked for it by a customs or government official?

RESOURCES

- Security Tips for Traveling Abroad

Top of page

9. How long do I need to keep my research data?

Granting agencies will require researchers who submit grant proposals to include an appendix that describes plans for the management of research data. Specific requirements of a data management plan will vary from agency to agency but the following are common requirements: Type of data created, collection methodology, backup, storage, and preservation, access policies, and security provisions to ensure confidentiality and integrity.

RESOURCES

- University of Minnesota Funding Agency and Data Management Guidelines
- Records Retention and Disposition Toolkit

Top of page

10. What if my research data gets into the wrong hands?

a. Does my institution have a Security Incident Notification policy and process?
b. Do I know when to get legal affairs and law enforcement involved?
c. Would I know when and who to notify?
d. Would I know how to notify impacted individuals?
e. Am I aware of the adverse impact of a security incident/breach? Some examples:

- Increased legal liability
- Loss of revenue, grants, gifts, and donations
- Loss of data, information resources related assets, and productivity
- Injury to Researcher and UT Institution reputation, bad publicity
- Loss of public trust
- Default on project(s)
- Increased regulation, sanctions and/or legislation

RESOURCES

- Incident Management and Response - Information Security Guide chapter.
- Data Incident Notification Toolkit
- Incident Checklist

Top of page

Questions or comments? Contact us.