Secure UD Managing Research Data Risks

All data, including research data, carries risk. Although risk management probably isn't the primary focus of your research efforts, it's an important step in helping your project stay on track and avoiding penalties.

You can use the information in this guide to inform your data management and security plans. You can also contact IT Security (secadmin@udel.edu) for a consultation about managing the risks to your project. For more information, explore the resources available on the **Secure UD website: www.udel.edu/security/research**

CONFIDENTIALITY RISKS: Will your project involve any data that has restrictions on who can view or access it?

Do you have any data that...

❑ can only be disclosed to authorized parties?
❑ is required by law, regulation, or contract to remain confidential?
❑ may not be published or made public until authorized by a funding agency?
❑ is sensitive by nature and would have a negative impact if disclosed?
❑ would be valuable to hackers, corporate spies, foreign intelligence, etc.?

The big picture: Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.

If you do, then...

- encrypt the data at rest and in transit
- control access to the data[1]
- physically secure devices and paper documents
- securely dispose of unneeded data and devices
- acquire data only as needed
- use data only as needed
- manage devices[2]

INTEGRITY RISKS: Will your project involve any data that, if not maintained with integrity, would significantly impact the accuracy or feasibility of the study?

Do you have any data that...

❑ must remain accurate and uncorrupted?
❑ must only be modified by certain individuals or in a controlled manner?
❑ must come only from trusted sources?

The big picture: Data integrity is about protecting data against improper maintenance, modification, or alteration. It includes data authenticity.

If you do, then...

- back up the data
- control access to the data[1]
- log data access and changes
- use hashing to check file integrity
- perform data verification and validation

AVAILABILITY RISKS: Will your project involve any data that, if lost, stolen, or destroyed, would be irreplaceable or would significantly impact the feasibility of the study?

Do you have any data that...

❑ must remain available or accessible during the project?
❑ must remain available or accessible after the project is complete?
❑ cannot be easily re-obtained or re-created?

The big picture: Data availability is about the timeliness and reliability of access to and use of data. It includes data accessibility.

If you do, then...

- back up the data
- inventory the data
- use metadata to identify and describe data
- manage record retention
- securely dispose of unneeded data and devices
- arrange for data publication and curation

Notes

[1] Controlling access to data includes: authorizing access based on "need to know," uniquely identifying and authenticating users, using two-factor authentication (2FA) where practical, setting roles and permissions for access, and periodically reviewing access.

[2] Managing devices includes: using anti-virus software, routinely patching software, whitelisting applications, using device passcodes, suspending inactive sessions, enabling firewalls, and using whole-disk encryption.

PHYSICAL ASSET RISKS: How will you manage devices and paper documents containing project data?

Physical assets include...

- □ Desktop and laptop computers
- □ Mobile devices (smartphones and tablets)
- □ Servers
- □ Removable storage media
- □ Paper documents

The big picture: Every project involves some number of physical assets necessary for project activities. All of these assets facilitate the completion of your project, but they and the data they contain must be managed and protected appropriately.

If you do, then...

- manage devices[2]
- control access to the devices/data[1]
- physically secure devices and paper documents
- securely dispose of unneeded data and devices
- prohibit the use of unsecured personal devices

PRIVACY RISKS: Will your project involve any data that, either by itself or in combination with publicly available information, has the potential to violate privacy expectations of individuals?

Do you have any data that...

- □ involved human subjects?
- □ has explicit legal or regulatory privacy protection requirements?
- □ is sensitive, or has the potential to be sensitive if combined with other information?

The big picture: Data privacy is about respecting individuals' reasonable expectations to be free from unreasonable observation and excessive collection or use of personal data (what is being observed and collected and how it is being used).

If you do, then...

- de-identify or aggregate data where appropriate
- provide fair notice of monitoring, data collection, and/or data usage
- see the recommendations for confidentiality risks on the other side of this resource

LEGAL, REGULATORY, AND CONTRACTUAL RISKS: Will your project involve any data that is subject to legal, regulatory, or contractual requirements?

Do you have any data that...

- □ is subject to laws or regulations (e.g., FERPA, HIPAA, COPPA)?
- □ is provided to you under a contract or agreement?
- □ is subject to grant or contract restrictions or security requirements?

The big picture: Data laws and regulations govern the handling of particularly sensitive kinds of information and may present the risk of fines, funding loss, or even imprisonment. Health data, education records, defense articles, and other data present legal and regulatory risk that goes hand-in-hand with other risks like confidentiality, privacy, human, etc.

Sponsored research agreements may specify data security standards and requirements that must be followed during or after the study. Data contracts may govern how data from a particular source or generated by a particular contract can be used or what rights researchers acquire to that data.

If you do, then...

- be aware of relevant laws, regulations, and contract requirements and how they apply to your data
- include requirements in your data management plan
- consult General Counsel or IT if you have compliance questions

HUMAN RISKS: Is every member of your team, including you, aware of data risk and security?

Is your team...

- □ aware of their responsibility for security?
- □ aware of security best practices?
- □ watchful for unusual behavior that may indicate data theft?

The big picture: Human risk includes human vulnerability to social engineering, awareness of security practices, and insider threats.

If not, then...

- sign up for Secure UD Training
- discuss security with your team and make it integral to your project
- consult IT if you have questions