University of Delaware

Secure UD Research Security Plan

|  |  |
| --- | --- |
| Project name | Click here to enter text. |
| Project start/end dates | Click here to enter text. |
| Principal investigator | Click here to enter text. |
| Project team members | Click here to enter text. |

Data is central to research, innovation, and opportunity. Data—and the risks inherent in its use—must be managed in order to realize its potential.

This tool is designed to (1) identify key controls available to you to manage your data risk and (2) enable you to easily and thoroughly document your project’s risk-driven data security plan by answering a series of questions grouped by risk type. **Not all controls will apply to every project.** As the principal investigator, you determine which controls to implement based on your data needs, applicable regulations, and funding agency or data provider agreements.

# Project Summary

Briefly describe your project, including the data sets involved and their relative classifications.

In some cases, especially when an outside agency provides the data, classifications may already be defined (e.g., confidential, top secret). If no other agency has classified the data, you may use the University’s information classifications to describe the sensitivity of your project data:

* Level I—Low Risk
Information that is intended for public distribution or that has low confidentiality risks.
* Level II—Moderate Risk
Information that is neither Level I nor Level III; information with moderate confidentiality risks.
* Level III—High Risk
Information that is highly sensitive; information with significant confidentiality risks.

Click here to enter text.

# Physical Asset Risk

Every project involves some number of physical assets necessary for project activities. These assets can include:

* desktop and laptop computers
* mobile devices (smartphones and tablets)
* servers
* removable storage media
* paper documents.

All of these assets facilitate the completion of your project, but they and the data they contain must be managed and protected appropriately.

## Risk management plan

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Members of the project team are prohibited from using personal devices for project activities. | [ ]  Yes | [ ]  No | [ ]  N/A |
| a. | If no, describe how the security of personal devices and project data is ensured. |  |  |  |
|  | Click here to enter text. |  |  |  |

### Computer management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2. | Computers used for project activities are centrally managed (i.e., by UD central IT or departmental IT staff). | [ ]  Yes | [ ]  No |  |
| a. | If no, describe how computers are managed (e.g., by the project team or a third party, by using a software solution). |  |  |  |
|  | Click here to enter text. |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3. | Computers used for project activities have a standard configuration. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4. | Computers used for project activities have separate user and administrator accounts. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5. | Computer administrator account access is granted only to authorized individuals with a project- or system-related need for privileged access. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6. | Computers used for project activities have only the minimum functionality necessary for those project activities (e.g., no additional software or services unrelated to the project). | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 7. | Computers used for project activities have current (vendor-supported) versions of operating systems and software. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8. | Computers used for project activities have firewalls enabled. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 9. | Computers used for project activities have University-provided anti-virus software installed. | [ ]  Yes | [ ]  No |  |
| a. | Computers used for project activities have University-provided advanced anti-virus software (Cylance) installed. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 10. | Computers used for project activities have appointed local support providers (individuals responsible for providing technical services to support the device and its users). | [ ]  Yes | [ ]  No | [ ]  N/A |

Other comments

Click here to enter text.

### Mobile devices

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 11. | Mobile devices used for project activities have a standard configuration. | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 12. | Mobile devices used for project activities have only the minimum functionality necessary for those project activities (e.g., no additional software or services unrelated to the project). | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 13. | Mobile devices used for project activities have current (vendor-supported) versions of operating systems and software. | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 14. | Mobile devices used for project activities have appointed local support providers (individuals responsible for providing technical services to support the device and its users). | [ ]  Yes | [ ]  No | [ ]  N/A |

Other comments

Click here to enter text.

### Server management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 15. | Servers used for project activities are centrally managed (i.e., by UD central IT or departmental IT staff). | [ ]  Yes | [ ]  No | [ ]  N/A |
| a. | If no, describe how servers are managed (e.g., by the project team or a third party, by using a software solution). |  |  |  |
|  | Click here to enter text.  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 16. | Servers used for project activities have a standard configuration. | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 17. | Servers used for project activities have appointed administrators. | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 18. | Server administrator account access is granted only to authorized individuals with a project- or system-related need for privileged access. | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 19. | Servers used for project activities have only the minimum functionality necessary for those project activities (e.g., no ports or services unrelated to the project). | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 20. | Servers used for project activities have current (vendor-supported) versions of operating systems and software. | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 21. | Servers used for project activities log system and security events. | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 22. | Servers used for project activities are protected by firewalls. | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 23. | Servers used for project activities are protected by intrusion detection systems or intrusion prevention systems (IDS/IPS). | [ ]  Yes | [ ]  No | [ ]  N/A |

Other comments

Click here to enter text.

### Storage media management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 24. | Devices and media containing project data are physically secured against theft and unauthorized access (e.g., through storage in locked areas). | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 25. | Paper documents containing project data are physically secured against theft and unauthorized access (e.g., through storage in locked areas). | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 26. | Project data is prohibited from being stored on removable storage media (e.g., external hard drives, flash drives). | [ ]  Yes | [ ]  No |  |
| a. | If no, describe how use of removable storage media is managed to prevent unnecessary proliferation or loss of project data. |  |  |  |
|  | Click here to enter text. |  |  |  |

Other comments

Click here to enter text.

# Confidentiality Risks

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

Confidentiality risks apply if your project includes data that has restrictions on who can view or access it. For example, if your project includes data that…

* can only be disclosed to authorized parties.
* is required by law, regulation, or contract to remain confidential.
* is sensitive by nature and would have a negative impact if disclosed.
* would be valuable to hackers, corporate spies, foreign intelligence, etc.

## Risk management plan

### Data access

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Access to project data is managed by the project team. | [ ]  Yes | [ ]  No |  |
| a. | Describe who is responsible for managing access to project data (including the name of the project team member or third party). |  |  |  |
|  | Click here to enter text. |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2. | Access to project data is granted only to authorized individuals with a project-related need for access. | [ ]  Yes | [ ]  No |  |
| a. | If no, describe which other individuals or organizations are granted access, the data they can access, and the reason for their access. |  |  |  |
|  | Click here to enter text. |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3. | Access to project data is granted only to the extent (privileges and amount of data) required to fulfill project needs. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4. | Access to project data is promptly revoked when no longer necessary or at the conclusion of the project. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5. | Authentication using unique individual identifiers is required to access project data. | [ ]  Yes | [ ]  No |  |
| a. | If yes, describe which systems authenticate access (e.g., the University’s Central Authentication System [CAS], Shibboleth, or a third-party authentication system) and to which data. |  |  |  |
|  | Click here to enter text. |  |  |  |

Other comments

Click here to enter text.

### Encryption

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6. | Sensitive project data is encrypted at the file level while at rest (in storage and not in use). | [ ]  Yes | [ ]  No | [ ]  N/A |
| a. | If no, describe how sensitive project data is protected while at rest. |  |  |  |
|  | Click here to enter text. |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 7. | Devices containing project data are encrypted using whole-disk encryption. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 8. | Sensitive project data is transmitted securely (e.g., it is transmitted through secure connections or portals, or files containing project data are encrypted prior to transmission). | [ ]  Yes | [ ]  No | [ ]  N/A |
| a. | If no, describe how sensitive project data is protected while in transmission. |  |  |  |
|  | Click here to enter text. |  |  |  |

Other comments

Click here to enter text.

# Integrity Risks

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

Integrity risks apply if your project includes data that, if not maintained with integrity, would significantly impact the accuracy or feasibility of the study. For example, if your project includes 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.

## Risk management plan

### Data integrity functions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Hashing functions are used to check file integrity. | [ ]  Yes | [ ]  No |  |

Other comments

Click here to enter text.

### Logging

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2. | Access to project data is logged. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3. | Logs are reviewed if a suspected or actual IT security incident is identified. | [ ]  Yes | [ ]  No |  |

Other comments

Click here to enter text.

# Availability Risks

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

Availability risks apply if your project includes data that, if lost, stolen, or destroyed, would be irreplaceable or would significantly impact the feasibility of the study. For example, if your project includes 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.

## Risk management plan

### Backups

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Data is backed up. | [ ]  Yes | [ ]  No |  |
| a. | If yes, describe briefly the backup plan. If no, describe why data is not backed up. |  |  |  |
|  | Click here to enter text. |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2. | Backups are periodically tested and verified. | [ ]  Yes | [ ]  No | [ ]  N/A |

Other comments

Click here to enter text.

### Accessibility after project

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4. | Devices containing project data are securely erased or destroyed when no longer needed. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5. | Paper documents containing project data are shredded when no longer needed. | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6. | Some or all project data is disposed of after project completion. | [ ]  Yes | [ ]  No |  |
| a. | If yes, describe briefly which data is disposed of, at what time, and whether by a specific process. |  |  |  |
|  | Click here to enter text. |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 7. | Some or all project data must be retained after project completion. | [ ]  Yes | [ ]  No | [ ]  N/A |
| a. | If yes, describe briefly which data must be retained, for how long, and in which system. |  |  |  |
|  | Click here to enter text. |  |  |  |

Other comments

Click here to enter text.

# Privacy Risks

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).

Privacy risks apply if your project includes data that, either by itself or in combination with publicly available information, has the potential to violate privacy expectations of individuals. For example, if your project includes data that…

* involves human subjects.
* has explicit legal or regulatory privacy protection requirements.
* is sensitive, or has the potential to be sensitive if combined with other information.

Privacy risks apply to projects involving human-related data, such as data related to individuals’ behavior, medical records, or learning patterns. **Some projects may not involve data with privacy-related risks.**

## Risk management plan

### Data collection and creation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Only data necessary to the project is collected or created. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2. | Informed consent statements are collected from research participants. | [ ]  Yes | [ ]  No | [ ]  N/A |

Other comments

Click here to enter text.

### Data utilization

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3. | Data is de-identified or aggregated. | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4. | Data is utilized only as necessary for project activities and only as relevant to the project purpose (e.g., no use of data for administrative voyeurism). | [ ]  Yes | [ ]  No |  |
| a. | Describe briefly how data utilization is managed. |  |  |  |
|  | Click here to enter text. |  |  |  |

Other comments

Click here to enter text.

# Legal, Regulatory, and Contractual Risk

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.

Legal, regulatory, and contractual risks apply if your project is funded under certain grant requirements or if it includes data that is subject to legal, regulatory, or contractual requirements. For example, if your project includes data that…

* is subject to laws or regulations (e.g., FERPA, HIPAA, COPPA).
* is provided under a contract or agreement.
* is subject to grant or contract restrictions or security requirements.
* may not be published or made public until authorized by a funding agency.

## Risk management plan

### Applicable laws and regulations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Project data is subject to the requirements of |  |  |  |
| a. | Children’s Online Privacy Protection Rule (COPPA) | [ ]  Yes | [ ]  No |  |
| b. | Family Education Rights and Privacy Act (FERPA) | [ ]  Yes | [ ]  No |  |
| c. | Federal Policy for the Protection of Human Subjects (Common Rule) | [ ]  Yes | [ ]  No |  |
| d. | Health Insurance Portability and Accountability Act (HIPAA) | [ ]  Yes | [ ]  No |  |
| e. | NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations | [ ]  Yes | [ ]  No |  |
| f. | Other (specify). | [ ]  Yes | [ ]  No |  |
|  | Click here to enter text. |  |  |  |

Other comments

Click here to enter text.

### Third parties and contracts

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2. | The project utilizes cloud-based services (e.g., vendor-provided software, infrastructure, platforms, or storage as a service). | [ ]  Yes | [ ]  No |  |
| a. | If yes, briefly describe the services, including vendor names and purpose of the services. |  |  |  |
|  | Click here to enter text. |  |  |  |
| b. | If yes, cloud vendor security controls are assessed (in partnership with IT) to ensure that vendors satisfy security standards and requirements for project data. | [ ]  Yes | [ ]  No | [ ]  N/A |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3. | Responsibility for project data or systems is shared with third parties (including other organizations, researchers at other institutions, and vendors providing cloud services). | [ ]  Yes | [ ]  No |  |
| a. | If yes, describe how the boundaries of responsibility between all parties are defined and managed (e.g., through written contracts). |  |  |  |
|  | Click here to enter text. |  |  |  |

Other comments

Click here to enter text.

### Funding agency requirements

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4. | Project data must remain accessible after the project is complete. | [ ]  Yes | [ ]  No |  |
| a. | If yes, describe those requirements. |  |  |  |
|  | Click here to enter text. |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5. | Project data must be made accessible in a specific format. | [ ]  Yes | [ ]  No |  |
| a. | If yes, describe those requirements.  |  |  |  |
|  | Click here to enter text. |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6. | Project data may not be published without approval by a funding agency. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 7. | Project data must be transmitted in compliance with external (e.g., funding agency, regulatory) requirements. | [ ]  Yes | [ ]  No |  |
| a. | If yes, describe those requirements. |  |  |  |
|  | Click here to enter text. |  |  |  |

Other comments

Click here to enter text.

# Human Risks

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

Human risks apply to every project. Every member of your project team must be aware of data risk and security. For example, your project team must be...

* aware of their responsibility for security.
* aware of security best practices.
* watchful for unusual behavior that may indicate data theft.

## Risk management plan

### Training

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Every member of the project team is made aware of the project’s data management and security plans. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 2. | Every member of the project team is made aware of the classifications of project data. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 3. | Every member of the project team is required to complete Secure UD Training prior to handling data. | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4. | Every member of the project team is aware of the need to report suspicious behavior (e.g., excessive duplication of data that may indicate data theft). | [ ]  Yes | [ ]  No |  |

Other comments

Click here to enter text.

### Personnel management

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5. | Every member of the project team is required to attest in writing to their data and security responsibilities (e.g., via the Secure UD End User Acknowledgement). | [ ]  Yes | [ ]  No |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6. | Contract employees (non-UD personnel) are required to sign the Secure UD Contractor Confidentiality Agreement. | [ ]  Yes | [ ]  No | [ ]  N/A |

Other comments

Click here to enter text.