Secure UD

Data Governance
&
Security Program

Official business use only
Version 1.10

University of Delaware Information Technologies
IT Security

For official University of Delaware business use only.
Document content is subject to official University approval.
This resource is for informational purposes only and is currently recommended by UD Information Technologies to meet a standard of due care for managing risks to IT resources.

The most current version of this document is available online:
https://www1.udel.edu/security/framework/isp/

Version 1.10
Last updated: 28 Feb. 2018

The Secure UD Data Governance & Security Program is developed and maintained by:

UD Information Technologies
IT Security

192 South Chapel Street
Newark, DE 19716

secadmin@udel.edu

Non-Discrimination Statement
The University of Delaware is an equal opportunity/affirmative action employer and Title IX institution. For the University's complete non-discrimination statement, please visit www.udel.edu/aboutus/legalnotices.html.

Attribution
The Secure UD Data Governance & Security Program (Secure UD DGSP) is a derivative of The Ohio State University's Information Security Standard and Information Security Control Requirements, used under CC BY-SA. The Secure UD DGSP is licensed under CC BY-SA.

PDF Optimization
This document has been optimized for digital use in PDF format. It includes clickable links in the header tabs and content.

Executive Summary

Information security and risk management are fundamental to the success, safety, and reputation of the University, its assets, and its community. The University has an obligation to appropriately manage its risks consistent with its strategies, missions, and vision.

The Secure UD Data Governance & Security Program (Secure UD DGSP) is the blueprint for the security and risk management of the University's information technology (IT) resources, including its data, systems, and network. It draws from leading security models in higher education and federal standards published by the National Institute of Standards and Technology (NIST) to create a foundation for broader legal and regulatory compliance.

The Secure UD DGSP establishes the University's information risk management framework and requires understanding and active participation from all end users of IT resources. The Secure UD DGSP is built upon the premise that information risk management is an organizational issue, not exclusively an IT issue. It mandates clear administrative, operational, and technical requirements for IT resource management. These requirements guide the uniform implementation of security controls and generate measurable compliance. Supplemental assessment tools ensure simplicity and consistency of reporting, tracking, and auditing.

This document is intended for reference by University executive leadership and general use by unit heads and unit technical staff. All end users are responsible for complying with their unit's requirements for implementing the Secure UD DGSP.

Table of Contents

Figures & Tables

Introduction

Information security and risk management help ensure that the missions of the University—teaching, research, and service—can be realized. They identify the requirements for protecting University information to limit financial, reputational, legal, operational, and other risks to the University and individuals. While information security and risk management cannot guarantee the success of the University, their absence increases the risk of failure.

The Secure UD Data Governance & Security Program (Secure UD DGSP) is designed to manage institutional information technology (IT) and information-related risk by establishing mandates for unit heads and local support providers to coordinate the protection of IT resources within their units.[1]

All end users of IT resources are responsible for understanding and complying with their unit's requirements for implementing the Secure UD DGSP.[2]

Context of the Secure UD DGSP

UD Information Technologies is authorized by University Information Security Policy, to develop, promulgate, and enforce information security program requirements as an extension of policy. Included in these requirements are the set of administrative, operational, and technical controls for information security and risk management at the University.

The Secure UD DGSP is built upon the premise that information risk management is an organizational issue, not exclusively an IT issue. This framework requires active participation in information security across the University. Each University unit is responsible for complying with the requirements of the Secure UD DGSP. Not all requirements are applicable to every unit.

Objectives of the Secure UD DGSP

The Secure UD DGSP is designed to accomplish five core objectives:

1. Establish a University information security program.
2. Establish information risk management objectives.
3. Assess risk to IT resources.
4. Establish security standards and controls.
5. Guide evaluation and management of information risk.

Each objective is central to establishing, maintaining, and improving the University's information security posture. By combining these objectives with actionable requirements and evaluations, the Secure UD DGSP provides a comprehensive plan for managing IT and information-related risk.

Objective 1: Establish a University information security program

The first function of the Secure UD DGSP is to establish a University-wide information security program. The Secure UD DGSP provides the organizational framework; administrative, operational, and technical security controls; and supplemental tools to establish, maintain, and improve the University's information security posture.

1 Roles and responsibilities are addressed in "Roles and Responsibilities" (p. 14).
2 It is not anticipated that end users will reference this document unless they fulfill a managerial or technical role within their unit. The mandate to understand and comply with Secure UD DGSP requirements may be fulfilled through unit security education and clear unit security requirements.

Additionally, the Secure UD DGSP draws from leading security models in the higher education industry and federal standards published by the National Institute of Standards and Technology (NIST) to create a foundation for broader legal and regulatory compliance.

Objective 2: Establish information risk management objectives

The Secure UD DGSP details 25 risk management objectives across 10 risk areas. These risk management objectives—informed by industry and federal risk management frameworks—address critical security considerations.

Each risk management objective maps to a set of security standards and controls that provide the administrative, organizational, and technical requirements for compliance. Security controls in the Secure UD DGSP reference parallel security and privacy controls in the National Institute for Standards and Technology (NIST) Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations.

By systematically achieving the prescribed security controls, the University strengthens its security posture and realizes its risk management objectives.

Objective 3: Assess risk to IT resources

Because of the breadth and depth of its data processing, the University is a target for hackers. IT resources—which include both University information and the IT devices involved in accessing, processing, storing, and transmitting it—must be protected to limit risks to the University, individuals, other organizations, and the nation.

The Secure UD DGSP is designed to facilitate assessments of the risk posed to University IT resources by threats in the complex information security landscape. These assessments establish the foundation for the Secure UD DGSP's operation and provide the metrics for its continual evaluation.

Objective 4: Establish security standards and controls

The Secure UD DGSP establishes clear security standards for IT resource security. These requirements guide the uniform implementation of administrative, operational, and technical security controls.

Units are granted considerable autonomy to identify and implement security controls. Each unit is responsible for identifying which security controls are applicable to its information needs and ensuring that all applicable security controls are implemented to protect the unit's IT resources.

Reporting requirements and accountability are, where specifically managed, detailed in the security control requirements.

Objective 5: Guide evaluation and management of information risk

The Secure UD DGSP requires each University unit to regularly assess its security posture. The Secure UD DGSP's companion assessment tools are based on the security standards and controls required by the Secure UD DGSP itself. Risk areas and risk management objectives help focus these assessments on defined risks relevant to the University's administration, operation, and technology.

The Secure UD DGSP also facilitates the development of unit information security plans, which define and organize unit security efforts, and risk management strategies, which project unit goals for risk management and policy compliance.

Secure UD Policy

The Secure UD DGSP is part of a larger information security and risk management framework, the Secure UD policy. Based on threats and risks to the University and its IT resources, Secure UD policy is comprised of:

1. IT policies
2. The Secure UD DGSP

IT also provides supporting tools and guidance to assist units in assessing and improving their security practices within the context of their operations.

Together, these components enable the University to consistently organize, measure, and manage information risk across the institution.

IT policies

Three policies form the foundation of the University's information security and risk management framework:

1. University Data Governance Policy
2. University Information Security Policy
3. University Information Classification Policy

The University Data Governance Policy defines the University's data management and governance framework, including information management roles and responsibilities.

The University Information Security Policy empowers IT to develop, implement, and maintain the Secure UD DGSP as the list of administrative, operational, and technical requirements for the security of IT resources.

The University Information Classification Policy defines the three University information classifications and requires that all University information be classified to facilitate the consistent and appropriate application of security standards and controls.[1]

The Secure UD DGSP

The Secure UD DGSP organizes risk according to a risk management model and prescribes security standards and controls for appropriately managing risk.

Risk management model

There are four layers to the risk management model, illustrated in Figure 1 (p. 11):

1. Risk areas—Broad groups of IT and information-related risks posed to the University
2. Risk management objectives—Specific goals for managing and mitigating information-related risk to the University
3. Security standards—Requirements for achieving information risk management objectives and compliance with laws, regulations, and policies
4. Security controls—Prescriptions for meeting information security standards.

1 University information classifications are addressed in "University Information Classifications" (p. 12).

Each layer builds upon the last to create a sophisticated methodology for appropriately addressing both broad concerns and specific, procedural solutions.

Security standards and controls

Security standards are the set of requirements set forth by the Secure UD DGSP for the security of IT resources, including University information and IT devices. Standards are organized into 25 risk management objectives across 10 risk areas.

Security controls are the administrative, operational, and technical requirements and recommendations for meeting security standards. Each security standard defines one or more security controls, and each security control has one or more specific requirements and/or recommendations. Security standards and controls apply to University information in all forms and in all locations.

Security standards and controls are designed to be consistent, yet flexible. The goal is to produce measurable results, including compliance, without impeding University function.

Not all security controls will apply to all units. Each unit must assess the applicability and feasibility of the security control requirements and implement those security controls necessary to appropriately manage risk in accordance with its missions and activities.

Supporting tools and guidance

Supporting tools and guidance simplify the implementation of information security across the University by equipping and empowering units to understand, assess, and improve their information security and risk postures.

Assessment tools are applied to analyze risks, identify control gaps, and measure compliance with Secure UD DGSP requirements. Each assessment tool is designed to work in conjunction with the objectives and requirements of the Secure UD DGSP to create a nuanced understanding of the University's risk and security needs. The Secure UD Compliance and Risk Survey (Secure UD CARS) combines unit compliance and risk assessments to provide a single, actionable solution for unit assessment requirements.

Awareness

Employee training about and awareness of information security issues are central to the success of the University's information security and risk management efforts. Employees are one of the University's most valuable resources, but they also represent a major information security risk. Continual reinforcement of IT risks and security practices is vital to helping employees protect IT resources.

Figure 1: *Risk management model*

University Information Classifications

The University Information Classification Policy establishes three University information classifications based on the confidentiality risks to University if information:

1. Level I—Low Risk information
2. Level II—Moderate Risk information
3. Level III—High Risk information.

Table 1 (p. 13) characterizes the three University information classifications and provides examples.

How information is classified

Information confidentiality

Information is classified by University data stewards according to its confidentiality risks.[1]

IT devices inherit the classification of the University information they access, process, store, or transmit.

Information criticality

Information classifications consider only the confidentiality of University information. However, information also has risks related to integrity and availability—collectively addressed as criticality—that may affect how it should be managed. There are three criticality categories: non-critical, critical, and mission critical.

1. Non-critical—Necessary to the business continuity or operational effectiveness of the unit. Loss of integrity or availability of non-critical IT resources would have limited or no short-term impact on business continuity or operational effectiveness.
2. Critical—Important to the business continuity or operational effectiveness of the unit. Loss of integrity or availability of critical IT resources would have moderate short-term impact on business continuity or operational effectiveness.
3. Mission critical—Vital to the business continuity or operational effectiveness of the unit. Loss of integrity or availability of mission critical IT resources would have significant short-term impact on business continuity or operational effectiveness.

Critical or mission-critical information may not necessarily have high confidentiality risks, but its importance to business continuity or operational effectiveness may warrant management practices and security standards beyond those required by its University information classification.

How information is protected

Security controls apply based on the classification of the IT resources at risk. Therefore, it is vital to properly and completely classify IT resources to ensure that security controls can be implemented appropriately.

Each security control applies to one, two, or three of the University information classifications.

Optionally data stewards and/or unit heads may require that certain University information or IT devices be managed as though they were of a higher classification due to their criticality risks. In these cases, the University information or IT device is effectively classified at a higher University information classification.

1 Data steward—An individual within the University who is the primary institutional authority for a particular data set and who is principally responsible for the management and security of that data set across the institution.

Level I Low Risk	Level II Moderate Risk	Level III High Risk
Risks: Unintentional, unlawful, or unauthorized disclosure presents **limited or no risk**.	**Risks:** Unintentional, unlawful, or unauthorized disclosure presents **moderate risk**.	**Risks:** Unintentional, unlawful, or unauthorized disclosure presents **significant risk**.
Examples: • Publicly released information • Directory information • General access data • Data with low confidentiality, integrity, and availability concerns	**Examples:** • FERPA records • HR information • Non-public applicant and donor information • Legal investigation records • Unpublished intellectual property (including research data) • Unpublished business information • Other information as specified by contractual, legal, or other requirements	**Examples:** • Personally Identifiable Information (PII) – Social Security numbers – Driver's license numbers – Passport or visa numbers – Financial account numbers • Protected Health Information (PHI/ePHI) • Export-restricted data • Human subject data • UDelNet passwords • Encryption keys • Other information as specified by contractual, legal, or other requirements
Protection requirements: • Level I information is explicitly approved for distribution publicly with no restrictions on access or usage	**Protection requirements:** • Share only with those who need to know • Dispose of securely	**Protection requirements:** • Encrypt at rest and in transit • Do not send in unencrypted email attachments • Share only with those who need to know • Dispose of securely

Table 1: *University information classifications*

Roles and Responsibilities

The success of the University's information security and risk management efforts depends on a data governance framework that establishes the roles and responsibilities for managing University information. Accountability for IT resources and their security drives ownership of information security and risk management issues and creates an institutional context for management efforts.

University policies—including the University Data Governance Policy and the University Information Security Policy—define the University's data governance framework, including general roles and responsibilities for information security. A synopsis of how these roles interact at the institutional level is illustrated in Figure 2 (p. 15).

Because the University encompasses many units with diverse administrative, operational, and technical needs, the allocation of security roles may vary across units and functional areas. The data governance framework has the flexibility to accomodate this diversity. Roles and responsibilities established by the framework should be fulfilled by appropriate individuals based on their unit's or functional area's specific needs.

Any employee may fulfill one or more roles as necessary and has the responsibilities of each of his or her roles.

The following roles coordinate and manage data governance and information security efforts across the University:

1. President
2. Council for Data Governance (CDG)
3. Data trustee
4. Data steward
5. Data Management Advisory Committee (DMAC)[1]
6. Data Security Advisory Committee (DSAC)
7. Data custodian
8. Information Technologies (IT)

The following roles implement data governance and information security at the unit level.

1. Unit head
2. Local support provider
3. End user

1 The DMAC is not covered extensively in the Secure UD Data Governance & Security Program because it is concerned with the management of data in the context of informational quality, effectiveness, usability, and strategic value rather than in the context of security.

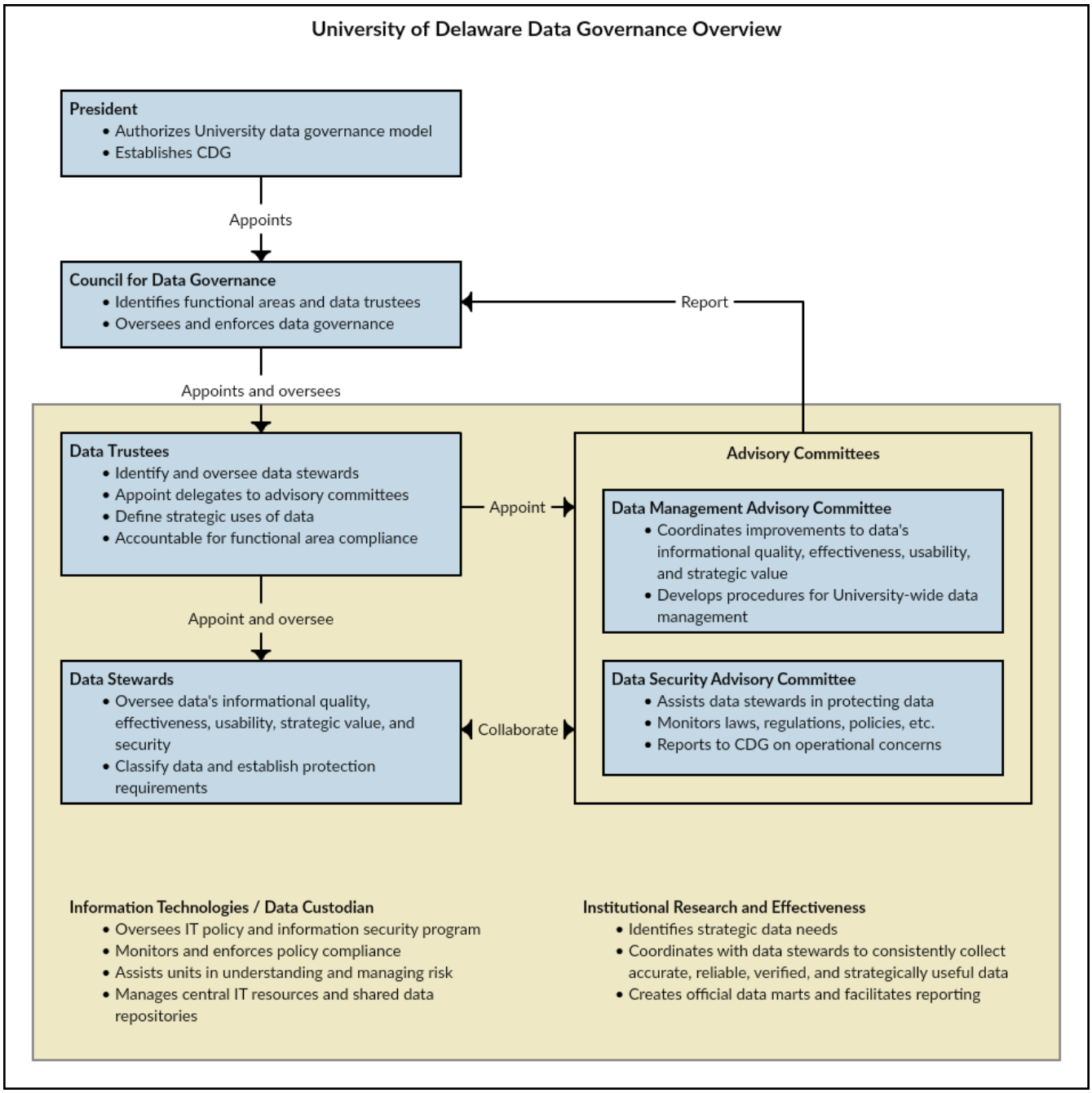

Figure 2: *Data governance overview*

Data governance overview

The University Data Governance Policy grants the President of the University, and his or her delegates, the highest degree of authority over the University's data governance framework.

The University's data governance and information security roles are arranged by functional area[2] and unit[3] to facilitate the coordination of data governance and information security efforts.

- Each functional area has a data trustee who holds ultimate strategic and policy-setting authority for that functional area.
- Each data set has a data steward who establishes the policies and procedures for managing and securing the data sets within his or her stewardship.
- Each unit has a unit head who is responsible for managing the unit's use of University information.
- The individuals who use data are end users.

Data stewardship

The University, as an organization, owns all University information.

Organizing and leading institutional data governance efforts are the University's executive officers. As data trustees, these individuals are ultimately accountable for the strategic use of University information and for overseeing its stewardship. Each data trustee is accountable for the data for which his or her functional area is principally responsible.

Each data trustee appoints a data steward for each data set within his or her jurisdiction. Data stewards are operational experts on those data sets and understand the value of the data and how it is used across the institution. They are actively engaged in the acquisition, utilization, maintenance, access, and protection of University information to ensure that it is suitable to support institutional missions, strategies, and activities.

Each data steward establishes standards and guidelines for the data sets within his or her stewardship. These standards apply to that University information wherever it exists, even across functional areas.

Data stewards set management requirements for data.

Data management

In the course of fulfilling University missions, each functional area uses many kinds of University information, including some University information from that functional area and some from other functional areas.

Data trustees are ultimately accountable for ensuring that their functional areas adhere to appropriate data management practices for all University information and other IT resources in use by their units.

Every unit head is primarily responsible for ensuring his or her unit's compliance with University policies, including data management standards and guidelines.

Every end user of IT resources, including University information, has a responsibility to appropriately manage and protect those IT resources.

All University information must be managed according to the requirements set for it by the respective data steward.

2 Functional area—One or more units that have primary responsibility for managing a core University mission or business function.
3 Unit—A University department, school, institute, program, office, initiative, center, or other operating unit.

Data governance committees

To coordinate University-wide data governance and security efforts, University policy establishes two data governance committees[4]:

- The Council for Data Governance (CDG)
- The Data Security Advisory Committee (DSAC)

The CDG is an executive-level committee formed by the President to identify and organize the University's functional areas and data trustees. Initially, the CDG defines the University's functional areas and appoints a data trustee for each one. From that point forward, it ensures institutional accountability for data management by assisting data trustees in coordinating and executing their governance responsibilities.

The DSAC is an operational committee chaired by the director of IT Security. It is composed of delegates as appointed at the discretion of data trustees and/or the chair. The DSAC is tasked with coordinating the University's information security and risk management efforts across functional areas. It facilitates collaboration between data stewards to establish and enforce consistent and effective requirements for protecting University information.

The CDG and DSAC collaborate to promote and improve the confidentiality, integrity, and availability of University information. The DSAC monitors legal, regulatory, and technological developments for relevance to the University. Based on relevant developments and the initiatives of the data trustees and data stewards, it then provides recommendations to the CDG for follow-up as necessary.

4 University policy also establishes a third data governance committee, the Data Management Advisory Committee (DMAC), which is concerned with data management in the context of the informational quality, effectiveness, usability, and strategic value of data.

University-wide data governance roles and responsibilities

The following roles are responsible for managing information security policy, including the Secure UD DGSP, and for making University-wide data governance decisions.

Council for Data Governance (CDG)

The CDG is the University council responsible for overseeing the appointment and action of data trustees for each of the University's functional areas.

The CDG includes the Chief Information Officer, VP & General Counsel, and other individuals as appointed by the President of the University and/or his or her delegates.

The CDG's primary data governance responsibilities include:

1. Monitoring and managing the University's data governance framework.
2. Identifying the University's functional areas and their data trustees.
3. Ensuring that data trustees fulfill their responsibilities according to policy.
4. Resolving disputes of responsibility where data overlaps the functional areas of multiple data trustees.
5. Overseeing the formation and operation of the DSAC.

Data Security Advisory Committee (DSAC)

The DSAC is the University council responsible for coordinating information security and risk management efforts and monitoring and recommending necessary security actions to the University.

The DSAC is chaired by the director of IT Security and includes delegates as appointed by data trustees and/or IT.

The DSAC's primary data governance and information security responsibilities include:

1. Assisting the CDG and data stewards in protecting University information.
2. Monitoring changes in laws, technology, and best practices..
3. Assessing risks to University information.
4. Recommending updates to policy, including the Secure UD DGSP, as necessary.
5. Reporting to the CDG relevant security initiatives and recommendations.

Data trustee

A data trustee is an executive officer of the University who has the highest level of strategic planning and policy-setting authority for his or her functional area. A data trustee may delegate select authorities appropriately.

Data trustees' primary data governance and information security responsibilities include:

1. Appointing and overseeing data stewards for each data set entrusted to their care.
2. Ultimate accountability for their functional areas' compliance with policies, standards, and guidelines for data management and information security, including the implementation of reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of IT resources within their functional areas.
3. Coordinating the use of University infromation in a manner commensurate with the University's missions and strategic goals.
4. Appointing delegates to participate in the DMAC and DSAC.
5. Defining risk tolerance related to security threats to University information.
6. Requiring annual assessments of security controls within their functional areas and reporting the results to IT.

Data steward

A data steward is an individual within the University who is the primary institutional authority for a particular data set and who is principally responsible for the management and security of that data set across the institution.

Data stewards' primary data governance and information security responsibilities include:

1. Overseeing the informational quality, effectiveness, usability, strategic value, and security of University information.
2. Developing data management standards and guidelines for the management and security of University information.
3. Authorizing and auditing the access of individual users to University information.
4. Reviewing and approving uses or proposed uses, including the creation of shared data repositories, of University information.
5. Requiring the implementation of reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of University information within their stewardship.
6. Identifying and classifying University information from their functional areas and periodically reviewing classifications.

Data custodian

A data custodian is a University entity or employee with operational responsibility to manage a shared data repository on behalf of a data steward.[5]

Data custodians' primary data governance and information security responsibilities include:

1. Facilitating the technical management of the shared data repositories for which they are responsible.
2. In compliance with data stewards' standards and guidelines, granting and managing end user access to the shared data repositories for which they are responsible.

Information Technologies

IT will fulfill administrative, operational, and technical roles within the governance model.

IT's primary data governance and information security responsibilities include:

1. Maintaining overview responsibility for IT policy, including the Secure UD DGSP.
2. Establishing policy requirements, including security standards and controls, and monitoring and enforcing compliance.[6]
3. Assisting units in understanding risk and developing security plans.
4. Training and educating the University community on IT policies.
5. Functioning as the local support provider for IT devices for which there is no appointed local support provider.
6. Fulfilling other responsibilities commensurate with IT's role as a unit, including the management of central IT resources.
7. In collaboration with data stewards, developing and maintaining a University data dictionary based on the classifications assigned by data stewards to the University information from their functional areas.

5 Shared data repository—A collection of University information to which multiple individuals or entities have access.
6 IT's role in establishing, monitoring, and enforcing policy requirements does not abrogate the responsibility of individuals and units to comply with policy requirements.

Unit-level data governance roles and responsibilities

The University's governance model emphasizes the role of the unit as a largely autonomous entity. Each unit is individually responsible for its data management practices. The responsibility of other roles for establishing, monitoring, and enforcing policy requirements for the University does not abrogate individuals and units of their responsibility to comply with policy requirements. Units are individually responsible for their compliance.

Unit head

A unit head is a University official with the highest level of authority over the day-to-day management or oversight of a unit's operation.

Unit heads' primary information security responsibilities include:

1. Assuming primary policy compliance responsibility for the IT resources under their control.
2. Identifying at least one local support provider for each unit IT device and reporting that individual or unit to IT.
3. Developing and implementing a unit information security plan.
4. Ensuring the implementation of appropriate security controls for the IT resources under their control.
5. Approving exceptions to policy based on operational or technical needs.
6. Reporting to data trustees the effectiveness of data management and information security their units.
7. Assisting in the investigation of incidents and representing their unit in the incident response process.
8. Disseminating information about security, including policies and procedures, to their unit.

Local support provider

A local support provider is an individual or unit with primary responsibility for the installation, configuration, security, and ongoing maintenance of an IT device. IT will be the local support provider for IT devices for which a local support provider is not otherwise appointed.

Local support providers' primary information security responsibilities include:

1. Maintaining knowledge of the IT devices for which they are responsible.
2. Implementing security controls for the IT devices for which they are responsible at the direction of the unit head.
3. Understanding and documenting the configurations and characteristics of the IT devices for which they are responsible.
4. Recommending security controls and practices for the IT devices for which they are responsible.

End user

An end user is any individual who accesses and/or utilizes IT resources.

Every end user is responsible for being aware of data management and security and for protecting the IT resources in their care as required by laws, regulations, and policies.[7]

7 It is not anticipated that end users will reference this document unless they fulfill a managerial role within their unit. The mandate to understand and comply with requirements may be fulfilled through unit security education and clear unit security requirements.

Federal Standard Mapping

The Secure UD DGSP draws from leading security models in the higher education industry and federal standards published by the National Institute of Standards and Technology (NIST).

The Secure UD DGSP includes a selection of relevant and significant federal and industry standards with special attention given to the University's unique information needs and security culture.

NIST references

Security controls in the Secure UD DGSP have, where applicable, a NIST Special Publication 800-53 reference identifying the NIST security and privacy controls they substantively represent. Table 2 (p. 22) lists the NIST control families and their IDs and can assist in identifying which areas of NIST are being referenced by each of the Secure UD DGSP's security controls.

ID	Family	ID	Family
AC	Access Control	RA	Risk Assessment
AT	Awareness and Training	SA	Systems and Services Acquisition
AU	Audit and Accountability	SC	System and Communications Protection
CA	Security Assessment and Authorization	SI	System and Information Integrity
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	AP	Authority and Purpose
IA	Identification and Authentication	AR	Accountability, Audit, and Risk Management
IR	Incident Response	DI	Data Quality and Integrity
MA	Maintenance	DM	Data Minimization and Retention
MP	Media Protection	IP	Individual Participation and Redress
PE	Physical and Environmental Protection	SE	Security
PL	Planning	TR	Transparency
PS	Personnel Security	UL	Use Limitation

Table 2: *NIST security and privacy control families*

Compliance and Exceptions

Compliance requirements

Each unit is generally responsible for its own compliance with the requirements of the Secure UD DGSP.[1] Security standards and controls are written with an emphasis on the unit as a discrete entity in the University's security landscape.

Each unit head is primarily responsible for the security compliance of his or her unit. Local support providers and end users are responsible for implementing controls at the direction of the unit head to ensure unit compliance with security requirements.

Each unit must develop an information security plan.[2] This plan—which will be based on the unit's particular information and security needs—will outline which security controls the unit will implement and how they will be implemented. Security controls are flexible enough to accomodate the needs of individual units. Not all security controls are applicable to every unit.

All end users of IT resources are required to comply with security standards and controls.[3]

The security standards and controls apply to University information in all forms and in all locations. Specifically:

- Personally-owned devices used for University purposes are subject to the same compliance requirements as University-owned devices.
- Units remain responsible for the security of University information accessed, processed, stored, or transmitted through cloud or other outsourced services.

Compliance must be reported as described in University policies and in security control requirements. Compliance is subject to audit.

Compliance exceptions and reporting

Exceptions to security standards and controls must be justified by operational or technical needs and must be approved by the unit head.[4]

IT will work in an advisory capacity to assist units in finding alternatives to security controls that cannot be administratively, operationally, or technically implemented.

Compliance assistance

End users may contact their unit head or local support provider for assistance with compliance.

Units may contact IT for consultation regarding compliance, implementation, and exceptions.

1 Unit—A University department, school, institute, program, office, initiative, center, or other operating unit..
2 Unit information security plan requirements are addressed in security control IS 2.1.1 (p. 33)
3 It is not anticipated that end users will reference this document unless they fulfill a managerial role within their unit. The mandate to understand and comply with requirements may be fulfilled through unit security education and clear unit security requirements.
4 Exception requirements are addressed in security control IS 2.1.2 (p. 33)

This page intentionally left blank.

Risk Management Overview

This section provides an overview of the risk areas and risk management objectives central to the Secure UD DGSP. Detailed security control requirements related to these risk management objectives are addressed in "Security Controls" (p. 30). An overview of security standards and controls is provided in "Appendix A: Security Standards and Controls Summary" (p. 108).

The Secure UD DGSP is divided into 25 risk management objectives in 10 risk areas. Collectively, these risk areas and risk management objectives address critical information security concerns relevant to the University and its IT resources.

The 10 risk areas provide a high-level picture of how information security affects the University. Each risk area describes a different kind of security risk that the University must manage.

The 25 risk management objectives are the driving force behind the implementation of the Secure UD DGSP. They guide the organization of information security initiatives, inform the application of security standards and controls, and drive the evaluation of unit compliance.

PDF

PDF tip: Text in the tables of this section serve as clickable links. Click the text of a risk area or risk management objective to jump to that information in the Security Controls.

Information Security Program	IS—Risk Area 1
Objective IS 1	**Information Risk Assessment** *Objective: To identify, assess, and remediate risk.*
Objective IS 2	**Information Security Planning** *Objective: To ensure that information risk is managed by consistent and appropriate plans.*
IT Resource Acquisition	**AQ—Risk Area 2**
Objective AQ 1	**Vendor Service Acquisition** *Objective: To manage risks regarding vendor service acquisition.*
Objective AQ 2	**Vendor Management** *Objective: To ensure vendors are satisfying University security requirements.*
Objective AQ 3	**Software License Management** *Objective: To comply with laws and regulations governing software use.*
Application Security	**AS—Risk Area 3**
Objective AS 1	**Application Software Security** *Objective: To protect application operation, function, and data.*
Objective AS 2	**Application Development Process** *Objective: To securely develop applications.*
Contingency Planning	**CP—Risk Area 4**
Objective CP 1	**Business Continuity Planning** *Objective: To mitigate disruptions of University business processes.*
Objective CP 2	**Disaster Recovery** *Objective: To mitigate disruptions of IT resources.*
Data Management	**DM—Risk Area 5**
Objective DM 1	**Data Acquisition** *Objective: To collect data with appropriate breadth and depth.*
Objective DM 2	**Data Utilization** *Objective: To utilize data in support of University missions and business processes.*
Objective DM 3	**Data Maintenance** *Objective: To maintain data in compliance with policies.*
Objective DM 4	**Data Access** *Objective: To access data according to authorization and operational requirement.*
Objective DM 5	**Data Protection** *Objective: To protect data from unintentional, unlawful, or unauthorized disclosure, alteration, or destruction.*

Human Resources	HR—Risk Area 6
Objective HR 1	**Awareness and Training** *Objective: To educate users about security threats and best practices.*
Objective HR 2	**Employment Management** *Objective: To ensure due diligence management of employees.*
Identification and Authentication	**IA—Risk Area 7**
Objective IA 1	**Identification and Authentication** *Objective: To securely manage digital identities and authentication processes.*
Incident Response	**IR—Risk Area 8**
Objective IR 1	**Incident Response** *Objective: To address incidents promptly and appropriately.*
Physical Security	**PE—Risk Area 9**
Objective PE 1	**IT Resource Physical Security** *Objective: To physically protect IT resources in University locations.*
Objective PE 2	**Data Center Protection** *Objective: To physically protect University data centers.*
System and Communication Management	**SC—Risk Area 10**
Objective SC 1	**Client Management** *Objective: To protect client systems.*
Objective SC 2	**Mobile Device Management** *Objective: To protect mobile devices.*
Objective SC 3	**Server Management** *Objective: To protect server systems.*
Objective SC 4	**Network Management** *Objective: To protect networks and network devices.*
Objective SC 5	**Transmission and Communication Management** *Objective: To protect communication systems.*

Risk areas and risk management objectives

The above table shows how Secure UD policy organizes information- and IT-related risk. Risks are categorized into 10 risk areas, and 25 risk management objectives are established to guide the management of each "family" of risk.

Risk area explanations

Below are brief explanations of the ten risk areas. Each risk area encompasses a different group of IT and information-related risk to the University.

Information Security Program (IS—Risk Area 1)

This risk area is primarily concerned with information risk management and security planning. Planning is essential to consistently and appropriately protecting the University's IT resources from unintentional, unlawful, or unauthorized disclosure, alteration, or destruction. Assessments are used to gauge the effectiveness of risk management and information security efforts and to identify areas of improvement.

IT Resource Acquisition (AQ—Risk Area 2)

This risk area is primarily concerned with mitigating the risk of acquiring and using IT services and software. Appropriate IT resource acquisition is essential to ensuring the secure and reliable function of vendor or third-party services and products.

Application Security (AS—Risk Area 3)

This risk area is primarily concerned with the risks associated with internally developing application software that will access, process, store, or transmit University information. Application security is essential to preventing information systems from exposing University information or being vulnerable to attack.

Contingency Planning (CP—Risk Area 4)

This risk area is primarily concerned with mitigating disruptions of the University's operations and IT resources. Continuity of operations and the integrity and availability of IT resources are essential to mitigating operational risk to the University.

Data Management (DM—Risk Area 5)

This risk area is primarily concerned with establishing standards for the management—including the acquisition, utilization, maintenance, access, and protection—of University information. Appropriate data management is one of the fundamental concepts of information security.

Human Resources (HR—Risk Area 6)

This risk area is primarily concerned with ensuring and improving employee management and information security awareness through training and other resources. Employee information security awareness is essential to protecting both individual employees and the IT resources for which they are responsible.

Identification and Authentication (IA—Risk Area 7)

This risk area is primarily concerned with ensuring appropriate authorization and access to IT resources throughthe use of secure authentication mechanisms. Identification and authentication are essential to ensuring that only authorized users can access IT resources.

Incident Response (IR—Risk Area 8)

This risk area is primarily concerned with consistent and appropriate response to incidents. Appropriate incident response procedures are essential to mitigating harm to the University and affected stakeholders.

Physical Security (PE—Risk Area 9)

This risk area is primarily concerned with physically protecting IT resources in unit locations and data centers. Physical security is essential to ensuring the overall security of IT resources, including computers, mobile devices, server systems, electronic storage media, and printed University information.

System and Communication Management (SC—Risk Area 10)

This risk area is primarily concerned with the technical controls that protect IT devices and communications data. These controls are essential to ensuring the security of the University's computers, mobile devices, server systems, network, and transmissions.

Security Controls

This section provides a detailed explanation of the security controls required for compliance with the Secure UD DGSP. An overview of security standards and controls is provided in "Appendix A: Security Standards and Controls Summary" (p. 108).

Security controls are the detailed prescriptions for achieving policy compliance and IT resource security.

Each security control prescribes administrative, operational, and/or technical requirements or recommendations for protecting IT resources. Each security control also, when applicable, references relevant parallel controls in NIST SP 800-53.[1]

Security controls are applied based on the three University information classifications: Level I—Low Risk information, Level II—Moderate Risk information, and Level III—High Risk information.[2] Each security control has an information classification indicator, shown in Figure 3 (p. 30), that denotes the classification(s) to which it applies. Some security controls may apply based on criticality instead of, or in addition to, classification.[3]

Each unit is responsible for meeting all security standards and implementing all security controls applicable to its administration, operation, and IT resources. Not all security controls are applicable to every unit; the unit is responsible for identifying which security controls are applicable as part of its information security plan.[4] Exceptions to security standards and controls must be approved by the unit head and documented.[5]

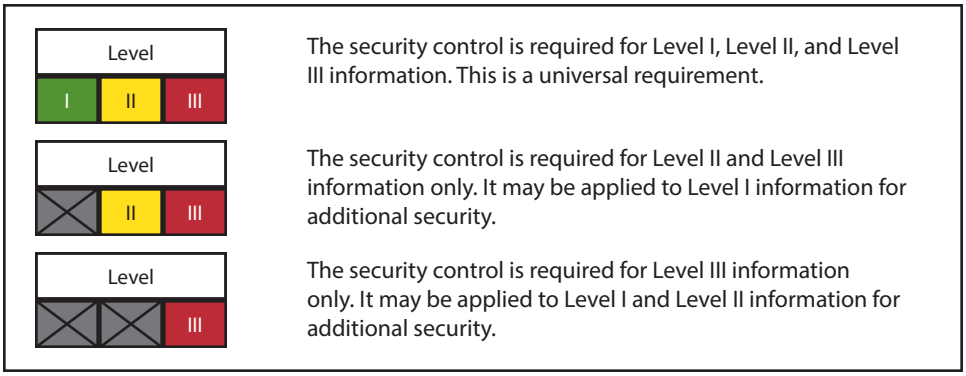

Figure 3: *Information classification indicators*

PDF

PDF tip: Text in the footers of this section serve as clickable links. Click the risk area initials in the footer to jump to that risk area in this section.

1 NIST references are addressed in "Federal Standard Mapping" (p. 22).
2 University information classifications are addressed in "University Information Classifications" (p. 12).
3 Criticality is addressed in "Information criticality" (p. 12).
4 Information security plan requirements are addressed in security control IS 2.1.1 (p. 33).
5 Procedures for handling exceptions to security standards and controls are addressed in "Compliance exceptions and reporting" (p. 23).

Information Security Program — IS—Risk Area 1

Objective IS 1

Information Risk Assessment

Objective: To identify, assess, and remediate risk.

Standard IS 1.1

Risk assessments are conducted regularly.

Control IS 1.1.1

Conduct information risk surveys.

Level: I | II | III

Requirements:

A. Complete the Secure UD Compliance and Risk Survey (Secure UD CARS) as required by the unit's data trustee.
B. Identify security controls, resources, and planned timelines to close control gaps.
C. Submit Secure UD CARS results to the unit's data trustee and IT Security for review.

NOTE: For many units, the Secure UD CARS satisfies the minimum requirements. Additional unit, legal, regulatory, or contractual risk assessment requirements may also apply.

References: *NIST SP 800-53 RA-1, RA-3; Secure UD Compliance and Risk Survey question #1*

Control IS 1.1.2

Conduct risk assessments.

Level: ~~I~~ | ~~II~~ | III

Requirements:

A. Complete a risk assessment where required by law or regulation for all information systems that process, store, or transmit Level III University information. The process must:
   1. identify and characterize IT resources
   2. identify threat sources and capabilities
   3. identify threat events
   4. identify vulnerabilities
   5. assess existing security controls
   6. assess likelihood of threat occurrence
   7. assess potential adverse impacts
   8. assign an overall risk rating
   9. develop a plan to remediate risk
   10. perform comprehensive analysis and detailed reporting.
B. Submit risk assessment results to the unit's data trustee and IT Security for review and approval.

NOTE: This security control applies to both cloud and traditional information systems.

References: *NIST SP 800-53 RA-1, RA-3; Secure UD Compliance and Risk Survey question #2*

Standard IS 1.2

A risk management strategy is developed, implemented, and maintained.

Control IS 1.2.1

Develop, implement, and maintain a risk management strategy.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain a risk management strategy. For each of the 25 risk management objectives identified in the Secure UD Data Governance & Security Program, the risk management strategy must:
   1. identify the current level of risk as assessed in the most recently completed Secure UD Compliance and Risk Survey (Secure UD CARS)
   2. identify the risk management decision for this risk management objective from the following list (choose one):
      a. retain the risk (accept the risk as it is, without any plan for mitigation)
      b. reduce the risk (plan to mitigate the risk, to lessen the impact on the unit)
      c. share the risk (find a third party or University partner to transfer some part of the risk)
      d. avoid the risk (stop or disassociate from the activity creating the risk).

B. Update the risk management strategy annually or after unit or technological changes.

C. Submit the risk management strategy to the unit's data trustee and IT Security for review and approval after each update.

NOTE: The Secure UD CARS includes guidance and a template for creating a three-year risk management strategy.

References: *NIST SP 800-53 PM-9; Secure UD Data Governance & Security Program; Secure UD Compliance and Risk Survey question #3*

Standard IS 1.3

Security assessments are conducted regularly.

Control IS 1.3.1

Conduct IT security assessments.

Level: I | II | III

Requirements:

A. Complete an IT security assessment as required by the unit's data trustee to ensure that security controls meet the risk management objectives specified in the Secure UD Data Governance & Security Program and to provide feedback on how well the unit is meeting their strategic risk management goals. Security assessments include:
   1. security self-assessments performed by the unit using the Secure UD Compliance and Risk Survey (Secure UD CARS)
   2. security assessments performed by an University-approved security assessor.

B. Submit security assessment results to the unit's data trustee and IT Security for review.

NOTE: For many units, the Secure UD CARS satisfies the minimum requirements for this control. Additional unit, legal, regulatory, or contractual security assessment requirements may also apply.

References: *NIST SP 800-53 AU-1, CA-1, CA-2; University Information Security Policy; Secure UD Compliance and Risk Survey*

Objective IS 2

Information Security Planning

Objective: To ensure that information risk is managed by consistent and appropriate plans.

Standard IS 2.1

An information security plan is developed, implemented, and maintained.

Control IS 2.1.1

Develop, implement, and maintain an information security plan.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain an information security plan. For each of the 25 risk management objectives identified in the Secure UD Data Governance & Security Program, the information security plan must:
   1. identify the security controls that will be implemented by the unit, consistent with the unit's risk management strategy
   2. apply the University's security resources, including services, templates, and job aids, as appropriate
   3. address security requirements as they apply to both University-owned and personal (or work-from-home) devices used for University activities.

B. Update the information security plan annually or after major unit or technological changes.

References: *NIST SP 800-53 PL-1, PM-1; Secure UD Data Governance & Security Program; Secure UD Security Plan Tool; Secure UD Compliance and Risk Survey question #4*

Control IS 2.1.2

Manage exceptions to security standards and controls.

Level: I | II | III

Requirements:

A. Exceptions to security standards and controls must be justified by operational or technical needs.

B. Document policy exceptions (including exceptions to information security plans, standards, and controls) in the unit information security plan. Documentation must include:
   1. the exception being requested or implemented
   2. the operational or technical need for the exception.

C. Exceptions must be approved by the unit head.

NOTE: The unit may consult with IT as necessary to determine the appropriateness of exceptions.

References: *University Information Security Policy*

Standard IS 2.2

Information security roles and responsibilities are defined and assigned.

Control IS 2.2.1

Assign information security roles.

Level: I | II | III

Requirements:

A. Appoint at least one local support provider for each unit IT device.

B. Ensure that employees understand their information security roles and responsibilities.

References: *NIST SP 800-53 PM-2, PM-10; University Information Security Policy*

Standard IS 2.3

Changes in law, regulation, and technology are assessed.

Control IS 2.3.1

Assess legal, regulatory, and technological changes.

Level: I | II | III

Requirements:

A. Consult with IT Security to identify legal, regulatory, and policy changes that may affect the unit.
B. Monitor organizational or technological changes that may affect the unit.
C. Update information security plans and practices to comply with relevant changes as identified.

References: *ISO 27001 A.15.1.1; University Information Security Policy; Secure UD Compliance and Risk Survey question #5*

IT Resource Acquisition — AQ—Risk Area 2

Objective AQ 1

Vendor Service Acquisition

Objective: To manage risks regarding vendor service acquisition.

Standard AQ 1.1

Risks are assessed in the IT vendor service acquisition process.

Control AQ 1.1.1

Assess vendor security risks.

Level: I | II | III

Requirements:

A. Identify the privacy, security, operational, policy, legal, regulatory, contractual, or other risks to any University information to be accessed, processed, stored, or transmitted by vendors.

NOTE: Security concerns include the confidentiality, integrity, and availability of data.

References: *NIST SP 800-53 RA-3, SA-1, SA-4, SA-5*

Control AQ 1.1.2

Assess vendor security controls.

Level: I | II | III

Requirements:

A. Complete the Cloud Service Security Assessment Questionnaire for externally-hosted services.

B. Submit the Cloud Service Security Assessment Questionnaire to IT Security for review and approval.

References: *NIST SP 800-53 RA-3, SA-1, SA-4, SA-5*

Standard AQ 1.2

Vendor compliance with security standards is required.

Control AQ 1.2.1

Assess the need for a vendor contract.

Level: I | II | III

Requirements:

A. Require a contract for all vendor services except those by which the University information accessed, processed, stored, or transmitted:

1. is not sensitive and therefore poses little to no risk to confidentiality, or legal, regulatory, contractual, or other compliance
2. is not critical or mission critical and therefore would not materially affect operational effectiveness in the short term if it were lost, corrupted, or unavailable.

B. Prohibit self-provisioning of cloud computing services to store, process, share, or manage University information for which a contract is required.

NOTE: Contract scope requirements are defined in security control AQ 1.2.3 (p. 36).

References: *NIST SP 800-53 AC-20, SA-1, SA-4, SA-9; Secure UD Compliance and Risk Survey question #6*

cont.

cont.

Control AQ 1.2.2

Require vendor adherence to University policy.

Level: I | II | III

Requirements:

A. Require vendors managing or using University IT resources to be obligated to adhere to University policy.

References: *NIST SP 800-53 AC-20, SA-1, SA-4, SA-9*

Control AQ 1.2.3

Require a written vendor contract.

Level: I | II | III

Requirements:

A. Require that vendor contracts be in writing and include terms and conditions to satisfy all privacy, security, operational, policy, legal, regulatory, contractual, or other requirements for any University information to be processed, stored, or transmitted by cloud vendors.

NOTE: Security concerns include the confidentiality, integrity, and availability of data.

References: *NIST SP 800-53 AC-20, SA-1, SA-4, SA-9; Secure UD Compliance and Risk Survey question #6*

Control AQ 1.2.4

Review vendor contracts.

Level: I | II | III

Requirements:

A. Submit proposed vendor contracts to IT Security, VP & General Counsel, and Procurement Services for review and approval.

B. Submit the vendor's terms of service/use and privacy policy to IT Security for review when a contract is not required.

References: *NIST SP 800-53 AC-20, SA-1, SA-4, SA-9; Secure UD Compliance and Risk Survey question #6*

Objective AQ 2

Vendor Management

Objective: To ensure vendors are satisfying University security requirements.

Standard AQ 2.1

Vendor compliance with security standards is verified.

Control AQ 2.1.1

Assess mission critical or Level III vendor security controls.

Level: I | II | III

Requirements:

A. Require vendors processing or transmitting mission critical or Level III information, or providing mission critical services, to submit verification of their security controls to the unit for review annually. Acceptable verification is either:
   1. documentation detailing the vendor's security controls; or
   2. attestation from a third-party assessor validating the vendor's security controls.

B. Submit the verification of vendor security controls to IT Security.

C. Assess the vendor's security controls to ensure compliance with laws and regulations governing that vendor's services to the University.

Recommendations:

D. Require all vendors to submit verification of their security controls to the unit for review annually.

NOTE: Documentation may include the Cloud Service Security Assessment Questionnaire.

NOTE: Attestation may include an SSAE 16 SOC 2 or SOC 3 report.

NOTE: Attestation satisfies the requirement to evaluate vendor security controls.

References: *NIST SP 800-53 SA-9; Secure UD Compliance and Risk Survey question #7*

Standard AQ 2.2

Third-party personnel attestation to security agreements is required.

Control AQ 2.2.1

Require Contractor Confidentiality Agreement attestation.

Level: I | II | III

Requirements:

A. Require all contractor personnel who work directly with University information to attest to the Contractor Confidentiality Agreement annually.

B. Inventory Contractor Confidentiality Agreements.

NOTE: This requirement does not apply to contractor personnel who supply external infrastructure or services.

References: *NIST SP 800-53 AC-20, PS-7, SA-9; Contractor Confidentiality Agreement; Secure UD Compliance and Risk Survey question #8*

Objective AQ 3

Software License Management

Objective: To comply with laws and regulations governing software use.

Standard AQ 3.1

Compliance with software license agreements and law is ensured.

Control AQ 3.1.1

Develop and maintain a software inventory.

Level: I | II | III

Recommendations:

A. Develop, implement, and maintain an inventory of all software presently in local use.
   1. For each piece of software, the inventory must identify:
      a. software publisher/vendor
      b. software name
      c. software version
      d. operating system platform
      e. software purpose
      f. number of copies currently installed
      g. systems on which the software is installed
      h. software support level (e.g., full support, partial support, minimal support, unsupported)
      i. software type (e.g., commercial, open source, freeware, shareware, in-house).
   2. For software types (A. 1. i.) of commercial or shareware, the inventory must contain the following additional information:
      a. license type (e.g., single use, for a named user or machine; multiple-use, for concurrent/floating users or machines)
      b. license scope (e.g., institutional site license, unit site license, unit bulk license, or unit individual license).
   3. For license scopes (A. 2. b.) that are unit, the inventory must contain the following additional information:
      a. purchase date
      b. license expiration date
      c. support expiration date (especially for perpetual licenses).

B. Update the software inventory annually or after unit or technological changes.

C. Submit the software inventory to the unit head for review annually.

References: *NIST SP 800-53 CM-10; Secure UD Compliance and Risk Survey question #9*

Control AQ 3.1.2

Manage software usage.

Level: I | II | III

Requirements:

A. Ensure that all software in local use is being used in compliance with license agreements and copyright law.

B. Where possible, use University-licensed copies of software.

References: *NIST SP 800-53 CM-10; Secure UD Compliance and Risk Survey question #9*

Application Security — AS—Risk Area 3

Objective AS 1 — Application Software Security

Objective: To protect application operation, function, and data.

Standard AS 1.1 — Input data is validated.

Control AS 1.1.1 — Implement input data validation.

Level: I | II | III

Requirements:

A. Implement features to validate and restrict input to applications, allowing only those data types that are known to be correct. Input validation includes:
   1. checking data syntax and semantics (e.g., character set, length, numerical range, or acceptable values)
   2. verifying that inputs match specified definitions for format and content
   3. validating client-provided data
   4. validating data moving between trusted and untrusted connections.

References: *NIST SP 800-53 SI-10*

Control AS 1.1.2 — Implement manual override capability.

Level: I | II | III

Requirements:

A. Implement a mechanism for overriding input validation. Manual overrides must:
   1. provide the capability to suppress input validation in limited cases where an exception to standard input is needed
   2. be restricted for use to a limited group of administrative accounts.

References: *NIST SP 800-53 SI-10*

Standard AS 1.2 — Error message outputs are limited.

Control AS 1.2.1 — Manage error handling.

Level: I | II | III

Requirements:

A. Restrict application error messages to include information necessary for corrective actions without exposing data that could be exploited.

B. Restrict application error message access to only authorized IT staff (e.g., application production support and security management).

References: *NIST SP 800-53 SI-11*

Standard AS 1.3

Information system role assignments are able to be separated.

Control AS 1.3.1

Implement data role separation features.

Level: I | II | III

Requirements:

A. Ensure that applications permit the definition of data roles for the separation of duties at implementation.

References: *NIST SP 800-53 AC-5*

Standard AS 1.4

Secure application boundaries are enforced.

Control AS 1.4.1

Configure application security features.

Level: I | II | III

Requirements:

A. Configure application system security features (e.g., application firewalls) if available. Application security features include:
   1. verifying and controlling communications at the external boundary of the application system and at key internal boundaries (e.g., web server firewalls, access filters)
   2. terminating network connections associated with a communication sessions at the end of the session or after a specified and limited period of inactivity based on business or usability requirements.

References: *NIST SP 800-53 SC-7*

Standard AS 1.5

Application and security events are logged.

Control AS 1.5.1

Log application and security events.

Level: I | II | III

Requirements:

A. Log significant application and security events, including:
   1. configuration changes
   2. input validation failures including:
      a. protocol violations
      b. unacceptable encodings
      c. invalid parameter names and values.
   3. authentication failures
   4. authorization failures
   5. application errors including:
      a. syntax and runtime errors
      b. connectivity problems
      c. performance issues
      d. application specific errors.
   6. alteration or destruction of critical or mission critical logs
   7. session management failures (e.g., cookie session identification value modification)
   8. changes in access to an IT resource.

cont.

References: *NIST SP 800-53 AU-2, AU-3; Secure UD Compliance and Risk Survey question #10*

cont.

Control AS 1.5.2

Log additional application and security events for Level III applications.

Level: III

Requirements:

A. Log additional application and security events for applications accessing, processing, storing, or transmitting Level III information. Additional application and security events include:
   1. use of manual override capabilities
   2. network connections
   3. addition or deletion of users
   4. changes to privileges
   5. assigning users to tokens
   6. adding or deleting tokens
   7. use of administrative privileges
   8. access by application administrators
   9. access to restricted/sensitive/regulated data
   10. use of data encrypting keys
   11. encryption key changes
   12. creation, modification, or deletion of system-level objects
   13. data import and export including screen-based reports
   14. submission of user-generated content (e.g., file uploads).

References: *NIST SP 800-53 AU-2, AU-3; Secure UD Compliance and Risk Survey question #10*

Standard AS 1.6

Secure sessions are enforced.

Control AS 1.6.1

Configure inactive authenticated session suspension.

Level: II III

Requirements:

A. Configure inactive authenticated application session suspension. Session suspension must:
   1. prevent further access to the system
   2. be enforced after one of the following conditions:
      a. an interval of inactivity commensurate with the application's sensitivity
      b. receiving a request from the user
   3. persist until the user renews access using established identification and authentication procedures.

References: *NIST SP 800-53 AC-11, IA-11*

cont.

cont.

Control AS 1.6.2

Implement secure web application session mechanisms.

Level: I | II | III

Requirements:

A. Implement secure session tracking mechanisms for session-oriented web applications to prevent session hijacking or other session-based attacks. Secure session tracking mechanisms must:
   1. use random (or pseudo-random) session identification (id) numbers
   2. prevent the disclosure of the session id during transit
   3. suspend and/or terminate the session after a period of inactivity
   4. provide the ability for users to terminate their own session
   5. prevent the re-use of the session id after a session is terminated
   6. generate a new session id when moving from nonauthenticated to authenticated sessions
   7. generate session ids in a way that makes them difficult to guess.

NOTE: Session suspension requirements are addressed in security control AS 1.6.1 (p. 41).

References: *NIST SP 800-53 AC-11, SC-23*

Standard AS 1.7

The effects of denial of service attacks are limited.

Control AS 1.7.1

Implement denial of service protection.

Level: I | II | III

Requirements:

A. Ensure that applications protect against or limit the effects of denial of service attacks. Denial of service protection may include:
   1. resource, connection, and account monitoring
   2. application load balancing
   3. soft account lockout
   4. computing resource allocation restriction (allocate resources only when necessary and authorized)
   5. controlled error handling.

NOTE: Denial of service attacks include resource exhaustion, account lock out, application level connection/request flooding, corruption of data structures, and exception processing.

References: *NIST SP 800-53 SC-5*

Control AS 1.7.2

Conduct denial of service protection validations.

Level: I | II | III

Requirements:

A. Validate application denial of service controls. An acceptable denial of service control validation is one of the following:
   1. load testing; or
   2. vulnerability scanning; or
   3. penetration testing.

References: *NIST SP 800-53 SC-5*

Standard AS 1.8

Application data is protected during processing.

Control AS 1.8.1

Implement application data processing protection.

Level: III

Requirements:

A. Ensure that applications protect Level III information during processing. Data protection techniques include:
   1. data masking (concealing/obscuring restricted data elements data from improper access)
   2. client-side encryption (encrypting data before transmission to the application using an encryption key known only by the client)
   3. parameterizing database queries.

References: *NIST SP 800-53 SC-4, SC-8*

Standard AS 1.9

Vendor-supported system components are implemented and maintained.

Control AS 1.9.1

Implement and maintain vendor-supported system components.

Level: I II III

Requirements:

A. Implement and maintain vendor-supported software and firmware.
B. Verify software versions are supported and security patches are being released as needed.
C. Update or replace unsupported versions of software or software for which vendors refuse to mitigate vulnerabilities.

References: *NIST SP 800-53 SA-22*

Standard AS 1.10

Security vulnerabilities are identified, assessed, and remediated.

Control AS 1.10.1

Conduct web application vulnerability scans.

Level: I II III

Requirements:

A. Complete a University-approved web application vulnerability scan prior to implementation to ensure that web application and/or service vulnerabilities are identified and managed. Web application vulnerability scans must:
   1. measure vulnerability severity using the Common Vulnerability Scoring System (CVSS) to help determine urgency and priority of response.
   2. be performed using a University-approved vulnerability scanning tool to detect:
      a. web authorization vulnerabilities
      b. session tracking vulnerabilities
      c. input form processing vulnerabilities (e.g., injection, buffer overflow, or cross-site scripting)
      d. web server software flaws or improper configurations.
B. Update vulnerability databases and the vulnerability scanning engine weekly.

NOTE: Vulnerability remediation requirements are defined in security control SC 3.3.1 (p. 89) and security control SC 3.4.1 (p. 90).

References: *NIST SP 800-53 RA-5*

Objective AS 2

Application Development Process

Objective: To securely develop applications.

Standard AS 2.1

A software development process is developed, implemented, and maintained.

Control AS 2.1.1

Develop, implement, and maintain a software development process.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain a formal software development process. The software development process must:
   1. include information security considerations at appropriate points throughout the software development lifecycle
   2. define information security roles and responsibilities and assign those roles to employees.

References: *NIST SP 800-53 SA-3, SA-15; Secure UD Compliance and Risk Survey question #11*

Control AS 2.1.2

Classify application data.

Level: I | II | III

Requirements:

A. Classify application data according to University policy.

B. Submit data classifications to the project team and the unit head for review and approval at the beginning of the software development lifecycle.

References: *NIST SP 800-53 RA-2; University Information Classification Policy; Secure UD Compliance and Risk Survey question #11*

Control AS 2.1.3

Develop, implement, and maintain a system security plan.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain a system security plan for all new or upgraded information systems. The system security plan must:
   1. identify application security requirements based on the Secure UD Data Governance & Security Program
   2. identify security controls in place or planned for meeting those requirements during the architecture or design phase(s) of the software development process
   3. identify remediation plans and implementation timelines for addressing security issues identified during the software development process.

B. Submit the system security plan to the project team and the unit head for review and approval before the system is deployed into production.

References: *NIST SP 800-53 CA-2, SA-15; Secure UD Compliance and Risk Survey question #11*

cont.

cont.

Control AS 2.1.4

Conduct a peer code review.

Level: I | II | III

Requirements:

A. Complete a peer code review during the system development process for all new or upgraded information systems. Peer code reviews must check application security controls to verify the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the requirements of the system security plan and the Secure UD Data Governance & Security Program.

B. Submit peer code review results to the project team and the unit head for review and approval before the system is deployed into production.

NOTE: Minimally, all information systems must be reviewed before being deployed into production.

References: *NIST SP 800-53 SA-11, SA-15*

Control AS 2.1.5

Implement application data environment protection.

Level: III

Requirements:

A. Implement security controls in non-production environments to protect Level III information during processing, storage, and transmission. Security controls include:

1. using non-routable development environments accessible only from on-campus or VPN connections.

References: *NIST SP 800-53 CA-2, SA-15*

Standard AS 2.2

Application and configuration changes are managed.

Control AS 2.2.1

Develop, implement, and maintain a change management process.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain a formal change management process to control the software development process. The change management process must:

1. determine the types of changes to applications or the software development processes that are subject to change management
2. evaluate proposed changes with explicit consideration of the security impact
3. approve or disapprove proposed changes
4. implement only approved changes
5. remove or disable functionality that allows the bypass of security controls prior to implementation in a staging or production environment
6. document change management decisions, retaining change management records according to records retention schedules.

References: *NIST SP 800-53 CM-3*

cont.

cont.

Control AS 2.2.2

Conduct change tests.

Level: I | II | III

Requirements:

A. Complete tests of approved changes to applications before implementing them in the production environment.
   1. Test proposed changes to critical or mission critical applications in a separate test environment.
B. Submit test results to the project team and the unit head for review and approval before the approved change is deployed into production.

References: *NIST SP 800-53 CM-3*

Standard AS 2.3

Application data access is managed.

Control AS 2.3.1

Manage application data access.

Level: I | II | III

Requirements:

A. Ensure that applications that access the University's network or University information document and receive authorization for application data access. Application data access documentation must include:
   1. the type of data to be accessed
   2. the classifications of the data to be accessed
   3. the application interface characteristics
   4. a data flow diagram
   5. the endpoint connections (for network access).
B. Update application data access documentation when applications are modified or upgraded.
C. Submit application data access documentation to the project team and the data steward of the requested data for review and approval.

References: *NIST SP 800-53 CA-9*

Contingency Planning — CP—Risk Area 4

Objective CP 1

Business Continuity Planning

Objective: To mitigate disruptions of University business processes.

Standard CP 1.1

A business continuity plan is developed, implemented, and maintained.

Control CP 1.1.1

Develop, implement, and maintain a business continuity plan.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain a business continuity plan. The business continuity plan must:
   1. include a business impact analysis. A business impact analysis defines:
      a. business priorities (critical or mission critical business processes)
      b. business dependencies (critical or mission critical IT resources or other business processes)
      c. maximum allowable disruption (how long the unit can operate without a given critical or mission critical business process before suffering a significant consequence).
   2. identify recovery roles and responsibilities and assign those roles to University staff
   3. identify contact information for critical or mission critical employees, departments, agencies, and/or vendors
   4. identify strategies to maintain or recover essential business processes and functions under each of the following conditions:
      a. A significant disruption, compromise, or failure of the information system(s) needed to support essential business processes and functions has occurred.
      b. Work space(s) are rendered unavailable for a period long enough to significantly impact essential business processes and functions.
      c. A number of employees are unavailable for a period long enough to significantly impact essential business processes and functions.

B. Update the business continuity plan annually or after unit or technological changes.

cont.

References: *NIST SP 800-53 CP-2; Secure UD Compliance and Risk Survey question #12*

cont.

Control
CP 1.1.2

Conduct business continuity tests.

Level: I | II | III

Requirements:

A. Complete a business continuity test or review annually to determine the effectiveness of the business continuity plan and the organizational readiness to execute the plan. An acceptable business continuity test or review is one of the following:
   1. checklist test; or
   2. structured walkthrough; or
   3. simulation; or
   4. actual disruptive event.

B. Update the business continuity plan after testing or review as necessary.

NOTE: Checklist test—A test in which a plan or procedure is reviewed to ensure accuracy and consistency.

NOTE: Structured walkthrough—A test in which a plan or procedure is reviewed step by step with the individuals responsible for its execution to ensure accuracy and consistency.

NOTE: Simulation—A test in which a plan or procedure is executed during a mock disruptive event to ensure its function.

NOTE: Disruptive event—An event that requires the execution of a plan or procedure to recover from operational loss.

References: *NIST SP 800-53 CP-4; Secure UD Compliance and Risk Survey question #13*

Objective CP 2

Disaster Recovery

Objective: To mitigate disruptions of IT resources.

Standard CP 2.1

A disaster recovery plan is developed, implemented, and maintained.

Control CP 2.1.1

Develop, implement, and maintain a disaster recovery plan.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain a data center disaster recovery plan. The disaster recovery plan must define:
   1. critical or mission critical IT resources
   2. recovery point objective (RPO)
   3. recovery time objective (RTO)
   4. IT recovery roles and responsibilities and the University employees assigned to those roles
   5. contact information for critical or mission critical IT employees, departments, agencies, and/or vendors.

B. Update the disaster recovery plan annually or after unit or technological changes.

NOTE: IT maintains and tests a disaster recovery plan for central IT resources. Unit disaster recovery plans may not be necessary.

NOTE: Business priority (critical or mission critical business process) requirements are defined in security control CP 1.1.1 (p. 47).

NOTE: Recovery point objective—The targeted maximum time period for which data might be lost as a result of a disruptive event before incurring unacceptable consequences associated with a break in business continuity. Simplified: the acceptable extent of data loss due to a disruptive event.

NOTE: Recovery time objective—The targeted duration of time and degree of business function resumption required following a disruptive event to avoid unacceptable consequences associated with a break in business continuity. Simplified: the acceptable duration of downtime following a disruptive event.

References: *NIST SP 800-53 CP-10*

cont.

cont.

Control CP 2.1.2

Conduct disaster recovery tests.

Level: I | II | III

Requirements:

A. Conduct a data center disaster recovery test or review annually. An acceptable disaster recovery test or review is one of the following:
   1. checklist test; or
   2. structured walkthrough; or
   3. simulation; or
   4. actual disruptive event.

B. Update the disaster recovery plan after testing or review as necessary.

NOTE: IT maintains and tests a disaster recovery plan for central IT resources. Unit disaster recovery plans may not be necessary.

NOTE: Checklist test—A test in which a plan or procedure is reviewed to ensure accuracy and consistency.

NOTE: Structured walkthrough—A test in which a plan or procedure is reviewed step by step with the individuals responsible for its execution to ensure accuracy and consistency.

NOTE: Simulation—A test in which a plan or procedure is executed during a mock disruptive event to ensure its function.

NOTE: Disruptive event—An event that requires the execution of a plan or procedure to recover from operational loss.

References: *NIST SP 800-53 CP-4*

Standard CP 2.2

Backups of IT resources are required.

Control CP 2.2.1

Develop, implement, and maintain a backup plan.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain a backup plan consistent with the unit's recovery point objective (RPO) and recovery time objective (RTO). The backup plan must define:
   1. the institutional and system data that requires backup
   2. the frequency with which backup copies are to be made.

B. Update the backup plan annually or after unit or technological changes.

C. Submit the backup plan to the unit head for review and approval after each update.

NOTE: The Secure UD Security Plan Tool includes guidance and a template for creating a backup plan.

NOTE: RTO and RPO requirements are defined in security control CP 2.1.1 (p. 49).

NOTE: Recovery point objective—The targeted maximum time period for which data might be lost as a result of a disruptive event before incurring unacceptable consequences associated with a break in business continuity. Simplified: the acceptable extent of data loss due to a disruptive event.

NOTE: Recovery time objective—The targeted duration of time and degree of business function resumption required following a disruptive event to avoid unacceptable consequences associated with a break in business continuity. Simplified: the acceptable duration of downtime following a disruptive event.

References: *NIST SP 800-53 CP-9; Secure UD Compliance and Risk Survey question #14*

cont.

cont.

Control CP 2.2.2

Conduct backups.

Level: I | II | III

Requirements:

A. Complete backups consistent with the unit backup plan.
B. Monitor backup logs to ensure that backups are completed as expected without warnings or errors.
C. Maintain a media inventory to track the location of backup data.

References: *NIST SP 800-53 CP-9; Secure UD Compliance and Risk Survey question #14*

Control CP 2.2.3

Conduct backup verification tests.

Level: I | II | III

Requirements:

A. Complete a test of backup media and systems annually or after technological changes to verify media reliability and information integrity.
B. Submit backup test results to the unit head for review and approval.

References: *NIST SP 800-53 CP-9(1); Secure UD Compliance and Risk Survey question #15*

Control CP 2.2.4

Manage critical and mission critical backup storage.

Level: I | II | III

Requirements:

A. Require that critical and mission critical backup copies be stored in a separate facility or in a fire-rated container that is not colocated with the operational system.

NOTE: This security control applies to all critical or mission critical backups irrespective of their classification(s). Criticality is addressed in "Information criticality" (p. 12).

References: *NIST SP 800-53 CP-9*

Data Management — DM—Risk Area 5

Objective DM 1

Data Acquisition

Objective: To collect data with appropriate breadth and depth.

Standard DM 1.1

Data is acquired only if it fulfills an operational requirement.

Control DM 1.1.1

Manage data acquisition.

Level: I | II | III

Requirements:

A. Require that data be collected only if it is necessary to support University activities.
B. Review controls, rules, and procedures that ensure data is acquired only to support University activities.

References: *NIST SP 800-53 DM-1; University Data Governance Policy; Secure UD Compliance and Risk Survey question #16*

Standard DM 1.2

Compliance with laws, regulations, and policies governing data acquisition is ensured.

Control DM 1.2.1

Assess laws, regulations, and policies governing data acquisition.

Level: I | II | III

Requirements:

A. Assess laws, regulations, and policies governing data acquisition including:
   1. the Children's Online Privacy Protection Act (COPPA)
   2. human research informed consent
B. Ensure that data acquisition practices are in compliance with applicable laws, regulations, and policies.
C. Provide web data collection notices. (Technology service providers who collect data via website interfaces must post a customized privacy statement to notify visitors regarding the types and uses of data that is gathered and whether any third parties are involved.)

References: *NIST SP 800-53 AP-1; University Data Governance Policy; Secure UD Compliance and Risk Survey question #16*

Objective	Data Utilization
DM 2	*Objective: To utilize data in support of University missions and business processes.*

Standard DM 2.1 — **Data is utilized only to fulfill an operational requirement.**

Control DM 2.1.1 — **Manage data utilization.** Level: I | II | III

Requirements:

A. Require that data be used only
   1. according to authorization
   2. to support University activities.

B. Review controls, rules, and procedures that ensure data is used only to support University activities.

References: *NIST SP 800-53 UL-1; University Data Governance Policy; Secure UD Compliance and Risk Survey question #17*

Standard DM 2.2 — **Compliance with laws, regulations, and policies governing data utilization is ensured.**

Control DM 2.2.1 — **Assess laws, regulations, and policies governing data utilization.** Level: I | II | III

Requirements:

A. Assess laws, regulations, policies, and contracts governing data use.

B. Ensure that data is used only in accordance with applicable laws, regulations, policies, and contracts.

C. Provide web data privacy statements. (Technology service providers who collect data via website interfaces must post a customized privacy statement to notify users regarding the uses of data that is gathered and whether any third party entities are involved.)

References: *NIST SP 800-53 UL-1; University Data Governance Policy; University Web Privacy Policy; Secure UD Compliance and Risk Survey question #17*

Objective DM 3

Data Maintenance

Objective: To maintain data in compliance with policies.

Standard DM 3.1

University information is classified.

Control DM 3.1.1

Classify University information.

Level: I | II | III

Requirements:

A. Classify all University information according to University policy.

B. Update the University information classifications annually or after relevant legal, business process, or technological changes.

References: *NIST SP 800-53 RA-2; University Information Classification Policy*

Standard DM 3.2

An inventory of IT resources is developed and maintained.

Control DM 3.2.1

Inventory business processes and data.

Level: I | II | III

Requirements:

A. Inventory business processes and the data relevant to those processes. The inventory must include:

1. the business processes of the unit
2. the applications relevant to the business processes
3. the kinds of data relevant to the business processes
4. the classifications of the data relevant to the business processes.

B. Update the inventory annually or after unit or technological changes.

NOTE: IT inventories business processes and data on central IT resources.

References: *NIST SP 800-53 PM-5, SE-1; University Information Security Policy; Secure UD Inventory Tool*

cont.

cont.

Control DM 3.2.2

Inventory IT resources.

Level: I | II | III

Requirements:

A. Inventory IT devices. The inventory must include:
   1. the IT device type
   2. the classifications of the data processed or stored on the device
   3. the criticality of the IT devices
   4. the unique system identifier (serial number, device name, MAC address)
   5. the operating system name and version
   6. the asset owner/assigned user
   7. the local support provider or system administrator
   8. the physical location (or "mobile" for mobile devices)
   9. the network location (IP address for non-mobile devices where possible)
   10. date inventory item was last verified.

B. Update the inventory annually or after unit or technological changes.

NOTE: IT inventories central IT devices.

References: *NIST SP 800-53 CM-8, PM-5, SE-1; University Information Security Policy; Secure UD Inventory Tool; Secure UD Compliance and Risk Survey question #18*

Control DM 3.2.3

Conduct scans to identify Level III information.

Level: I | II | III

Requirements:

A. Complete quarterly scans of systems to identify unencrypted and/or at-risk Level III information. Scans must include:
   1. desktop and laptop computers
   2. network drives.

B. Manage instances of identified Level III information. Management includes:
   1. removing identified Level III information from IT devices
   2. encrypting identified Level III information on IT devices
   3. adding identified Level III information to IT resource inventories
   4. reclassifying IT devices to reflect changes in data inventories.

NOTE: IT scans central IT resources for instances of unencrypted and/or at-risk Level III information.

References: *NIST SP 800-53 PM-5; Secure UD Compliance and Risk Survey question #19, #20*

Standard DM 3.3

Data is retained only for as long as it fulfills an operational requirement.

Control DM 3.3.1

Manage data retention.

Level: I | II | III

Requirements:

A. Require that data be retained only for as long as necessary to fulfill an operational requirement.
B. Review controls, rules, and procedures to ensure that data is retained only for as long as necessary to fulfill an operational requirement.
C. Dispose of unnecessary data in a manner commensurate with its sensitivity.

NOTE: Data disposal requirements are defined in security standard DM 5.3 (p. 62).

References: *NIST SP 800-53 DM-1, DM-2; Secure UD Compliance and Risk Survey question #21*

Standard DM 3.4

Compliance with laws, regulations, and policies governing records retention is ensured.

Control DM 3.4.1

Assess laws, regulations, and policies governing records retention.

Level: I | II | III

Requirements:

A. Complete a records management review annually or after unit, regulatory, or technological changes. The records management review must:
   1. review the applicable University records retention schedules to determine if there have been any changes
   2. assess if there have been any organizational, legal, regulatory, or technological changes that would affect the unit's record retention requirements
   3. define procedures and practices for erasing and archiving data, taking into account laws, policies, regulations, and University needs
   4. erase data when no longer necessary to fulfill an operational requirement or as required by law, regulation, or policy
   5. verify that records are not being disposed of before the authorized disposition date
   6. assess whether the unit needs to take action to be in compliance with all applicable record retention requirements.
B. Submit the records management review results to the unit's data trustee and the University Archivist for review and approval.

NOTE: Data disposal requirements are defined in security standard DM 5.3 (p. 62).

References: *NIST SP 800-53 AU-11, SI-12; Secure UD Compliance and Risk Survey question #21*

cont.

cont.	Control DM 3.4.2	**Manage data accessibility.** **Requirements:** A. Manage the accessibility of data. Management includes: 1. ensuring that data is stored in suitable data storage systems 2. ensuring that published research and underlying data is stored in accessible data storage systems 3. using only University accounts, not personal accounts, for University activities 4. restricting propagation of sensitive data (e.g., consolidate data on a secure system to minimize instances). **NOTE:** The use of only University accounts is important when the University has a legitimate interest in accessing University information for the continuity of University operations or missions. References: *OSTP Public Access Memo (22 Feb. 2013); Secure UD Compliance and Risk Survey question #22*	Level I II III

Objective DM 4

Data Access

Objective: To access data according to authorization and operational requirement.

Standard DM 4.1

Information system access controls are implemented and maintained.

Control DM 4.1.1

Manage information system access controls.

Level: I | II | III

Requirements:

A. Ensure that access controls enforce authorized access to data.

References: *NIST SP 800-53 AC-3*

Standard DM 4.2

Data access is managed.

Control DM 4.2.1

Manage data access authorizations.

Level: I | II | III

Requirements:

A. Manage data access authorizations. Management includes:
   1. authorizing access to University information. Authorized access must be all of the following:
      a. for legitimate interests
      b. to fulfill operational requirements
      c. to the minimum necessary University information
      d. in compliance with laws, regulations, policies, and contractual requirements.
   2. identifying external entities with whom data is shared
   3. ensuring, prior to granting access, that the recipient is authorized to access/view specific information and understands his/her responsibility as a end user
   4. reviewing and reauthorizing access to University information on a periodic basis
   5. revoking access to University information promptly when it is no longer necessary to fulfill an operational requirement.

NOTE: This security control also applies to cloud services.

References: *NIST SP 800-53 AC-1, AC-6, AC-22, PS-4, UL-2; University Data Governance Policy; Secure UD End User Acknowledgement; Contractor Confidentiality Agreement; Secure UD Compliance and Risk Survey question #23, #24*

Standard DM 4.3

Data role assignments are separated.

Control DM 4.3.1

Manage data role assignments.

Level: I | II | III

Requirements:

A. Manage data role assignments. Management includes:
1. separating role request and role approval functions
2. separating data entry and validation, deletion, and approval functions
3. defining roles to facilitate the separation of functions
4. documenting the separation of functions across data roles.

References: *NIST SP 800-53 AC-1, AC-5*

Objective DM 5

Data Protection

Objective: To protect data from unintentional, unlawful, or unauthorized disclosure, alteration, or destruction.

Standard DM 5.1

IT resources at rest are encrypted.

Control DM 5.1.1

Encrypt University information at rest.

Level: III

Requirements:

A. Encrypt University information at rest on electronic storage media. Cryptography must be implemented at the file level.

NOTE: Cryptography requirements are defined in security control DM 5.2.1 (p. 61).

NOTE: Electronic storage media—Any standalone or integrated electronic media that can be used to store data. Includes optical media, magnetic media, disk drives, and flash drives.

References: *NIST SP 800-53 SC-28(1); Secure UD Compliance and Risk Survey question #25*

Control DM 5.1.2

Encrypt portable IT devices.

Level: II III

Requirements:

A. Encrypt portable IT devices with whole disk encryption.

NOTE: Cryptography requirements are defined in security control DM 5.2.1 (p. 61).

NOTE: Portable device—Any IT device that is a laptop computer, mobile device, or removable electronic storage media.

References: *NIST SP 800-53 SC-28(1); Secure UD Compliance and Risk Survey question #26*

Standard DM 5.2

Encryption is managed.

Control DM 5.2.1

Manage cryptosystems.

Level: I | II | III

Requirements:

A. Ensure that cryptosystems implemented for information systems use one of the following University-approved algorithms, protocols, or attributes:
   1. protocols for implementing encrypted Virtual Private Networks (VPNs):
      a. IETF Transport Layer Security (TLS) (RFC 5246) version 1.2 or later preferred, 1.1 or later required
      b. Microsoft Remote Desktop Protocol (RDP) version 6.1 or later
      c. Secure Shell (SSH) (RFC 4251)
      d. IEEE 802.11i-2004 (WPA2).
   2. symmetric key encryption algorithms:
      a. Advanced Encryption Algorithm (AES) (FIPS 197)
      b. Triple Data Encryption Algorithm (3DES) (NIST SP 800-67).
   3. asymmetric key encryption algorithms:
      a. Digital Signature Algorithm (DSA)
      b. RSA Algorithm (ANSI X9.31)
      c. Elliptic Curve Digital Signature Algorithm (ECDSA) (ANSI X9.62).
   4. cryptographic hash algorithms:
      a. Message Digest Algorithm (MD5) (RFC 1321) (RFC 6151)
      b. Secure Hash Algorithms (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) (FIPS 180-4).
   5. encryption key lengths:
      a. symmetric key lengths of at least 256 bits preferred, 128 bits required
      b. asymmetric key lengths of at least 3072 bits preferred, 2048 bits required
         (1) Elliptic Curve Cryptography (ECC) asymmetric key lengths of at least 256 bits.

NOTE: This security control applies to all cryptosystems implemented for University information systems irrespective of the classification(s) of the University information they protect.

NOTE: TLS 1.0 is approved for use with Microsoft RDP as the most secure encryption option currently available.

NOTE: MD-5 and SHA-1 are considered less secure and should not be used in any new implementations. SHA-3 will be approved when released.

References: *NIST SP 800-53 SC-13*

cont.

cont.

Control DM 5.2.2

Manage encryption keys.

Level: I | II | III

Requirements:

A. Manage encryption keys used to protect IT resources. Secure key management includes:
1. using keys for a single purpose, function or application
2. protecting keys at rest from disclosure, misuse, or loss by using appropriate logical and physical access controls
3. consulting with the unit head to select key passwords
4. ensuring that key passwords are strong enough that they cannot be easily guessed
5. storing and transmitting key passwords in a way that does not identify which files they protect
6. distributing asymmetric private keys and all symmetric keys in a manner that ensures their confidentiality and integrity
7. distributing asymmetric public keys in a manner that ensures their integrity
8. rotating keys where required by regulation
9. ensuring continuity of access through key escrow or master keys
10. revoking keys when they are no longer needed.

NOTE: This security control applies to all encryption keys used for IT resources irrespective of the classification(s) of the IT resources they protect.

References: *NIST SP 800-53 SC-12*

Standard DM 5.3

Disposal of IT resources is managed.

Control DM 5.3.1

Manage digital information disposal.

Level: III

Requirements:

A. Dispose of digital files containing Level III information by securely erasing them.

Recommendations:

B. Dispose of digital files containing Level II information by securely erasing them.

References: *NIST SP 800-53 DM-2; Secure UD Compliance and Risk Survey question #27*

Control DM 5.3.2

Manage physical information disposal.

Level: III

Requirements:

A. Dispose of physical documents containing Level III information by securely destroying them through shredding prior to disposal.

B. Implement bulk secure destruction and disposal only through a University-approved destruction and/or disposal service.

Recommendations:

C. Dispose of physical documents containing Level II information by securely destroying them through shredding prior to disposal.

References: *NIST SP 800-53 MP-6*

cont.

cont.

Control
DM 5.3.3

Manage IT device disposal.

Level: I | II | III

Requirements:

A. Securely dispose of University information when disposing of IT devices. Secure University information disposal includes either:
   1. securely erasing University information stored on an IT device
   2. securely destroying electronic storage media.

B. Complete an Equipment Activity web form to request secure IT device disposal. Equipment Activity web forms must:
   1. verify that University information stored on reusable IT devices either:
      a. has been securely erased; or
      b. fulfills an operational requirement of the unit or entity receiving the IT device.
   2. verify that University information stored on unserviceable IT devices either:
      a. has been securely erased; or
      b. has been rendered irrecoverable by completely destroying electronic storage media.

C. Submit Equipment Activity web forms to the unit head for review and approval.

NOTE: Electronic storage media—Any standalone or integrated electronic media that can be used to store data. Includes optical media, magnetic media, disk drives, and flash drives.

NOTE: Complete destruction of an IT device's electronic storage media includes secure destruction of either the IT device that contains the electronic storage media or the electronic storage media itself.

References: *NIST SP 800-53 MP-6; Secure UD Compliance and Risk Survey question #27*

Human Resources — HR—Risk Area 6

Objective HR 1

Awareness and Training

Objective: To educate users about security threats and best practices.

Standard HR 1.1

Employee information security awareness training is provided.

Control HR 1.1.1

Provide employee information security awareness training.

Level: I | II | III

Requirements:

A. Provide employee end users of University information with University-approved information security awareness training annually.
B. Document employee information security awareness training completion status.
C. Ensure that information security training topics are addressed at staff meetings.
D. Provide security awareness resources to assist employees in recognizing and reporting potential indicators of an insider threat.

Recommendations:

E. Require completion of University-approved security awareness training and include completion in employee performance appraisals.

References: *NIST SP 800-53 AT-1, AT-2, AT-2(2), AT-4; Secure UD Compliance and Risk Survey question #28*

Standard HR 1.2

Employee attestation to security agreements is required.

Control HR 1.2.1

Require annual employee Secure UD End User Acknowledgement attestation.

Level: I | II | III

Requirements:

A. Require all end users of University information to attest to the Secure UD End User Acknowledgement annually.

References: *NIST SP 800-53 AT-1, PS-6; University Data Governance Policy; Secure UD End User Acknowledgement; Secure UD Compliance and Risk Survey question #29*

Objective	**Employment Management**
HR 2	*Objective: To ensure due diligence management of employees.*

Standard	**Background checks are performed prior to employment.**
HR 2.1	

Control	**Require background checks for positions with access to Level III information.**	Level
HR 2.1.1		III

Requirements:

A. Require background checks for potential employees who would require access to Level III information.

References: *NIST SP 800-53 PS-3; Secure UD Compliance and Risk Survey question #30*

Standard	**IT resources are recovered.**
HR 2.2	

Control	**Require IT resource recovery.**	Level
HR 2.2.1		I II III

Requirements:

A. Ensure that IT resources are recovered from terminated and transferred employees. Recoverable IT resources include:
   1. IT devices (e.g., University-owned network devices, information systems, laptop computers, or mobile devices)
   2. security access tokens (e.g. fobs) and physical access devices (e.g., keys and ID cards)
   3. Level II and III University information.

B. Identify and report unrecovered IT resources to IT Security and Human Resources for investigation. Reports must be filed:
   1. within five business days past the termination date for voluntary terminations
   2. immediately for involuntary terminations.

References: *NIST SP 800-53 PS-4, PS-5*

Identification and Authentication — IA—Risk Area 7

Objective IA 1

Identification and Authentication

Objective: To securely manage digital identities and authentication processes.

Standard IA 1.1

Authenticated access to IT resources is managed.

Control IA 1.1.1

Require authenticated access to IT resources.

Level: I | II | III

Requirements:

A. Require authentication before granting access to IT resources. Authentication includes:
   1. a password or passcode lock on an IT device
   2. a username and password requirement for applications and systems

B. Require authentication before granting access to:
   1. write Level I information
   2. read or write Level II or Level III information.

NOTE: Read-only access to Level I information is unrestricted and does not require authentication.

References: *NIST SP 800-53 AC-14, IA-2; Secure UD Compliance and Risk Survey question #31, #44*

Control IA 1.1.2

Manage authentication to IT resources.

Level: I | II | III

Requirements:

A. Implement and maintain authentication systems to authenticate access to IT resources. Authentication systems include:
   1. University authentication systems (where practical, University authentication systems must be used)
   2. University-approved authentication systems (only where implementation of University authentication systems is not possible or practical).

B. Require the use of University-approved authentication methods, including:
   1. a password or passcode
   2. a second factor based on something the user has
   3. a biometric (e.g., fingerprint).

NOTE: This control applies to cloud services as well as University-owned or University-managed systems.

NOTE: University-approved—Either: required or permitted by a University contract; or approved by a unit head in the interests of facilitating the unit's administrative, operational, or technical ability to fulfill its missions.

References: *NIST SP 800-53 IA-2; Secure UD Compliance and Risk Survey question #32*

Control IA 1.1.3

Require multi-factor authentication to IT resources.

Level: ~~I~~ | II | III

Requirements:

A. Require multi-factor authentication to IT resources where practical.

References: *NIST SP 800-53 IA-2*

Standard IA 1.2

User accounts are managed.

Control IA 1.2.1

Develop, implement, and maintain a user account management process.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain a user account management process. The user account management process must include:
   1. granting accounts only to users for whom access to IT resources fulfills an operational requirement
   2. assigning account identifiers that uniquely identify individuals
      a. preventing the sharing of accounts
   3. defining account roles and criteria for membership
   4. identifying authorized users, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account
   5. updating account roles appropriately following account-related events:
      a. personnel events that will affect staff account status (e.g., hiring, transfer, or termination)
      b. academic events that will affect student account status (e.g., application, enrollment, or graduation)
      c. events that will affect the status of other types of accounts
      d. security incidents that compromise accounts and will require immediate action.
   6. resetting the account only after verifying the user's identity
   7. disabling and/or removing inactive or unnecessary accounts
   8. requiring the use of only University accounts, not personal accounts, for University activities.

B. Review the account list at least annually.

NOTE: University activities do not include those activities related to individual scholarship, research, or pedagogy.

NOTE: Account list reviews may be manual or automated.

NOTE: Shared accounts do not conform to the requirements of this security control. Shared accounts must be documented as exceptions, and they must be used only as necessary to fulfill an operational requirement. Exception requirements are addressed in security control IS 2.1.2 (p. 33).

NOTE: Separation of duties requirements are defined in security control AS 1.3.1 (p. 40) and security control DM 4.3.1 (p. 59).

References: *NIST SP 800-53 AC-1, AC-2, AC-6, IA-4, PS-4, PS-5; Secure UD Compliance and Risk Survey question #33*

cont.

cont.

Control
IA 1.2.2

Develop, implement, and maintain an administrator account management process.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain an administrator account management process. The administrator account management process must include:
   1. assigning administrator accounts only to specific employees for whom privileged access fulfills an operational requirement
   2. using administrator accounts only for activities that require the use of an account with privileged access (e.g., prohibiting the use of administrator accounts to perform routine tasks that do not require privileged access such as reading email, general web browsing, etc.)
   3. restricting administrator account access and use to employees who have the requisite skills to use privileged access safely
   4. disabling and/or removing inactive or unnecessary accounts
   5. revoking access to administator accounts when it is no longer necessary to fulfill an operational requirement
   6. inventorying administrator accounts. The inventory must include:
      a. all active administrator accounts
      b. all employees with access to each administrator account.

B. Submit the administrator account list to the unit head for review and approval at least annually.

NOTE: Administrator accounts are accounts granted privileged access to system resources (e.g., the UNIX and Mac OS X "root" account, the Windows "administrator" account, database management system "dba" accounts, and service accounts with elevated privilege).

NOTE: Whenever possible, users should not have access to administrator accounts on client systems. If required, separate administrator and user privileges should be used.

NOTE: Administrator account inventories must be maintained by system administrators.

References: *NIST SP 800-53 AC-2, AC-6; Secure UD Compliance and Risk Survey question #43*

Standard IA 1.3

Authentication credentials are managed.

Control IA 1.3.1

Manage passwords.

Level: I | II | III

Requirements:

A. Require that passwords conform to University password guidelines wherever username and password authentication is employed. Passwords must:
   1. be between 12 and 30 characters in length
   2. include at least three of the following character types:
      a. uppercase letters
      b. lowercase letters
      c. numbers
      d. special characters (!, $, ?, etc.)
   3. not be easily guessable.

B. Manage password implementation. Management includes:
   1. ensuring that initial passwords are created only by the University and only after verifying the user's identity
   2. ensuring that default vendor passwords are modified prior to implementation
   3. ensuring that passwords are reset only after verifying the user's identity
   4. ensuring that passwords are not stored in cleartext
   5. denying access to password hashes.

C. Require that passwords not be shared between end users.

D. Require different passwords for user accounts and privileged accounts.

E. Require that University passwords not be used to authenticate to non-UD hosted services or resources.

F. Require that passwords be changed if compromised.

NOTE: Password sharing for shared accounts does not conform to the requirements of this security control. Password sharing must be documented as an exception, and passwords must be shared only as necessary to fulfill an operational requirement. Exception requirements are addressed in security control IS 2.1.2 (p. 33).

References: *NIST SP 800-53 IA-5*

Standard IA 1.4

Secure sessions are enforced.

Control IA 1.4.1

Restrict invalid login attempts.

Level: I | II | III

Requirements:

A. Ensure that information systems protect against unlimited consecutive invalid login attempts. Invalid login protection mechanisms include:
   1. soft account locks: locking accounts automatically when a threshold of consecutive invalid login attempts has been exceeded, using:
      a. a lockout threshold of 10 invalid login attempts
      b. a duration of 10 minutes to limit the impact of denial of service attacks.
   2. out-of-band signaling: sending some message or code outside of the information system to assist in authentication (e.g., an authentication code sent via SMS)
   3. detective logging and response.

References: *NIST SP 800-53 AC-7*

cont.

cont.	Control IA 1.4.2	**Configure inactive authenticated session suspension.** **Requirements:** A. Configure systems to suspend inactive authenticated sessions after a period of inactivity. Session suspensions must: 1. prevent further access to the system 2. be enforced after one of the following conditions: a. 15 minutes of inactivity for client systems and server systems; or b. 5 minutes of inactivity for mobile devices; or c. an interval of inactivity commensurate with sensitivity for applications; or d. a request from the user. 3. persist until the user renews access using established identification and authentication procedures. References: *NIST SP 800-53 AC-11, IA-11*	Level II III

Incident Response — IR—Risk Area 8

Objective IR 1

Incident Response

Objective: To address incidents promptly and appropriately.

Standard IR 1.1

An incident response plan is developed, implemented, and maintained.

Control IR 1.1.1

Develop, implement, and maintain an incident response plan.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain an incident response plan. The incident response plan must:
   1. define reportable incidents
   2. define the steps to be taken to respond to an incident
   3. define roles and responsibilities for incident response.

B. Update the incident response plan annually, after major unit or technological changes, or in response to problems encountered during plan implementation.

NOTE: University incident response procedures are addressed in the University Incident Response Policy.

NOTE: The Secure UD Security Plan Tool includes guidance and a template for creating a unit incident response plan.

References: *NIST SP 800-53 IR-1, IR-4, IR-5, IR-8; University Incident Response Policy; Secure UD Compliance and Risk Survey question #34*

Control IR 1.1.2

Develop, implement, and maintain incident response capabilities.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain an incident response capability that is consistent with the incident response plan. The incident response plan must describe the structure of the incident response capability in terms of role(s) and resources.

NOTE: Incident response plan requirements are defined in security control IR 1.1.1 (p. 71).

References: *NIST SP 800-53 IR-1, IR-4, IR-5, IR-8; University Incident Response Policy*

Standard IR 1.2

Incidents are reported promptly.

Control IR 1.2.1

Require prompt incident reporting.

Level: I | II | III

Requirements:

A. Report suspected or actual incidents promptly according to the process defined in University Incident Response Policy.
   1. In the event that a user suspects that an incident may have occurred or may be imminent, the user must report the incident to the local support provider.
   2. The local support provider must report the incident to IT Security.
   3. If a computer has been stolen, the local support provider must notify Public Safety.

References: *NIST SP 800-53 IR-1, IR-6; University Incident Response Policy*

Physical Security — PE—Risk Area 9

Objective PE 1

IT Resource Physical Security

Objective: To physically protect IT resources in University locations.

Standard PE 1.1

Physical access controls for University locations are implemented and maintained.

Control PE 1.1.1

Implement and maintain physical access controls.

Level: I | II | III

Requirements:

A. Implement, as required by the unit information security plan, controls to enforce authorized physical access to unit locations. Physical access controls may include:
   1. verifying that access is authorized prior to granting access to unit locations
   2. controlling ingress/egress to unit locations using one or more University-approved physical access systems
   3. providing access to public areas within the unit location
   4. labeling nonpublic areas within the unit location as restricted to authorized personnel only
   5. escorting visitors and monitoring visitor activity
   6. securing keys, combinations, and other physical access devices
   7. inventorying physical access devices annually.

NOTE: Examples of ingress/egress controls include locking unit locations outside of operational hours.

NOTE: Physical access devices include keys, key cards, fobs, etc.

References: *NIST SP 800-53 PE-1, PE-2, PE-3, PE-5, PE-6, PE-8; Secure UD Compliance and Risk Survey question #35*

cont.

cont.

Control PE 1.1.2

Manage physical access controls.

Level: I | II | III

Requirements:

A. Manage the use of the physical access controls at unit locations. Management of access controls includes:
   1. developing and maintaining a list of individuals with authorized access to unit locations by
      a. requesting issuance of physical access devices from the unit that controls the unit location's physical access system (e.g., Lock Shop, card access system administrator)
      b. reviewing and approving semiannually the access list detailing authorized facility access by individuals
      c. requesting removal of individuals from the unit location access list when access is no longer necessary to fulfill an operational requirement.
   2. taking unit location access-related actions, including
      a. notifying the unit that controls the unit location's physical access system of security incidents that compromise building access and will require immediate action
      b. notifying management of compromised physical access devices
      c. notifying the unit's data trustee and the Department of Public Safety when master keys (or physical access devices affecting a large number of locks) have been compromised
      d. revoking access from magnetic stripe cards or other access tokens when they are compromised
      e. changing combinations and keys when they are compromised.

NOTE: Physical access devices include keys, key cards, fobs, etc.

NOTE: Approval of access lists must be granted by the unit head responsible for the unit locations to which they pertain.

References: *NIST SP 800-53 PE-1, PE-2, PE-3, PE-5, PE-8*

Standard PE 1.2

IT resources are protected during transportation.

Control PE 1.2.1

Manage transportation of physical media.

Level: III

Requirements:

A. Ensure that physical media is transported securely between facilities by:
   1. transporting physical media in a sealed or locked container (e.g., envelopes, bags, or cases)
   2. using authorized personnel to transport physical media.

NOTE: Physical media includes documents or unencryptable electronic storage media.

NOTE: Electronic storage media—Any standalone or integrated electronic media that can be used to store data. Includes optical media, magnetic media, disk drives, and flash drives.

References: *NIST SP 800-53 MP-5, PE-2, PE-3, PE-5*

Standard PE 1.3

IT resources are protected during use and storage.

Control PE 1.3.1

Manage use and storage of IT devices.

Level: I | II | III

Requirements:

A. Ensure that IT devices are used and stored securely by:
   1. physically locking IT devices kept in public areas to prevent unintentional, unlawful, or unauthorized removal
   2. storing IT devices in locked cabinets, desks, offices, or other access restricted space outside of business hours.

References: *NIST SP 800-53 MP-1, MP-4, PE-5; Secure UD Compliance and Risk Survey question #36*

Control PE 1.3.2

Manage use and storage of documents.

Level: ~~I~~ | II | III

Requirements:

A. Ensure that documents containing Level II or Level III information are used and stored securely by:
   1. storing documents in locked cabinets, desks, offices, or other access restricted space outside of business hours
   2. removing or protecting documents in publicly accessible spaces such as service counters or unattended office spaces colocated with publicly accessible areas.

References: *NIST SP 800-53 MP-2; Secure UD Compliance and Risk Survey question #36*

Objective PE 2

Data Center Protection

Objective: To physically protect University data centers.

Standard PE 2.1

Physical access controls for data centers are implemented and maintained.

Control PE 2.1.1

Implement and maintain additional physical access controls.

Level: I | II | III

Requirements:

A. Implement, as required by the unit information security plan, additional controls to enforce authorized physical access at data centers. Physical access controls may include:
   1. logging ingress/egress to data centers using one or more University-approved physical access systems
   2. monitoring and logging signs of tampering
   3. implementing and monitoring security camera surveillance
   4. locating data centers in rooms with no windows.

NOTE: Examples of ingress/egress controls include locking data centers outside of operational hours.

NOTE: Physical access devices include keys, key cards, fobs, etc.

NOTE: Baseline physical access control requirements are addressed in security control PE 1.1.1 (p. 73).

NOTE: Physical access control management requirements are addressed in security control PE 1.1.2 (p. 74).

References: *NIST SP 800-53 PE-1, PE-2, PE-3, PE-5, PE-6, PE-8; Secure UD Compliance and Risk Survey question #37*

Standard PE 2.2

An alternate power source is implemented and maintained.

Control PE 2.2.1

Implement and maintain an alternate power source.

Level: I | II | III

Requirements:

A. Implement and maintain an alternate, uninterruptible power supply or generator that is commensurate with the criticality of the server systems in the data center and capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

B. Implement and maintain a short-term uninterruptible power supply with the capability to facilitate an orderly shutdown of the information system and/or transition of the information system to long-term alternate power in the event of a primary power source loss.

C. Ensure that installed alternate power sources are inspected at least annually by authorized and qualified inspectors.

NOTE: Minimal requirements are to be determined by the unit as part of its information security plan.

References: *NIST SP 800-53 PE-11; Secure UD Compliance and Risk Survey question #37*

Standard PE 2.3

Fire detection and fire suppression systems are implemented and maintained.

Control PE 2.3.1

Implement and maintain fire detection systems.

Level: I | II | III

Requirements:

A. Implement and maintain automatic fire detection systems that notify responsible personnel in the event of a fire.
B. Ensure that installed fire detection systems are inspected at least annually by authorized and qualified inspectors.

References: *NIST SP 800-53 PE-13; Secure UD Compliance and Risk Survey question #37*

Control PE 2.3.2

Implement and maintain fire suppression systems.

Level: I | II | III

Requirements:

A. Implement and maintain automatic fire suppression systems.
B. Ensure that installed fire suppression systems are inspected at least annually by authorized and qualified inspectors.

References: *NIST SP 800-53 PE-13; Secure UD Compliance and Risk Survey question #37*

Standard PE 2.4

Environmental controls are implemented and maintained.

Control PE 2.4.1

Implement and maintain temperature and humidity controls.

Level: I | II | III

Requirements:

A. Implement and maintain automatic temperature and humidity control systems.
B. Implement and maintain automatic temperature and humidity monitoring systems that notify responsible personnel in the event of a dangerous fluctuation in temperature or humidity.
C. Monitor temperature and humidity control system outputs for non-routine activity.
D. Ensure that installed temperature and humidity control systems are inspected at least annually by authorized and qualified inspectors.

References: *NIST SP 800-53 PE-14; Secure UD Compliance and Risk Survey question #37*

Control PE 2.4.2

Implement and maintain water leakage protection controls.

Level: I | II | III

Requirements:

A. Implement and maintain automatic water leakage detection systems that notify responsible personnel in the event of a leak.
B. Implement and maintain master shutoff or isolation valves that are accessible and known to key personnel.
C. Ensure that installed water leakage protection systems are inspected at least annually by authorized and qualified inspectors.

References: *NIST SP 800-53 PE-15; Secure UD Compliance and Risk Survey question #37*

cont.

cont.	Control PE 2.4.3	**Implement and maintain emergency lighting.** **Requirements:** A. Implement and maintain automatic emergency lighting capability that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility. B. Ensure that installed emergency lighting is inspected at least annually by authorized and qualified inspectors. References: *NIST SP 800-53 PE-12; Secure UD Compliance and Risk Survey question #37*	Level I II III

System and Communication Management — SC—Risk Area 10

Objective SC 1 — Client Management

Objective: To protect client systems.

Standard SC 1.1 — Only the minimum necessary functionality is configured.

Control SC 1.1.1 — Configure critical, mission critical, or Level III client systems with minimum functionality.

Level: I | II | III

Requirements:

A. Configure critical, mission critical, or Level III client systems with only the minimum necessary operational and technical functionality.

B. Remove or disable software or application specific services that are not being utilized or that do not fulfill an operational requirement.

Recommendations:

C. Configure Level I and Level II client systems with only the minimum necessary operational and technical functionality.

NOTE: This security control applies to all critical or mission critical client systems irrespective of their classification(s) and to all Level III client systems irrespective of their criticality. Criticality is addressed in "Information criticality" (p. 12).

References: *NIST SP 800-53 CM-7*

Standard SC 1.2 — System configuration changes are managed.

Control SC 1.2.1 — Develop, implement, and maintain a change management process.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain a change management process for centrally-managed client systems. The change management process may involve:

1. identifying the types of changes to client hardware, software, or firmware that are subject to change management
2. evaluating proposed changes with explicit consideration of the security impact
3. approving or disapproving proposed changes
4. testing approved changes prior to implementation
5. implementing only approved and tested changes
6. documenting change management decisions.

References: *NIST SP 800-53 CM-3*

Standard SC 1.3

Security vulnerabilities are identified, assessed, and remediated.

Control SC 1.3.1

Develop, implement, and maintain patch management procedures.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain procedures for deploying security patches and workarounds. The patch management procedures must include:
   1. monitoring vendor announcements regarding security patches
   2. identifying vulnerabilities through vulnerability scans (optional)
   3. identifying applicable systems for security patches or workarounds
   4. testing security patches or workarounds
   5. installing security patches or workarounds on systems
   6. maintaining a list of systems and the security patches or workarounds they have received
   7. documenting any exceptions to the patch and workaround management process, including a list of unpatched systems.

B. Submit the list of exceptions and unpatched systems to the unit head annually for review and approval.

NOTE: Scans must be reexecuted after patches or workarounds have been deployed for vulnerabilities identified by vulnerability scanning.

References: *NIST SP 800-53 RA-5, SI-2; Secure UD Compliance and Risk Survey question #38*

Control SC 1.3.2

Conduct penetration tests.

Level: III

Requirements:

A. Complete a University-approved penetration test where required by law or regulation to verify the effectiveness of the controls that have been implemented on systems that access, process, store, or transmit Level III information.

B. Assess penetration test results for risk.

C. Remediate identified vulnerabilities.

NOTE: Vulnerability remediation requirements are defined in security control SC 1.3.1 (p. 80) and security control SC 1.4.1 (p. 81).

References: *NIST SP 800-53 CA-8*

Standard SC 1.4

Vendor-supported system components are implemented and maintained.

Control SC 1.4.1

Implement and maintain vendor-supported system components.

Level: I | II | III

Requirements:

A. Implement and maintain current, vendor-supported software and firmware.
B. Verify software and firmware versions are supported and security patches are being released as needed.
C. Update or replace unsupported versions of software or software for which vendors refuse to mitigate vulnerabilities.

References: *NIST SP 800-53 SA-22*

Standard SC 1.5

System and security events are logged and monitored.

Control SC 1.5.1

Log system and security events.

Level: I | II | III

Requirements:

A. Log client system and security events including:
1. account creation, modification, and deletion
2. login (success/failure)
3. password reset activity
4. system startup and shutdown
5. host-based firewall state change (turned on or off)
6. malware or virus detection
7. anti-virus state change (turned on or off).

References: *NIST SP 800-53 AU-2, AU-3, AU-12*

Standard SC 1.6

Secure system boundaries are enforced.

Control SC 1.6.1

Configure an ingress-filtering host-based firewall.

Level: I | II | III

Requirements:

A. Configure firewalls or host-based intrusion prevention systems (HIPS) on client systems to:
1. secure inbound system boundaries
2. log and monitor events
3. block and report malicious activity.

References: *NIST SP 800-53 SC-7; Secure UD Compliance and Risk Survey question #39*

cont.

cont.

Control SC 1.6.2

Configure an egress-filtering host-based firewall.

Level: III

Requirements:

A. Configure firewalls or host-based intrusion prevention systems (HIPS) on client systems that access, process, store, or transmit Level III information to:
   1. secure outbound system boundaries
   2. log and monitor events
   3. block and report malicious activity.

References: *NIST SP 800-53 SC-7; Secure UD Compliance and Risk Survey question #39*

Standard SC 1.7

Anti-virus software is implemented and maintained.

Control SC 1.7.1

Implement and maintain anti-virus software.

Level: I II III

Requirements:

A. Implement University-approved anti-virus software on client systems. Anti-virus software must detect and remove malware by:
   1. scanning all local file systems for malware at least weekly
   2. scanning all new files downloaded from the network or made available through locally attached media immediately, in real time
   3. blocking (quarantining) or deleting any malware identified.
B. Update anti-virus signatures daily and anti-virus software engines at least weekly.

References: *NIST SP 800-53 SI-3; Secure UD Compliance and Risk Survey question #40*

Control SC 1.7.2

Implement and maintain advanced anti-virus software.

Level: III

Requirements:

A. Implement University-approved advanced anti-virus software on client systems that process, store, or transmit Level III information. Anti-virus software must detect and remove malware by:
   1. scanning all local file systems for malware weekly
   2. scanning all new files downloaded from the network or made available through locally attached media immediately, in real time
   3. blocking (quarantining) or deleting any malware identified.
B. Update anti-virus software engines at least daily.

References: *NIST SP 800-53 SI-3; Secure UD Compliance and Risk Survey question #41*

Standard SC 1.8

Clients are managed.

Control SC 1.8.1

Assign local support providers to client systems.

Level: I | II | III

Requirements:

A. Appoint at least one local support provider (LSP) for each client system used for University activities. Each LSP must configure and support the client systems for which he or she is responsible. The following conditions apply to LSP designations:
   1. An end user may decline LSP appointments for his or her client system and instead fulfill that role himself or herself.
   2. If no LSP is designated, the role will default to IT.

B. Ensure continuity of support over systems by ensuring that at least one LSP is assigned to each client system at all times.

C. Submit a list of LSPs to IT for review whenever LSP appointments change.

Recommendations:

D. Require that administrative and Level III client systems be centrally managed by the unit or IT.

NOTE: Change of LSP appointment includes initial LSP appointment to an IT device, LSP appointment to a new IT device, and change of LSP appointment for an existing IT device.

References: *NIST SP 800-53 CM-3; Secure UD Compliance and Risk Survey question #42*

Standard SC 1.9

Maintenance is managed.

Control SC 1.9.1

Manage third-party maintenance.

Level: I | II | III

Requirements:

A. Manage off-site maintenance of University-owned client systems. Management includes:
   1. requiring management or unit IT staff authorization of vendor and third party staff performing maintenance
   2. requiring management approval prior to the removal of client systems from University's facilities
   3. removing University information from client systems prior to removal from University buildings or workspaces
   4. documenting off-site removal of client systems. Maintenance documentation must include:
      a. client name
      b. date/time
      c. approval
      d. destination
      e. reason for maintenance.

NOTE: Data disposal requirements are defined in security standard DM 5.3 (p. 62).

References: *NIST SP 800-53 MA-2, MA-5*

Standard	System clock synchronization is enforced.	
SC 1.10		
Control SC 1.10.1	**Configure system clocks.** **Requirements:** A. Configure client system clocks using a reliable time source. References: *NIST SP 800-53 AU-8*	Level: I II III

Objective	Mobile Device Management
SC 2	*Objective: To protect mobile devices.*

Standard SC 2.1 — Only the minimum necessary functionality is configured.

Control SC 2.1.1 — Configure mobile devices with minimum functionality.

Level: II III

Recommendations:

A. Configure mobile devices with only the minimum necessary technical and operational functionality.

B. Remove or disable software or application specific services that are not being utilized or that do not fulfill an operational requirement.

NOTE: This security control is strongly recommended for mobile devices that process, store, or transmit Level III information.

References: *NIST SP 800-53 CM-7*

Standard SC 2.2 — Remote security features are configured.

Control SC 2.2.1 — Configure automatic secure erase.

Level: III

Requirements:

A. Configure mobile devices that process, store, or transmit Level III information to securely erase all University information from the mobile device after 10 consecutive failed authentication attempts.

References: *NIST SP 800-53 AC-7; Secure UD Compliance and Risk Survey question #44*

Control SC 2.2.2 — Configure remote lock, locate, and secure erase.

Level: III

Requirements:

A. Configure mobile devices that process, store, or transmit Level III information such that they can be remotely:

1. locked until a user reauthenticates access to the device
2. located if lost or stolen
3. securely erased.

NOTE: Remote secure erasure of a mobile device's data may be requested only by the device owner or management.

References: *NIST SP 800-53 AC-7; Secure UD Compliance and Risk Survey question #44*

Standard SC 2.3

Security vulnerabilities are identified, assessed, and remediated.

Control SC 2.3.1

Develop, implement, and maintain patch management procedures.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain procedures for deploying security patches and workarounds. The patch management procedures must include:
   1. monitoring vendor announcements regarding security patches
   2. identifying applicable systems for security patches or workarounds
   3. installing security patches or workarounds on systems in a timely manner.

References: *NIST SP 800-53 SI-2*

Standard SC 2.4

Vendor-supported system components are implemented and maintained.

Control SC 2.4.1

Implement and maintain vendor-supported system components.

Level: I | II | III

Requirements:

A. Implement and maintain current, vendor-supported software and firmware.
B. Verify software and firmware versions are supported and security patches are being released as needed.
C. Update or replace unsupported versions of software or software for which vendors refuse to mitigate vulnerabilities.

References: *NIST SP 800-53 SA-22*

Standard SC 2.5

Mobile devices are managed.

Control SC 2.5.1

Assign local support providers to mobile devices.

Level: I | II | III

Requirements:

A. Appoint at least one local support provider (LSP) for each mobile device used for University activities. Each LSP must configure and support the mobile devices for which he or she is responsible. The following conditions apply to LSP designations:
   1. An end user may decline LSP appointments for his or her mobile device and instead fulfill that role himself or herself.
   2. If no LSP is designated, the role will default to IT.
B. Ensure continuity of support over systems by ensuring that at least one LSP is assigned to each mobile device at all times.
C. Submit a list of LSPs to IT for review whenever LSP appointments change.

NOTE: Change of LSP appointment includes initial LSP appointment to an IT device, LSP appointment to a new IT device, and change of LSP appointment for an existing IT device.

References: *NIST SP 800-53 CM-3*

Standard SC 2.6

Maintenance is managed.

Control SC 2.6.1

Manage third-party maintenance.

Level: I | II | III

Requirements:

A. Manage off-site maintenance of University-owned mobile devices by:
   1. requiring management or unit IT staff authorization of vendor and third party staff performing maintenance on mobile devices
   2. requiring management approval prior to submitting the mobile device for maintenance
   3. removing University information from mobile devices prior to submitting the mobile device for maintenance
   4. documenting off-site removal of mobile devices. Maintenance documentation must include:
      a. device name
      b. date/time
      c. approval
      d. destination
      e. reason for maintenance.

NOTE: Data disposal requirements are defined in security standard DM 5.3 (p. 62).

References: *NIST SP 800-53 MA-2, MA-5*

Objective SC 3

Server Management

Objective: To protect server systems.

Standard SC 3.1

Only the minimum necessary functionality is configured.

Control SC 3.1.1

Configure server systems with minimum functionality.

Level: I | II | III

Requirements:

A. Configure server systems with only the minimum necessary operational and technical functionality.

B. Remove or disable software or application specific services that are not being utilized or that do not fulfill an operational requirement.

References: *NIST SP 800-53 CM-7; Secure UD Compliance and Risk Survey question #45*

Standard SC 3.2

System configuration changes are managed.

Control SC 3.2.1

Develop, implement, and maintain a change management process for critical, mission critical, or Level III server systems.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain a change management process for critical, mission critical, or Level III server systems. The change management processes may involve:

1. identifying the types of changes to server system hardware, software, or firmware that are subject to change management
2. evaluating proposed changes with explicit consideration of the security impact
3. approving or disapproving proposed changes
4. testing approved changes prior to implementation
5. implementing only approved and tested changes
6. documenting change management decisions.

NOTE: This security control applies to all critical or mission critical server systems irrespective of their classification(s) and to all Level III server systems irrespective of their criticality. Criticality is addressed in "Information criticality" (p. 12).

References: *NIST SP 800-53 CM-3*

Standard SC 3.3

Security vulnerabilities are identified, assessed, and remediated.

Control SC 3.3.1

Develop, implement, and maintain patch management procedures.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain procedures for deploying security patches and workarounds. The patch management procedures must include:
   1. monitoring vendor announcements regarding security patches
   2. identifying vulnerabilities through vulnerability scans
   3. identifying applicable systems for security patches or workarounds
   4. testing security patches or workarounds
   5. installing security patches or workarounds on systems
   6. maintaining a list of systems and the security patches or workarounds they have received
   7. documenting any exceptions to the patch and workaround management process, including a list of unpatched systems.
B. Submit the list of exceptions and unpatched systems to the unit head annually for review and approval.

NOTE: Scans must be reexecuted after patches or workarounds have been deployed for vulnerabilities identified by vulnerability scanning.

References: *NIST SP 800-53 RA-5, SI-2; Secure UD Compliance and Risk Survey question #46*

Control SC 3.3.2

Conduct vulnerability scans.

Level: I | II | III

Requirements:

A. Complete a University-approved vulnerability scan at least monthly to ensure that vulnerabilities are identified and managed. Vulnerability scans must :
   1. measure vulnerability severity using the Common Vulnerability Scoring System (CVSS) to help determine the urgency and priority of response.
   2. be performed using a University-approved vulnerability scanning tool.
B. Assess vulnerability scan results for risk.
C. Remediate identified vulnerabilities.
D. Update vulnerability databases and the vulnerability scanning engine weekly.
E. Submit vulnerability scan reports to the unit head for review and approval.

NOTE: Vulnerability remediation requirements are defined in security control SC 3.3.1 (p. 89) and security control SC 3.4.1 (p. 90).

References: *NIST SP 800-53 RA-5; Secure UD Compliance and Risk Survey question #46*

cont.

cont.

Control SC 3.3.3

Conduct penetration tests.

Level: III

Requirements:

A. Complete a University-approved penetration test where required by law or regulation to verify the effectiveness of the controls that have been implemented on systems that access, process, store, or transmit Level III information.
B. Assess penetration test results for risk.
C. Remediate identified vulnerabilities.

NOTE: Vulnerability remediation requirements are defined in security control SC 3.3.1 (p. 89) and security control SC 3.4.1 (p. 90).

References: *NIST SP 800-53 CA-8*

Standard SC 3.4

Vendor-supported system components are implemented and maintained.

Control SC 3.4.1

Implement and maintain vendor-supported system components.

Level: I | II | III

Requirements:

A. Implement and maintain current, vendor-supported software and firmware.
B. Verify software and firmware versions are supported and security patches are being released as needed.
C. Update or replace unsupported versions of software or software for which vendors refuse to mitigate vulnerabilities.

References: *NIST SP 800-53 SA-22*

Standard SC 3.5

System and security events are logged and monitored.

Control SC 3.5.1

Log system and security events.

Level: I | II | III

Requirements:

A. Log server system and security events where possible, including:
   1. account creation, modification, and deletion
   2. login (success/failure)
   3. password reset activity
   4. system startup and shutdown
   5. host-based firewall state change (turned on or off)
   6. malware or virus detection
   7. anti-virus state change (turned on or off).

References: *NIST SP 800-53 AU-2, AU-3, AU-12; Secure UD Compliance and Risk Survey question #47*

cont.

cont.

Control SC 3.5.2

Maintain remote copies of critical, mission critical, or Level III system logs.

Level: I II III

Requirements:

A. Maintain remote copies of critical, mission critical, or Level III server system and security logs.
B. Protect remote copies of logs from unintentional, unlawful, or unauthorized disclosure, alteration, or destruction.

NOTE: This security control applies to all critical or mission critical server systems irrespective of their classification(s) and to all Level III server systems irrespective of their criticality. Criticality is addressed in "Information criticality" (p. 12).

References: *NIST SP 800-53 AU-2, AU-3, A-4(1), AU-9; Secure UD Compliance and Risk Survey question #47*

Control SC 3.5.3

Review critical, mission critical, or Level III system logs.

Level: I II III

Requirements:

A. Review critical, mission critical, or Level III server log data. Reviews may include:
   1. routine manual reviews
   2. automated analysis and notification.
B. Identify abnormal or suspicious events, system alerts, and audit log failures.
C. Assess abnormal or suspicious log entries for risk.
D. Remediate identified vulnerabilities.

NOTE: This security control applies to all critical or mission critical server systems irrespective of their classification(s) and to all Level III server systems irrespective of their criticality. Criticality is addressed in "Information criticality" (p. 12).

NOTE: It is recommended that 24/7 automated log analysis and notification features be employed where practicable.

NOTE: Vulnerability remediation requirements are defined in security control SC 3.3.1 (p. 89) and security control SC 3.4.1 (p. 90).

References: *NIST SP 800-53 AU-6, AU-7; Secure UD Compliance and Risk Survey question #47*

Standard SC 3.6

Secure system boundaries are enforced.

Control SC 3.6.1

Configure an ingress-filtering host-based firewall.

Level: I II III

Requirements:

A. Configure firewalls on server systems to:
   1. restrict and monitor inbound communications to the server system, when technically possible, by:
      a. denying inbound network traffic by default
      b. allowing inbound network traffic according to justification.

References: *NIST SP 800-53 SC-7; Secure UD Compliance and Risk Survey question #48*

cont.

cont.

Control SC 3.6.2

Configure an egress-filtering host-based firewall.

Level: III

Requirements:

A. Configure firewalls on server systems that access, process, store, or transmit Level III information to:
   1. restrict and monitor outbound communications from the server system by:
      a. denying outbound network traffic by default
      b. allowing outbound network traffic according to justification.

References: *NIST SP 800-53 SC-7; Secure UD Compliance and Risk Survey question #48*

Control SC 3.6.3

Conduct firewall rule reviews.

Level: III

Requirements:

A. Complete a firewall rule review at least annually or after a technical change to a server system.
B. Revoke unjustified firewall rules not explicitly approved by the unit head.
C. Submit firewall rule review results to the unit head for review and approval.

References: *NIST SP 800-53 SC-7*

Standard SC 3.7

Unintentional, unlawful, or unauthorized system changes are identified, assessed, and remediated.

Control SC 3.7.1

Monitor critical or mission critical server system modification and integrity.

Level: I | II | III

Requirements:

A. Configure host-based intrusion prevention or detection software (HIPS/HIDS) to detect unintentional, unlawful, or unauthorized changes to:
   1. critical or mission critical OS, web, database and application files
   2. system logs
   3. system configuration and parameter files.

NOTE: This security control applies to all critical or mission critical server systems irrespective of their classification(s) and to all Level III server systems irrespective of their criticality. Criticality is addressed in "Information criticality" (p. 12).

References: *NIST SP 800-53 SI-4, SI-7*

Standard SC 3.8

Server systems are managed.

Control SC 3.8.1

Assign administrators to server systems.

Level: I | II | III

Requirements:

A. Appoint at least one administrator for each server system used for University activities. The administrator must configure and support the server systems for which he or she is responsible.

B. Ensure continuity of support over server systems by ensuring that at least one administrator is assigned to each server system at all times.

C. Submit a list of administrators to IT for review whenever administrator appointments change.

NOTE: Change of administrator appointment includes initial administrator appointment to a server system, administrator appointment for new server systems, and change of adminstrator appointment for an existing server system.

References: *NIST SP 800-53 CM-3; Secure UD Compliance and Risk Survey question #49*

Standard SC 3.9

Maintenance is managed.

Control SC 3.9.1

Manage third-party maintenance.

Level: I | II | III

Requirements:

A. Manage off-site maintenance of server systems by:

1. requiring management or unit IT staff authorization of vendor and third party staff performing maintenance on server systems
2. requiring management approval prior to the removal of server systems from University's facilities
3. removing University information from server systems prior to removal from University buildings or workspaces
4. documenting off-site removal of server systems. Maintenance documentation must include:
   a. server name
   b. date/time
   c. approval
   d. destination
   e. reason for maintenance.

NOTE: Data disposal requirements are defined in security standard DM 5.3 (p. 62).

References: *NIST SP 800-53 MA-2, MA-5, PE-16*

Standard SC 3.10

System clock synchronization is enforced.

Control SC 3.10.1

Configure system clocks.

Level: I | II | III

Requirements:

A. Configure server system clocks using a reliable time source.

References: *NIST SP 800-53 AU-8*

Standard SC 3.11

Server documentation is developed and maintained.

Control SC 3.11.1

Develop and maintain critical, mission critical, or Level III server documentation.

Level: I | II | III

Requirements:

A. Develop and maintain server documentation for server systems that access, process, store, or transmit critical, mission critical, or Level III information. Server documentation must:
   1. provide a general description, purpose and primary function of the server for the unit
   2. identify the primary and backup server owners, responsible security individual(s) and their contact information
   3. identify the primary business applications, the responsible owners and their contact information
   4. define explicitly the boundaries for the server and the supporting infrastructure (system environment)
   5. define and diagram the relationships and connections to other information systems, the data exchanged, and any third party agreements in place
   6. identify any applicable laws or regulations governing the protection of the data or system
   7. identify any Level III information stored or transmitted by the server, its location, and data flow
   8. identify the security controls in place and those planned to protect the server.

B. Update server documentation after technological changes.

NOTE: This security control applies to all critical or mission critical server systems irrespective of their classification(s) and to all Level III server systems irrespective of their criticality. Criticality is addressed in "Information criticality" (p. 12).

References: *NIST SP 800-53 CA-3, CM-8, PL-2, PM-5*

Standard SC 3.12

Information flow is managed.

Control SC 3.12.1

Develop, implement, and maintain information flow management policies.

Level: III

Requirements:

A. Develop, implement, and maintain information flow management policies for Level III information. Information flow management policies must:
   1. define how Level III information flow within systems and between interconnected systems will be controlled
   2. apply based on either:
      a. information characteristics, including:
         (1) label
         (2) data type or format
      b. information path, including:
         (1) source
         (2) destination.

C. Update information flow management policies after technological changes.

References: *NIST SP 800-53 AC-4*

Standard SC 3.13

Database management services are configured.

Control SC 3.13.1

Configure database management systems.

Level: I | II | III

Requirements:

A. Configure database management systems securely. Secure configuration includes:
   1. expiring passwords for and locking all default database accounts
   2. ensuring the service account under which the database server runs does not allow direct (interactive) login to the operating system
   3. assigning privileges to database accounts only as they fulfill operational requirements
   4. creating/requiring unique individual accounts for all users that require direct database access
   5. ensuring applications have rights and access to only the minimum necessary data
   6. limiting use of database administrator accounts to only administrative activities
   7. creating and requiring unique database accounts for applications requiring database access.

cont.

References: *NIST SP 800-53 AC-23*

cont.

Control SC 3.13.2

Configure advanced database management systems.

Level: III

Requirements:

A. Configure database management systems that access, process, store, or transmit Level III information securely. Secure configuration includes:
   1. ensuring that database server systems are on a dedicated server, not hosted on the associated web or application server systems
   2. separating development and production databases; separate testing/QA databases when implemented in the environment
   3. permitting database administrators to have the ability to directly modify the database through command access (non-programmatic)
   4. restricting direct access from untrusted networks to VPN or similar encrypted remote access strategies and from only University-owned devices
   5. reviewing database roles, role privileges and user role assignments on an annual basis and verify privileges are granted according to the user's assigned roles
   6. removing sample databases and accounts from production databases
   7. locking database user account after 10 failed database connections with no time limit
   8. turning on database auditing, at a minimum, for:
      a. the creation, alteration, or deletion of database accounts, storage structures, objects, and tables
      b. the enabling or disabling of and any changes to audit functionality
      c. granting and revoking of access rights
      d. connection failures.

References: *NIST SP 800-53 AC-23*

Standard SC 3.14

Name and address resolution services are managed.

Control SC 3.14.1

Manage secure name and address resolution.

Level: I | II | III

Requirements:

A. Develop and maintain DNS server documentation, including:
   1. the specific function of the DNS server
   2. what networks will be able to query each server
   3. how updates will be performed.
B. Implement logical separation of external and internal DNS severs and/or services.
C. Restrict zone transfers to only approved server systems with a justified need.

References: *NIST SP 800-53 SC-20*

Standard SC 3.15

The effects of denial of service attacks are limited.

Control SC 3.15.1

Implement and maintain denial of service protection.

Level: I | II | III

Requirements:

A. Ensure that server systems protect against or limit the effects of denial of service attacks. Denial of service attacks may include:
   1. system level connection/request flooding
   2. resource exhaustion (CPU, disk, memory)
   3. account lock out by employing techniques including:
      a. resource, connection and account monitoring
      b. procedures to block offending IP addresses, limit or meter transaction flow, limiting user connections, metered account lockout, communication to end users and other procedures as indicated in an incident response plan or by management, when applicable.

References: *NIST SP 800-53 SC-5*

Objective SC 4

Network Management

Objective: To protect networks and network devices.

Standard SC 4.1

Only the minimum necessary functionality is configured.

Control SC 4.1.1

Disable unauthorized ports.

Level: I | II | III

Requirements:

A. Disable unauthorized network ports for insecure network protocols.

References: *NIST SP 800-53 CM-7*

Control SC 4.1.2

Assign public IP addresses only as necessary.

Level: I | II | III

Requirements:

A. Assign public IP addresses only as necessary. Private IP addresses should be assigned unless public IP addresses are needed.

References: *NIST SP 800-53 AC-17*

Standard SC 4.2

System configuration changes are managed.

Control SC 4.2.1

Develop, implement, and maintain a change management process.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain a change management process for network devices, components, products, and rule sets. The change management process may involve:

1. identifying the types of changes to network devices, components, and products that are subject to change management
2. evaluating proposed changes with explicit consideration of the security impact
3. approving or disapproving changes proposed changes
4. testing approved changes prior to implementation
5. implementing only approved managed changes
6. documenting change management decisions.

References: *NIST SP 800-53 CM-3*

Standard SC 4.3

Security vulnerabilities are identified, assessed, and remediated.

Control SC 4.3.1

Develop, implement, and maintain patch management procedures.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain procedures for deploying security patches and workarounds. The patch management procedures must include:
   1. monitoring vendor announcements regarding security patches
   2. identifying vulnerabilities through vulnerability scans
   3. identifying applicable systems for security patches or workarounds
   4. testing security patches or workarounds
   5. installing security patches or workarounds on systems
   6. documenting any exceptions to the patch and workaround management process, including a list of unpatched systems.

NOTE: Scans must be reexecuted after patches or workarounds have been deployed for vulnerabilities identified by vulnerability scanning.

References: *NIST SP 800-53 RA-5, SI-2*

Control SC 4.3.2

Conduct vulnerability scans.

Level: I | II | III

Requirements:

A. Complete a University-approved vulnerability scan at least monthly to ensure that vulnerabilities are identified and managed. Vulnerability scans must measure vulnerability severity using the Common Vulnerability Scoring System (CVSS) to help determine the urgency and priority of response.
B. Assess vulnerability scan results for risk.
C. Remediate identified vulnerabilities.
D. Update vulnerability databases and the vulnerability scanning engine weekly.
E. Submit vulnerability scan reports to the unit head for review and approval.

NOTE: Vulnerability remediation requirements are defined in security control SC 4.3.1 (p. 99) and security control SC 4.4.1 (p. 100).

References: *NIST SP 800-53 RA-5*

Control SC 4.3.3

Conduct penetration tests.

Level: I | II | III

Requirements:

A. Complete a University-approved penetration test periodically to verify the effectiveness of the controls that have been implemented on the network.
B. Assess penetration test results for risk.
C. Remediate identified vulnerabilities.

NOTE: Vulnerability remediation requirements are defined in security control SC 4.3.1 (p. 99) and security control SC 4.4.1 (p. 100).

References: *NIST SP 800-53 CA-8*

Standard SC 4.4

Vendor-supported system components are implemented and maintained.

Control SC 4.4.1

Implement and maintain vendor-supported system components.

Level: I | II | III

Requirements:

A. Implement and maintain current, vendor-supported software and firmware.
B. Verify software and firmware versions are supported and security patches are being released as needed.
C. Update or replace unsupported versions of software or software for which vendors refuse to mitigate vulnerabilities.

References: *NIST SP 800-53 SA-22*

Standard SC 4.5

System and security events are logged and monitored.

Control SC 4.5.1

Log network and security events.

Level: I | II | III

Requirements:

A. Log network and security events where possible, including:
   1. device startup and shutdown
   2. device date/time modification
   3. device authentication and authorization attempts
   4. device alert, critical or mission critical, error, and warning condition messages
   5. device notice/significant event condition messages.

NOTE: Network audit events must be sufficient to determine attribution (NAT address translation logs, static log source address, etc.) and support security incident response and investigation activities including date/time, source and destination address, port and protocol.

References: *NIST SP 800-53 AU-2, AU-3, AU-12*

Control SC 4.5.2

Maintain remote copies of logs.

Level: I | II | III

Requirements:

A. Maintain remote copies of network and security logs.
B. Protect remote copies of logs from unintentional, unlawful, or unauthorized disclosure, alteration, or destruction.

References: *NIST SP 800-53 AU-2, AU-3*

cont.

cont.

Control SC 4.5.3

Review logs.

Level: I II III

Requirements:

A. Implement and maintain automated log analysis and notification features 24/7.
B. Identify abnormal or suspicious events, system alerts, and audit log failures.
C. Assess abnormal or suspicious log entries for risk.
D. Remediate identified vulnerabilities.

NOTE: Vulnerability remediation requirements are defined in security control SC 4.3.1 (p. 99) and security control SC 4.4.1 (p. 100).

References: *NIST SP 800-53 AU-6, AU-7*

Standard SC 4.6

Secure network boundaries are enforced.

Control SC 4.6.1

Configure a network firewall.

Level: I II III

Requirements:

A. Configure firewalls on networks to:
   1. restrict and monitor inbound and outbound communications as appropriate at the network and/or subnet levels.

References: *NIST SP 800-53 SC-7*

Control SC 4.6.2

Conduct a firewall rule review.

Level: I II III

Requirements:

A. Complete a firewall rule review at least annually or after a significant technical change to the network.
B. Revoke unjustified firewall rules not explicitly approved by the unit head.
C. Submit firewall rule review results to the unit head for review and approval.

References: *NIST SP 800-53 SC-7*

Control SC 4.6.3

Implement and maintain separate production and management networks.

Level: I II III

Requirements:

A. Implement boundary control devices to logically separate:
   1. IT administration environments from general purpose client and server environments
   2. management or service environments dedicated for system management from general purpose client and server environments.

References: *NIST SP 800-53 SC-7*

Standard SC 4.7

Unintentional, unlawful, or unauthorized network access is identified, assessed, and remediated.

Control SC 4.7.1

Implement perimeter intrusion detection.

Level: I | II | III

Requirements:

A. Configure an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) at the network perimeter to:
   1. analyze traffic and event patterns for malicious intent
   2. use the traffic/event baselines to tune system-monitoring devices to reduce the number of false positives and the number of false negatives
   3. heighten the level of information system monitoring activity for imminent threats to unit operations and for the University's critical or mission critical server systems.

References: *NIST SP 800-53 SI-4*

Standard SC 4.8

IT devices are uniquely identified prior to provisioning network access.

Control SC 4.8.1

Identify IT devices prior to provisioning network access.

Level: I | II | III

Requirements:

A. Require that IT devices be registered prior to provisioning network access.
B. Identify IT devices by the unique Media Access Control (MAC) address for the communications interface device.
C. Restrict IP addresses via DHCP to only registered devices.

References: *NIST SP 800-53 IA-3*

Standard SC 4.9

Maintenance is managed.

Control SC 4.9.1

Manage third-party maintenance.

Level: I | II | III

Requirements:

A. Manage off-site maintenance of network devices by:
   1. requiring management or unit IT staff authorization of vendor and third party staff performing maintenance on network devices
   2. requiring management approval prior to the removal of network devices from University's facilities
   3. removing University information from network devices prior to removal from University buildings or workspaces
   4. documenting off-site removal of network devices. Maintenance documentation must include:
      a. device name
      b. date/time
      c. approval
      d. destination
      e. reason for maintenance.

NOTE: Data disposal requirements are defined in security standard DM 5.3 (p. 62).

References: *NIST SP 800-53 MA-2, MA-5*

Standard SC 4.10

System clock synchronization is enforced.

Control SC 4.10.1

Synchronize system clocks.

Level: I | II | III

Requirements:

A. Configure network device system clocks using a reliable time source.

References: *NIST SP 800-53 AU-8*

Standard SC 4.11

Network documentation is developed and maintained.

Control SC 4.11.1

Develop and maintain network documentation.

Level: I | II | III

Requirements:

A. Develop and maintain network documentation and/or diagrams depicting:
   1. network access and control points
   2. logical networks (VLANs)
   3. network devices
   4. interconnections between logical networks.

B. Update network documentation after technological changes.

References: *NIST SP 800-53 CM-8, PM-5*

Standard SC 4.12

Information flow is managed.

Control SC 4.12.1

Develop, implement, and maintain information flow management policies.

Level: I | II | III

Requirements:

A. Develop, implement, and maintain information flow management policies for information. Information flow management policies must:
   1. define how information flow on the network will be controlled
   2. apply based on either:
      a. information characteristics, including:
         (1) label
         (2) data type or format
      b. information path, including:
         (1) source
         (2) destination.

C. Update information flow management policies after technological changes.

References: *NIST SP 800-53 AC-4*

Standard SC 4.13

Secure wireless access is enforced.

Control SC 4.13.1

Implement wireless network protection.

Level: ~~I~~ | II | III

Requirements:

A. Ensure that secure authentication and encryption protect 802.11 wireless access to internal systems.

References: *NIST SP 800-53 AC-18*

Control SC 4.13.2

Manage wireless networks.

Level: ~~I~~ | ~~II~~ | III

Requirements:

A. Prohibit the use of ad-hoc, unmanaged, or consumer grade 802.11 wireless access points in environments that process, store, or transmit Level III information.

References: *NIST SP 800-53 AC-18*

Objective SC 5

Transmission and Communication Management

Objective: To protect communication systems.

Standard SC 5.1

Spam filters are configured.

Control SC 5.1.1

Configure spam filters.

Level: I | II | III

Requirements:

A. Configure spam filters for messaging services to:
   1. detect spam in inbound and outbound messages or message attachments
   2. block, quarantine, or remove spam.

B. Update spam filters at least weekly.

References: *NIST SP 800-53 SI-8*

Standard SC 5.2

Anti-virus software is implemented and maintained.

Control SC 5.2.1

Implement and maintain anti-virus software.

Level: I | II | III

Requirements:

A. Implement University-approved anti-virus software on messaging systems. Anti-virus software must:
   1. scan all new messages and attachments immediately, in real time
   2. block, quarantine, or remove any malware identified
   3. block attachments with known harmful file extensions.

B. Update anti-virus signatures daily and anti-virus scanning engines at least weekly.

References: *NIST SP 800-53 SI-3*

Standard SC 5.3

Mail relays are managed.

Control SC 5.3.1

Manage mail relays.

Level: I | II | III

Requirements:

A. Manage which information systems can connect to mail relays directly.

References: *NIST SP 800-53 CM-2, CM-6*

Standard SC 5.4

University information in transmission is securely transmitted.

Control SC 5.4.1

Securely transmit Level III information.

Level: III

Requirements:

A. Securely electronically transmit Level III information. Secure transmission includes:
   1. using encrypted transmission protocols
   2. encrypting attachments containing Level III information
   3. using required official portals for transmitting Level III information.

References: *NIST SP 800-53 SC-8; Secure UD Compliance and Risk Survey question #50*

Standard SC 5.5

Voice over Internet Protocol services are managed.

Control SC 5.5.1

Implement Voice over Internet Protocol protection.

Level: I | II | III

Requirements:

A. Configure Voice over Internet Protocol (VoIP) services to protect VoIP traffic. VoIP services must:
   1. be designed using a secure network architecture for the specified VoIP standard/protocol (ITU-T H.323, IETF's SIP, etc,) based on the DISA VoIP STIG, NIST SP 800-58 or other industry standard secure VoIP architecture
   2. ensure that core VoIP components reside on a separate VLAN from the data network
   3. ensure that VoIP telephones are VLAN-capable and that this function is enabled and assigned to the VoIP VLAN segment
   4. ensure that VoIP telephones with built-in data network ports enabled must configure the port on the data VLAN
   5. ensure filtering is implemented between the IP telephony network and the IP data network to provide separation.

References: *NIST SP 800-53 SC-19*

Standard SC 5.6

Collaborative computing is managed.

Control SC 5.6.1

Manage collaborative computing.

Level: I | II | III

Requirements:

A. Manage collaborative computing applications, services, systems, or devices. Management includes:
   1. providing a visible indication of use to users physically present (e.g., light or tone)
   2. requiring explicit, local user interaction (automatic answering or connection must be disabled).

NOTE: This security control applies to instant messaging (IM) and Voice over Internet Protocol (VoIP).

References: *NIST SP 800-53 SC-15*

Standard SC 5.7

Secure remote access is enforced.

Control SC 5.7.1

Manage remote access.

Level: ~~I~~ II III

Requirements:

A. Require the use of secure protocols when remotely accessing Level II or Level III IT resources. Secure protocols include:
   1. secure shell (SSH)
   2. virtual private network (VPN).

B. Protect information about remote access mechanisms from unintentional, unlawful, or unauthorized disclosure.

C. Revoke remote access authorization promptly when it is no longer needed to fulfill an operational requirement.

NOTE: Remote access—Access to an IT resource through an off-network connection.

References: *NIST SP 800-53 AC-17*

Control SC 5.7.2

Manage third-party remote access.

Level: I II III

Requirements:

A. Manage third-party vendor remote access to systems. Remote access management includes:
   1. authorizing remote access to systems only to fulfill operational requirements
   2. restricting remote access to systems to temporary, preapproved access periods
   3. monitoring and logging remote access to systems
   4. reviewing and reauthorizing remote access to systems on a periodic basis
   5. revoking remote access to systems promptly when it is no longer necessary to fulfill an operational requirement.

NOTE: Remote access—Access to an IT resource through an off-network connection.

References: *NIST SP 800-53 AC-17*

Appendix A: Security Standards and Controls Summary

This section provides a synopsis of the security standards and controls required for compliance with the Secure UD DGSP. Detailed security control requirements are addressed in "Security Controls" (p. 30).

Security standards and controls are the mandates for policy compliance and IT resource security.

Each security standard addresses a particular risk to IT resources and contains one or more controls to mitigate that risk. Each security control prescribes administrative, operational, and/or technical requirements or recommendations for protecting IT resources. Each security control also, when applicable, references relevant parallel controls in NIST SP 800-53.[1]

Security controls are applied based on the three University information classifications: Level I—Low Risk information, Level II—Moderate Risk information, and Level III—High Risk information.[2] Each security control has an information classification indicator, shown in Figure 4 (p. 108), that denotes the classification(s) to which it applies. Some security controls may apply based on criticality instead of, or in addition to, classification.[3]

Each unit is responsible for meeting all security standards and implementing all security controls applicable to its administration, operation, and IT resources. Not all security controls are applicable to every unit; the unit is responsible for identifying which security controls are applicable as part of its information security plan.[4] Exceptions to security standards and controls must be approved by the unit head and documented.[5]

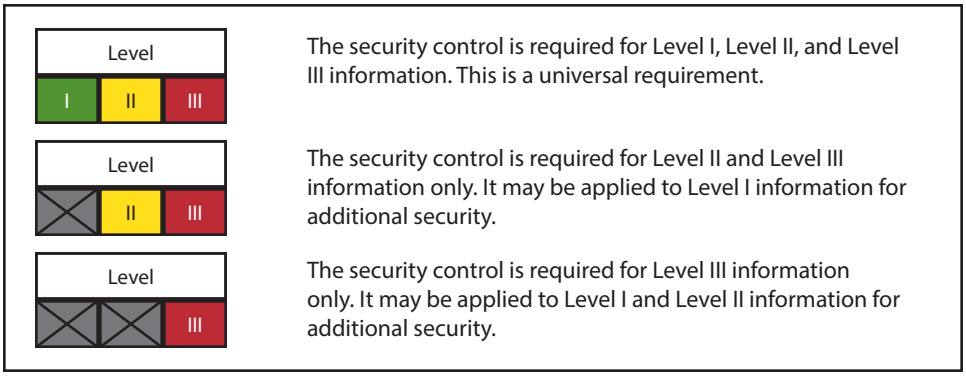

Figure 4: *Information classification indicators*

PDF

PDF tip: Text in the tables and footers of this section serve as clickable links. Click the text of a risk area, risk management objective, standard, or control to jump to that information in the Security Controls. Click the risk area initials in the footer to jump to that risk area in this section.

1 NIST references are addressed in "Federal Standard Mapping" (p. 22).
2 University information classifications are addressed in "University Information Classifications" (p. 12).
3 Criticality is addressed in "Information criticality" (p. 12).
4 Information security plan requirements are addressed in security control IS 2.1.1 (p. 33).
5 Procedures for handling exceptions to security standards and controls are addressed in "Compliance exceptions and reporting" (p. 23).

Information Security Program — IS—Risk Area 1

Objective IS 1	**Information Risk Assessment** *Objective: To identify, assess, and remediate risk.*	
Standard IS 1.1	**Risk assessments are conducted regularly.**	
Control IS 1.1.1	**Conduct information risk surveys.** *NIST SP 800-53 RA-1, RA-3; Secure UD Compliance and Risk Survey question #1*	Level: I II III
Control IS 1.1.2	**Conduct risk assessments.** *NIST SP 800-53 RA-1, RA-3; Secure UD Compliance and Risk Survey question #2*	Level: ~~I~~ ~~II~~ III
Standard IS 1.2	**A risk management strategy is developed, implemented, and maintained.**	
Control IS 1.2.1	**Develop, implement, and maintain a risk management strategy.** *NIST SP 800-53 PM-9; Secure UD Data Governance & Security Program; Secure UD Compliance and Risk Survey question #3*	Level: I II III
Standard IS 1.3	**Security assessments are conducted regularly.**	
Control IS 1.3.1	**Conduct IT security assessments.** *NIST SP 800-53 AU-1, CA-1, CA-2; University Information Security Policy; Secure UD Compliance and Risk Survey*	Level: I II III

Objective IS 2	**Information Security Planning** *Objective: To ensure that information risk is managed by consistent and appropriate plans.*		
Standard IS 2.1	**An information security plan is developed, implemented, and maintained.**		
	Control IS 2.1.1	**Develop, implement, and maintain an information security plan.** *NIST SP 800-53 PL-1, PM-1; Secure UD Data Governance & Security Program; Secure UD Security Plan Tool; Secure UD Compliance and Risk Survey question #4*	Level I II III
	Control IS 2.1.2	**Manage exceptions to security standards and controls.** *University Information Security Policy*	Level I II III
Standard IS 2.2	**Information security roles and responsibilities are defined and assigned.**		
	Control IS 2.2.1	**Assign information security roles.** *NIST SP 800-53 PM-2, PM-10; University Information Security Policy*	Level I II III
Standard IS 2.3	**Changes in law, regulation, and technology are assessed.**		
	Control IS 2.3.1	**Assess legal, regulatory, and technological changes.** *ISO 27001 A.15.1.1; University Information Security Policy; Secure UD Compliance and Risk Survey question #5*	Level I II III

IT Resource Acquisition — AQ—Risk Area 2

Objective AQ 1 — Vendor Service Acquisition

Objective: To manage risks regarding vendor service acquisition.

Standard AQ 1.1 — Risks are assessed in the IT vendor service acquisition process.

			Level
Control	AQ 1.1.1	**Assess vendor security risks.** *NIST SP 800-53 RA-3, SA-1, SA-4, SA-5*	I II III
Control	AQ 1.1.2	**Assess vendor security controls.** *NIST SP 800-53 RA-3, SA-1, SA-4, SA-5*	I II III

Standard AQ 1.2 — Vendor compliance with security standards is required.

			Level
Control	AQ 1.2.1	**Assess the need for a vendor contract.** *NIST SP 800-53 AC-20, SA-1, SA-4, SA-9; Secure UD Compliance and Risk Survey question #6*	I II III
Control	AQ 1.2.2	**Require vendor adherence to University policy.** *NIST SP 800-53 AC-20, SA-1, SA-4, SA-9*	I II III
Control	AQ 1.2.3	**Require a written vendor contract.** *NIST SP 800-53 AC-20, SA-1, SA-4, SA-9; Secure UD Compliance and Risk Survey question #6*	I II III
Control	AQ 1.2.4	**Review vendor contracts.** *NIST SP 800-53 AC-20, SA-1, SA-4, SA-9; Secure UD Compliance and Risk Survey question #6*	I II III

Objective AQ 2	**Vendor Management** *Objective: To ensure vendors are satisfying University security requirements.*		
Standard AQ 2.1	**Vendor compliance with security standards is verified.**		
	Control AQ 2.1.1	**Assess mission critical or Level III vendor security controls.** *NIST SP 800-53 SA-9; Secure UD Compliance and Risk Survey question #7*	Level: I II III
Standard AQ 2.2	**Third-party personnel attestation to security agreements is required.**		
	Control AQ 2.2.1	**Require Contractor Confidentiality Agreement attestation.** *NIST SP 800-53 AC-20, PS-7, SA-9; Contractor Confidentiality Agreement; Secure UD Compliance and Risk Survey question #8*	Level: I II III

Objective AQ 3	**Software License Management** *Objective: To comply with laws and regulations governing software use.*	
Standard AQ 3.1	**Compliance with software license agreements and law is ensured.**	
Control AQ 3.1.1	**Develop and maintain a software inventory.** *NIST SP 800-53 CM-10; Secure UD Compliance and Risk Survey question #9*	Level: I II III
Control AQ 3.1.2	**Manage software usage.** *NIST SP 800-53 CM-10; Secure UD Compliance and Risk Survey question #9*	Level: I II III

Application Security — AS—Risk Area 3

Objective AS 1	**Application Software Security** *Objective: To protect application operation, function, and data.*		
Standard AS 1.1	**Input data is validated.**		
	Control AS 1.1.1	**Implement input data validation.** *NIST SP 800-53 SI-10*	Level I II III
	Control AS 1.1.2	**Implement manual override capability.** *NIST SP 800-53 SI-10*	Level I II III
Standard AS 1.2	**Error message outputs are limited.**		
	Control AS 1.2.1	**Manage error handling.** *NIST SP 800-53 SI-11*	Level I II III
Standard AS 1.3	**Information system role assignments are able to be separated.**		
	Control AS 1.3.1	**Implement data role separation features.** *NIST SP 800-53 AC-5*	Level I II III
Standard AS 1.4	**Secure application boundaries are enforced.**		
	Control AS 1.4.1	**Configure application security features.** *NIST SP 800-53 SC-7*	Level I II III
Standard AS 1.5	**Application and security events are logged.**		
	Control AS 1.5.1	**Log application and security events.** *NIST SP 800-53 AU-2, AU-3; Secure UD Compliance and Risk Survey question #10*	Level I II III
	Control AS 1.5.2	**Log additional application and security events for Level III applications.** *NIST SP 800-53 AU-2, AU-3; Secure UD Compliance and Risk Survey question #10*	Level III

Standard AS 1.6	**Secure sessions are enforced.**	
Control AS 1.6.1	**Configure inactive authenticated session suspension.** *NIST SP 800-53 AC-11, IA-11*	Level: ~~I~~ II III
Control AS 1.6.2	**Implement secure web application session mechanisms.** *NIST SP 800-53 AC-11, SC-23*	Level: I II III
Standard AS 1.7	**The effects of denial of service attacks are limited.**	
Control AS 1.7.1	**Implement denial of service protection.** *NIST SP 800-53 SC-5*	Level: I II III
Control AS 1.7.2	**Conduct denial of service protection validations.** *NIST SP 800-53 SC-5*	Level: I II III
Standard AS 1.8	**Application data is protected during processing.**	
Control AS 1.8.1	**Implement application data processing protection.** *NIST SP 800-53 SC-4, SC-8*	Level: ~~I~~ ~~II~~ III
Standard AS 1.9	**Vendor-supported system components are implemented and maintained.**	
Control AS 1.9.1	**Implement and maintain vendor-supported system components.** *NIST SP 800-53 SA-22*	Level: I II III
Standard AS 1.10	**Security vulnerabilities are identified, assessed, and remediated.**	
Control AS 1.10.1	**Conduct web application vulnerability scans.** *NIST SP 800-53 RA-5*	Level: I II III

Objective AS 2	**Application Development Process** *Objective: To securely develop applications.*		
Standard AS 2.1	**A software development process is developed, implemented, and maintained.**		
	Control AS 2.1.1	**Develop, implement, and maintain a software development process.** *NIST SP 800-53 SA-3, SA-15; Secure UD Compliance and Risk Survey question #11*	Level I II III
	Control AS 2.1.2	**Classify application data.** *NIST SP 800-53 RA-2; University Information Classification Policy; Secure UD Compliance and Risk Survey question #11*	Level I II III
	Control AS 2.1.3	**Develop, implement, and maintain a system security plan.** *NIST SP 800-53 CA-2, SA-15; Secure UD Compliance and Risk Survey question #11*	Level I II III
	Control AS 2.1.4	**Conduct a peer code review.** *NIST SP 800-53 SA-11, SA-15*	Level I II III
	Control AS 2.1.5	**Implement application data environment protection.** *NIST SP 800-53 CA-2, SA-15*	Level III
Standard AS 2.2	**Application and configuration changes are managed.**		
	Control AS 2.2.1	**Develop, implement, and maintain a change management process.** *NIST SP 800-53 CM-3*	Level I II III
	Control AS 2.2.2	**Conduct change tests.** *NIST SP 800-53 CM-3*	Level I II III
Standard AS 2.3	**Application data access is managed.**		
	Control AS 2.3.1	**Manage application data access.** *NIST SP 800-53 CA-9*	Level I II III

Contingency Planning — CP—Risk Area 4

Objective CP 1	**Business Continuity Planning** *Objective: To mitigate disruptions of University business processes.*		
Standard CP 1.1	**A business continuity plan is developed, implemented, and maintained.**		
	Control CP 1.1.1	**Develop, implement, and maintain a business continuity plan.** *NIST SP 800-53 CP-2; Secure UD Compliance and Risk Survey question #12*	Level: I II III
	Control CP 1.1.2	**Conduct business continuity tests.** *NIST SP 800-53 CP-4; Secure UD Compliance and Risk Survey question #13*	Level: I II III

Objective CP 2	**Disaster Recovery** *Objective: To mitigate disruptions of IT resources.*		
Standard CP 2.1	**A disaster recovery plan is developed, implemented, and maintained.**		
	Control CP 2.1.1	**Develop, implement, and maintain a disaster recovery plan.** *NIST SP 800-53 CP-10*	Level I II III
	Control CP 2.1.2	**Conduct disaster recovery tests.** *NIST SP 800-53 CP-4*	Level I II III
Standard CP 2.2	**Backups of IT resources are required.**		
	Control CP 2.2.1	**Develop, implement, and maintain a backup plan.** *NIST SP 800-53 CP-9; Secure UD Compliance and Risk Survey question #14*	Level I II III
	Control CP 2.2.2	**Conduct backups.** *NIST SP 800-53 CP-9; Secure UD Compliance and Risk Survey question #14*	Level I II III
	Control CP 2.2.3	**Conduct backup verification tests.** *NIST SP 800-53 CP-9(1); Secure UD Compliance and Risk Survey question #15*	Level I II III
	Control CP 2.2.4	**Manage critical and mission critical backup storage.** *NIST SP 800-53 CP-9*	Level I II III

Data Management — DM—Risk Area 5

Objective DM 1	**Data Acquisition** *Objective: To collect data with appropriate breadth and depth.*		
Standard DM 1.1	**Data is acquired only if it fulfills an operational requirement.**		
	Control DM 1.1.1	**Manage data acquisition.** *NIST SP 800-53 DM-1; University Data Governance Policy; Secure UD Compliance and Risk Survey question #16*	Level: I II III
Standard DM 1.2	**Compliance with laws, regulations, and policies governing data acquisition is ensured.**		
	Control DM 1.2.1	**Assess laws, regulations, and policies governing data acquisition.** *NIST SP 800-53 AP-1; University Data Governance Policy; Secure UD Compliance and Risk Survey question #16*	Level: I II III

Objective DM 2	**Data Utilization** *Objective: To utilize data in support of University missions and business processes.*	
Standard DM 2.1	**Data is utilized only to fulfill an operational requirement.**	
Control DM 2.1.1	**Manage data utilization.** *NIST SP 800-53 UL-1; University Data Governance Policy; Secure UD Compliance and Risk Survey question #17*	Level: I II III
Standard DM 2.2	**Compliance with laws, regulations, and policies governing data utilization is ensured.**	
Control DM 2.2.1	**Assess laws, regulations, and policies governing data utilization.** *NIST SP 800-53 UL-1; University Data Governance Policy; University Web Privacy Policy; Secure UD Compliance and Risk Survey question #17*	Level: I II III

Objective DM 3	**Data Maintenance** *Objective: To maintain data in compliance with policies.*		
Standard DM 3.1	**University information is classified.**		
	Control DM 3.1.1	**Classify University information.** *NIST SP 800-53 RA-2; University Information Classification Policy*	Level I II III
Standard DM 3.2	**An inventory of IT resources is developed and maintained.**		
	Control DM 3.2.1	**Inventory business processes and data.** *NIST SP 800-53 PM-5, SE-1; University Information Security Policy; Secure UD Inventory Tool*	Level I II III
	Control DM 3.2.2	**Inventory IT resources.** *NIST SP 800-53 CM-8, PM-5, SE-1; University Information Security Policy; Secure UD Inventory Tool; Secure UD Compliance and Risk Survey question #18*	Level I II III
	Control DM 3.2.3	**Conduct scans to identify Level III information.** *NIST SP 800-53 PM-5; Secure UD Compliance and Risk Survey question #19, #20*	Level I II III
Standard DM 3.3	**Data is retained only for as long as it fulfills an operational requirement.**		
	Control DM 3.3.1	**Manage data retention.** *NIST SP 800-53 DM-1, DM-2; Secure UD Compliance and Risk Survey question #21*	Level I II III
Standard DM 3.4	**Compliance with laws, regulations, and policies governing records retention is ensured.**		
	Control DM 3.4.1	**Assess laws, regulations, and policies governing records retention.** *NIST SP 800-53 AU-11, SI-12; Secure UD Compliance and Risk Survey question #21*	Level I II III
	Control DM 3.4.2	**Manage data accessibility.** *OSTP Public Access Memo (22 Feb. 2013); Secure UD Compliance and Risk Survey question #22*	Level I II III

Objective DM 4	**Data Access** *Objective: To access data according to authorization and operational requirement.*		
Standard DM 4.1	**Information system access controls are implemented and maintained.**		
	Control DM 4.1.1	**Manage information system access controls.** *NIST SP 800-53 AC-3*	Level: I II III
Standard DM 4.2	**Data access is managed.**		
	Control DM 4.2.1	**Manage data access authorizations.** *NIST SP 800-53 AC-1, AC-6, AC-22, PS-4, UL-2; University Data Governance Policy; Secure UD End User Acknowledgement; Contractor Confidentiality Agreement; Secure UD Compliance and Risk Survey question #23, #24*	Level: I II III
Standard DM 4.3	**Manage data role assignments.**		
	Control DM 4.3.1	**Manage data role assignments.** *NIST SP 800-53 AC-1, AC-5*	Level: I II III

Objective DM 5	**Data Protection** *Objective: To protect data from unintentional, unlawful, or unauthorized disclosure, alteration, or destruction.*	
Standard DM 5.1	**IT resources at rest are encrypted.**	
Control DM 5.1.1	**Encrypt University information at rest.** *NIST SP 800-53 SC-28(1); Secure UD Compliance and Risk Survey question #25*	Level: ~~I~~ ~~II~~ III
Control DM 5.1.2	**Encrypt portable IT devices.** *NIST SP 800-53 SC-28(1); Secure UD Compliance and Risk Survey question #26*	Level: ~~I~~ II III
Standard DM 5.2	**Encryption is managed.**	
Control DM 5.2.1	**Manage cryptosystems.** *NIST SP 800-53 SC-13*	Level: I II III
Control DM 5.2.2	**Manage encryption keys.** *NIST SP 800-53 SC-12*	Level: I II III
Standard DM 5.3	**Disposal of IT resources is managed.**	
Control DM 5.3.1	**Manage digital information disposal.** *NIST SP 800-53 DM-2; Secure UD Compliance and Risk Survey question #27*	Level: ~~I~~ II III
Control DM 5.3.2	**Manage physical information disposal.** *NIST SP 800-53 MP-6*	Level: ~~I~~ II III
Control DM 5.3.3	**Manage IT device disposal.** *NIST SP 800-53 MP-6; Secure UD Compliance and Risk Survey question #27*	Level: I II III

Human Resources — HR—Risk Area 6

Objective HR 1	**Awareness and Training** *Objective: To educate users about security threats and best practices.*		
Standard HR 1.1	**Employee information security awareness training is provided.**		
	Control HR 1.1.1	**Provide employee information security awareness training.** *NIST SP 800-53 AT-1, AT-2, AT-2(2), AT-4; Secure UD Compliance and Risk Survey question #28*	Level: I II III
Standard HR 1.2	**Employee attestation to security agreements is required.**		
	Control HR 1.2.1	**Require annual employee Secure UD End User Acknowledgement attestation.** *NIST SP 800-53 AT-1, PS-6; University Data Governance Policy; Secure UD End User Acknowledgement; Secure UD Compliance and Risk Survey question #29*	Level: I II III

Objective HR 2	**Employment Management** *Objective: To ensure due diligence management of employees.*	
Standard HR 2.1	**Background checks are performed prior to employment.**	
Control HR 2.1.1	**Require background checks for positions with access to Level III information.** *NIST SP 800-53 PS-3; Secure UD Compliance and Risk Survey question #30*	Level: III
Standard HR 2.2	**IT resources are recovered.**	
Control HR 2.2.1	**Require IT resource recovery.** *NIST SP 800-53 PS-4, PS-5*	Level: I, II, III

Identification and Authentication — IA—Risk Area 7

Objective IA 1	**Identification and Authentication** *Objective: To securely manage digital identities and authentication processes.*	
Standard IA 1.1	**Authenticated access to IT resources is managed.**	
Control IA 1.1.1	**Require authenticated access to IT resources.** *NIST SP 800-53 AC-14, IA-2; Secure UD Compliance and Risk Survey question #31, #44*	Level I II III
Control IA 1.1.2	**Manage authentication to IT resources.** *NIST SP 800-53 IA-2; Secure UD Compliance and Risk Survey question #32*	Level I II III
Control IA 1.1.3	**Require multi-factor authentication to IT resources.** *NIST SP 800-53 IA-2*	Level ~~I~~ II III
Standard IA 1.2	**User accounts are managed.**	
Control IA 1.2.1	**Develop, implement, and maintain a user account management process.** *NIST SP 800-53 AC-1, AC-2, AC-6, IA-4, PS-4, PS-5; Secure UD Compliance and Risk Survey question #33*	Level I II III
Control IA 1.2.2	**Develop, implement, and maintain an administrator account management process.** *NIST SP 800-53 AC-2, AC-6; Secure UD Compliance and Risk Survey question #43*	Level I II III
Standard IA 1.3	**Authentication credentials are managed.**	
Control IA 1.3.1	**Manage passwords.** *NIST SP 800-53 IA-5*	Level I II III
Standard IA 1.4	**Secure sessions are enforced.**	
Control IA 1.4.1	**Restrict invalid login attempts.** *NIST SP 800-53 AC-7*	Level I II III
Control IA 1.4.2	**Configure inactive authenticated session suspension.** *NIST SP 800-53 AC-11, IA-11*	Level ~~I~~ II III

Incident Response — IR—Risk Area 8

Objective IR 1	**Incident Response** *Objective: To address incidents promptly and appropriately.*		
Standard IR 1.1	**An incident response plan is developed, implemented, and maintained.**		
	Control IR 1.1.1	**Develop, implement, and maintain an incident response plan.** *NIST SP 800-53 IR-1, IR-4, IR-5, IR-8; University Incident Response Policy; Secure UD Compliance and Risk Survey question #34*	Level: I II III
	Control IR 1.1.2	**Develop, implement, and maintain incident response capabilities.** *NIST SP 800-53 IR-1, IR-4, IR-5, IR-8; University Incident Response Policy*	Level: I II III
Standard IR 1.2	**Incidents are reported promptly.**		
	Control IR 1.2.1	**Require prompt incident reporting.** *NIST SP 800-53 IR-1, IR-6; University Incident Response Policy*	Level: I II III

Physical Security — PE—Risk Area 9

Objective PE 1	**IT Resource Physical Security** *Objective: To physically protect IT resources in University locations.*	
Standard PE 1.1	**Physical access controls for University locations are implemented and maintained.**	
Control PE 1.1.1	**Implement and maintain physical access controls.** *NIST SP 800-53 PE-1, PE-2, PE-3, PE-5, PE-6, PE-8; Secure UD Compliance and Risk Survey question #35*	Level: I II III
Control PE 1.1.2	**Manage physical access controls.** *NIST SP 800-53 PE-1, PE-2, PE-3, PE-5, PE-8*	Level: I II III
Standard PE 1.2	**IT resources are protected during transportation.**	
Control PE 1.2.1	**Manage transportation of physical media.** *NIST SP 800-53 MP-5, PE-2, PE-3, PE-5*	Level: ~~I~~ ~~II~~ III
Standard PE 1.3	**IT resources are protected during use and storage.**	
Control PE 1.3.1	**Manage use and storage of IT devices.** *NIST SP 800-53 MP-1, MP-4, PE-5; Secure UD Compliance and Risk Survey question #36*	Level: I II III
Control PE 1.3.2	**Manage use and storage of documents.** *NIST SP 800-53 MP-2; Secure UD Compliance and Risk Survey question #36*	Level: ~~I~~ II III

Objective PE 2	**Data Center Protection** *Objective: To physically protect University data centers.*		
Standard PE 2.1	**Physical access controls for data centers are implemented and maintained.**		
	Control PE 2.1.1	**Implement and maintain additional physical access controls.** *NIST SP 800-53 PE-1, PE-2, PE-3, PE-5, PE-6, PE-8; Secure UD Compliance and Risk Survey question #37*	Level I II III
Standard PE 2.2	**An alternate power source is implemented and maintained.**		
	Control PE 2.2.1	**Implement and maintain an alternate power source.** *NIST SP 800-53 PE-11; Secure UD Compliance and Risk Survey question #37*	Level I II III
Standard PE 2.3	**Fire detection and fire suppression systems are implemented and maintained.**		
	Control PE 2.3.1	**Implement and maintain fire detection systems.** *NIST SP 800-53 PE-13; Secure UD Compliance and Risk Survey question #37*	Level I II III
	Control PE 2.3.2	**Implement and maintain fire suppression systems.** *NIST SP 800-53 PE-13; Secure UD Compliance and Risk Survey question #37*	Level I II III
Standard PE 2.4	**Environmental controls are implemented and maintained.**		
	Control PE 2.4.1	**Implement and maintain temperature and humidity controls.** *NIST SP 800-53 PE-14; Secure UD Compliance and Risk Survey question #37*	Level I II III
	Control PE 2.4.2	**Implement and maintain water leakage protection controls.** *NIST SP 800-53 PE-15; Secure UD Compliance and Risk Survey question #37*	Level I II III
	Control PE 2.4.3	**Implement and maintain emergency lighting.** *NIST SP 800-53 PE-12; Secure UD Compliance and Risk Survey question #37*	Level I II III

System and Communication Management — SC—Risk Area 10

Objective SC 1 — Client Management

Objective: To protect client systems.

Standard SC 1.1 — Only the minimum necessary functionality is configured.

Control		Level I	Level II	Level III
SC 1.1.1	**Configure critical, mission critical, or Level III client systems with minimum functionality.** *NIST SP 800-53 CM-7*			III

Standard SC 1.2 — System configuration changes are managed.

Control		Level I	Level II	Level III
SC 1.2.1	**Develop, implement, and maintain a change management process.** *NIST SP 800-53 CM-3*			III

Standard SC 1.3 — Security vulnerabilities are identified, assessed, and remediated.

Control		Level I	Level II	Level III
SC 1.3.1	**Develop, implement, and maintain patch management procedures.** *NIST SP 800-53 RA-5, SI-2; Secure UD Compliance and Risk Survey question #38*			III
SC 1.3.2	**Conduct penetration tests.** *NIST SP 800-53 CA-8*			III

Standard SC 1.4 — Vendor-supported system components are implemented and maintained.

Control		Level I	Level II	Level III
SC 1.4.1	**Implement and maintain vendor-supported system components.** *NIST SP 800-53 SA-22*			III

Standard SC 1.5 — System and security events are logged and monitored.

Control		Level I	Level II	Level III
SC 1.5.1	**Log system and security events.** *NIST SP 800-53 AU-2, AU-3, AU-12*			III

Standard SC 1.6 — Secure system boundaries are enforced.

Control		Level I	Level II	Level III
SC 1.6.1	**Configure an ingress-filtering host-based firewall.** *NIST SP 800-53 SC-7; Secure UD Compliance and Risk Survey question #39*			III
SC 1.6.2	**Configure an egress-filtering host-based firewall.** *NIST SP 800-53 SC-7; Secure UD Compliance and Risk Survey question #39*			III

Standard SC 1.7	**Anti-virus software is implemented and maintained.**		
	Control SC 1.7.1	**Implement and maintain anti-virus software.** *NIST SP 800-53 SI-3; Secure UD Compliance and Risk Survey question #40*	Level I II III
	Control SC 1.7.2	**Implement and maintain advanced anti-virus software.** *NIST SP 800-53 SI-3; Secure UD Compliance and Risk Survey question #41*	Level III
Standard SC 1.8	**Clients are managed.**		
	Control SC 1.8.1	**Assign local support providers to client systems.** *NIST SP 800-53 CM-3; Secure UD Compliance and Risk Survey question #42*	Level I II III
Standard SC 1.9	**Maintenance is managed.**		
	Control SC 1.9.1	**Manage third-party maintenance.** *NIST SP 800-53 MA-2, MA-5*	Level I II III
Standard SC 1.10	**System clock synchronization is enforced.**		
	Control SC 1.10.1	**Configure system clocks.** *NIST SP 800-53 AU-8*	Level I II III

Objective SC 2	**Mobile Device Management** *Objective: To protect mobile devices.*		
Standard SC 2.1	**Only the minimum necessary functionality is configured.**		
	Control SC 2.1.1	**Configure mobile devices with minimum functionality.** *NIST SP 800-53 CM-7*	Level: II, III
Standard SC 2.2	**Remote security features are configured.**		
	Control SC 2.2.1	**Configure automatic secure erase.** *NIST SP 800-53 AC-7; Secure UD Compliance and Risk Survey question #44*	Level: III
	Control SC 2.2.2	**Configure remote lock, locate, and secure erase.** *NIST SP 800-53 AC-7; Secure UD Compliance and Risk Survey question #44*	Level: III
Standard SC 2.3	**Security vulnerabilities are identified, assessed, and remediated.**		
	Control SC 2.3.1	**Develop, implement, and maintain patch management procedures.** *NIST SP 800-53 SI-2*	Level: I, II, III
Standard SC 2.4	**Vendor-supported system components are implemented and maintained.**		
	Control SC 2.4.1	**Implement and maintain vendor-supported system components.** *NIST SP 800-53 SA-22*	Level: I, II, III
Standard SC 2.5	**Mobile devices are managed.**		
	Control SC 2.5.1	**Assign local support providers to mobile devices.** *NIST SP 800-53 CM-3*	Level: I, II, III
Standard SC 2.6	**Maintenance is managed.**		
	Control SC 2.6.1	**Manage third-party maintenance.** *NIST SP 800-53 MA-2, MA-5*	Level: I, II, III

Objective SC 3	**Server Management** *Objective: To protect server systems.*		
Standard SC 3.1	**Only the minimum necessary functionality is configured.**		
	Control SC 3.1.1	**Configure server systems with minimum functionality.** *NIST SP 800-53 CM-7; Secure UD Compliance and Risk Survey question #45*	Level I II III
Standard SC 3.2	**System configuration changes are managed.**		
	Control SC 3.2.1	**Develop, implement, and maintain a change management process for critical, mission critical, or Level III server systems.** *NIST SP 800-53 CM-3*	Level I II III
Standard SC 3.3	**Security vulnerabilities are identified, assessed, and remediated.**		
	Control SC 3.3.1	**Develop, implement, and maintain patch management procedures.** *NIST SP 800-53 RA-5, SI-2; Secure UD Compliance and Risk Survey question #46*	Level I II III
	Control SC 3.3.2	**Conduct vulnerability scans.** *NIST SP 800-53 RA-5; Secure UD Compliance and Risk Survey question #46*	Level I II III
	Control SC 3.3.3	**Conduct penetration tests.** *NIST SP 800-53 CA-8*	Level III
Standard SC 3.4	**Vendor-supported system components are implemented and maintained.**		
	Control SC 3.4.1	**Implement and maintain vendor-supported system components.** *NIST SP 800-53 SA-22*	Level I II III
Standard SC 3.5	**System and security events are logged and monitored.**		
	Control SC 3.5.1	**Log system and security events.** *NIST SP 800-53 AU-2, AU-3, AU-12; Secure UD Compliance and Risk Survey question #47*	Level I II III
	Control SC 3.5.2	**Maintain remote copies of critical, mission critical, or Level III system logs.** *NIST SP 800-53 AU-2, AU-3, A-4(1), AU-9; Secure UD Compliance and Risk Survey question #47*	Level I II III
	Control SC 3.5.3	**Review critical, mission critical, or Level III system logs.** *NIST SP 800-53 AU-6, AU-7; Secure UD Compliance and Risk Survey question #47*	Level I II III

Standard SC 3.6	**Secure system boundaries are enforced.**		
	Control SC 3.6.1	**Configure an ingress-filtering host-based firewall.** *NIST SP 800-53 SC-7; Secure UD Compliance and Risk Survey question #48*	Level I II III
	Control SC 3.6.2	**Configure an egress-filtering host-based firewall.** *NIST SP 800-53 SC-7; Secure UD Compliance and Risk Survey question #48*	Level III
	Control SC 3.6.3	**Conduct firewall rule reviews.** *NIST SP 800-53 SC-7*	Level III
Standard SC 3.7	**Unintentional, unlawful, or unauthorized system changes are identified, assessed, and remediated.**		
	Control SC 3.7.1	**Monitor critical or mission critical server system modification and integrity.** *NIST SP 800-53 SI-4, SI-7*	Level I II III
Standard SC 3.8	**Server systems are managed.**		
	Control SC 3.8.1	**Assign administrators to server systems.stems.** *NIST SP 800-53 CM-3; Secure UD Compliance and Risk Survey question #49*	Level I II III
Standard SC 3.9	**Maintenance is managed.**		
	Control SC 3.9.1	**Manage third-party maintenance.** *NIST SP 800-53 MA-2, MA-5, PE-16*	Level I II III
Standard SC 3.10	**System clock synchronization is enforced.**		
	Control SC 3.10.1	**Configure system clocks.** *NIST SP 800-53 AU-8*	Level I II III
Standard SC 3.11	**Server documentation is developed and maintained.**		
	Control SC 3.11.1	**Develop and maintain critical, mission critical, or Level III server documentation.** *NIST SP 800-53 CA-3, CM-8, PL-2, PM-5*	Level I II III

Standard SC 3.12	**Information flow is managed.**	
Control SC 3.12.1	**Develop, implement, and maintain information flow management policies.** *NIST SP 800-53 AC-4*	Level: III
Standard SC 3.13	**Database management services are configured.**	
Control SC 3.13.1	**Configure database management systems.** *NIST SP 800-53 AC-23*	Level: I II III
Control SC 3.13.2	**Configure advanced database management systems.** *NIST SP 800-53 AC-23*	Level: III
Standard SC 3.14	**Name and address resolution services are managed.**	
Control SC 3.14.1	**Manage secure name and address resolution.** *NIST SP 800-53 SC-20*	Level: I II III
Standard SC 3.15	**The effects of denial of service attacks are limited.**	
Control SC 3.15.1	**Implement and maintain denial of service protection.** *NIST SP 800-53 SC-5*	Level: I II III

Objective SC 4	**Network Management** *Objective: To protect networks and network devices.*		
Standard SC 4.1	**Only the minimum necessary functionality is configured.**		
	Control SC 4.1.1	**Disable unauthorized ports.** *NIST SP 800-53 CM-7*	Level I II III
	Control SC 4.1.2	**Assign public IP addresses only as necessary.** *NIST SP 800-53 AC-17*	Level I II III
Standard SC 4.2	**System configuration changes are managed.**		
	Control SC 4.2.1	**Develop, implement, and maintain a change management process.** *NIST SP 800-53 CM-3*	Level I II III
Standard SC 4.3	**Security vulnerabilities are identified, assessed, and remediated.**		
	Control SC 4.3.1	**Develop, implement, and maintain patch management procedures.** *NIST SP 800-53 RA-5, SI-2*	Level I II III
	Control SC 4.3.2	**Conduct vulnerability scans.** *NIST SP 800-53 RA-5*	Level I II III
	Control SC 4.3.3	**Conduct penetration tests.** *NIST SP 800-53 CA-8*	Level I II III
Standard SC 4.4	**Vendor-supported system components are implemented and maintained.**		
	Control SC 4.4.1	**Implement and maintain vendor-supported system components.** *NIST SP 800-53 SA-22*	Level I II III
Standard SC 4.5	**System and security events are logged and monitored.**		
	Control SC 4.5.1	**Log network and security events.** *NIST SP 800-53 AU-2, AU-3, AU-12*	Level I II III
	Control SC 4.5.2	**Maintain remote copies of logs.** *NIST SP 800-53 AU-2, AU-3*	Level I II III
	Control SC 4.5.3	**Review logs.** *NIST SP 800-53 AU-6, AU-7*	Level I II III

Standard SC 4.6	**Secure network boundaries are enforced.**		
	Control SC 4.6.1	**Configure a network firewall.** *NIST SP 800-53 SC-7*	Level I II III
	Control SC 4.6.2	**Conduct a firewall rule review.** *NIST SP 800-53 SC-7*	Level I II III
	Control SC 4.6.3	**Implement and maintain separate production and management networks.** *NIST SP 800-53 SC-7*	Level I II III
Standard SC 4.7	**Unintentional, unlawful, or unauthorized network access is identified, assessed, and remediated.**		
	Control SC 4.7.1	**Implement perimeter intrusion detection.** *NIST SP 800-53 SI-4*	Level I II III
Standard SC 4.8	**IT devices are uniquely identified prior to provisioning network access.**		
	Control SC 4.8.1	**Identify IT devices prior to provisioning network access.** *NIST SP 800-53 IA-3*	Level I II III
Standard SC 4.9	**Maintenance is managed.**		
	Control SC 4.9.1	**Manage third-party maintenance.** *NIST SP 800-53 MA-2, MA-5*	Level I II III
Standard SC 4.10	**System clock synchronization is enforced.**		
	Control SC 4.10.1	**Synchronize system clocks.** *NIST SP 800-53 AU-8*	Level I II III
Standard SC 4.11	**Network documentation is developed and maintained.**		
	Control SC 4.11.1	**Develop and maintain network documentation.** *NIST SP 800-53 CM-8, PM-5*	Level I II III
Standard SC 4.12	**Information flow is managed.**		
	Control SC 4.12.1	**Develop, implement, and maintain information flow management policies.** *NIST SP 800-53 AC-4*	Level I II III

Standard		Level
SC 4.13	**Secure wireless access is enforced.**	
Control SC 4.13.1	**Implement wireless network protection.** *NIST SP 800-53 AC-18*	II III
Control SC 4.13.2	**Manage wireless networks.** *NIST SP 800-53 AC-18*	III

Objective SC 5	**Transmission and Communication Management** *Objective: To protect communication systems.*	
Standard SC 5.1	**Spam filters are configured.**	
Control SC 5.1.1	**Configure spam filters.** *NIST SP 800-53 SI-8*	Level I II III
Standard SC 5.2	**Anti-virus software is implemented and maintained.**	
Control SC 5.2.1	**Implement and maintain anti-virus software.** *NIST SP 800-53 SI-3*	Level I II III
Standard SC 5.3	**Mail relays are managed.**	
Control SC 5.3.1	**Manage mail relays.** *NIST SP 800-53 CM-2, CM-6*	Level I II III
Standard SC 5.4	**University information in transmission is securely transmitted.**	
Control SC 5.4.1	**Securely transmit Level III information.** *NIST SP 800-53 SC-8; Secure UD Compliance and Risk Survey question #50*	Level ~~I~~ ~~II~~ III
Standard SC 5.5	**Voice over Internet Protocol services are managed.**	
Control SC 5.5.1	**Implement Voice over Internet Protocol protection.** *NIST SP 800-53 SC-19*	Level I II III
Standard SC 5.6	**Collaborative computing is managed.**	
Control SC 5.6.1	**Manage collaborative computing.** *NIST SP 800-53 SC-15*	Level I II III
Standard SC 5.7	**Secure remote access is enforced.**	
Control SC 5.7.1	**Manage remote access.** *NIST SP 800-53 AC-17*	Level ~~I~~ II III
Control SC 5.7.2	**Manage third-party remote access.** *NIST SP 800-53 AC-17*	Level I II III

Appendix B: University Data Governance Policy

The following policy has been reproduced below due to its foundational role in establishing the framework for data management and governance at the University.

This policy is currently a draft.

I. Scope of Policy

A. Data is an institutional asset and will be managed according to a University-wide data governance framework to facilitate the missions and activities of the University and minimize exposure to risk inherent in information management.

B. This policy creates, under the authority of the President, a data governance framework to support the consistent and appropriate management of University information.

C. This policy creates a framework for organizing the University into functional areas.

D. This policy sets forth a standard for management of University information and holds data trustees accountable for their functional area's compliance with data management requirements, including this policy.

E. This policy establishes the rules, roles, and responsibilities related to the management, including acquisition, utilization, maintenance, access, and protection, of University information.

F. This policy applies to all members of the University community and anyone with access to University information.

II. Definitions

See Appendix F: Glossary (p. 152).

III. Policy Statements

A. The University, as an organization, owns all University information. The management of University information is subject to the general oversight of the Board of Trustees.

B. The President of the University—and his or her delegates, including the Provost and the Executive Vice President & University Treasurer—exercises the highest degree of authority over the University's data governance model.

C. Individuals have particular roles and responsibilities for the appropriate management of University information. Roles are not exclusive. An individual fulfills any and all roles for which they meet the stated criteria.

D. This policy requires that University data governance practices, including management and security, comply with applicable laws and regulations. All individuals who have access to University information must manage it in a manner that is consistent with the University's need for privacy, analysis of strategic initiatives, security, and reporting standards compliance.

E. Functional areas must develop, implement, and maintain clear and consistent procedures for managing University information as appropriate.

IV. Policy Standards and Procedures

A. Data governance is a cooperative effort; the success of data governance efforts depends on collaboration between key University stakeholders,who provide critical expertise and perspectives related to specific aspects of data management and security.

1. Data trustees provide a strategic perspective on data governance. They direct institutional data initiatives and ensure that data is used in support of the University's missions and strategic goals.
2. Data stewards provide an operational perspective on data governance. They oversee efforts to ensure and improve the informational quality, effectiveness, usability, strategic value, and security of data. They also understand how their data is managed and used across the institution.
3. Data custodians provide a technical perspective on data governance. They manage information systems and shared data repositories on behalf of data trustees and data stewards. They also understand the underlying infrastructure that supports the management and security of data across the institution.

B. The President and/or his or her delegates will establish and oversee the Council for Data Governance (CDG).

1. The CDG facilitates the identification of the University's functional areas and their data trustees.
2. The CDG will include

a. The Chief Information Officer
b. The VP & General Counsel
c. Other University executives knowledgeable about the University's missions, strategy, administration, and operations.

C. This policy establishes an institutional data governance model
1. The University is organized into functional areas according to common strategic and operational objectives between units.
a. The functional areas are identified by the CDG.
b. Each functional area is assigned a data trustee by the CDG.
2. Each functional area has governance responsibilities for University information.
a. Ultimate accountability—including strategic oversight and authority—for a data set is entrusted to its data trustee.
(1) An individual is the data trustee for a particular data set if he or she is primarily accountable for the strategic value and use of that data across the institution.
(2) Each data trustee is responsible for overseeing University-wide data use in a manner consistent with the University's missions and goals.
b. Stewardship—including operational oversight and authority—for a data set is the responsibility of its data steward.
(1) An individual is the data steward for a particular data set if he or she is the primary authority for the management and security of that data across the institution.
(2) Each data steward is responsible for establishing University-wide standards and guidelines for the management, including acquisition, utilization, maintenance, access, and protection, of the University information within his or her stewardship.
(3) Data stewards are identified by data trustees based on their operational knowledge of a given data set and their understanding of its management and security needs.
3. Each functional area encompasses one or more units.
a. Each unit has an assigned unit head who is responsible for ensuring that his or her unit's management of University information complies with the policies, standards, and guidelines established by the appropriate data trustees and data stewards.
4. All University employees who use University information in any form or location are end users.
a. Every end user of University information is responsible for complying with policies, standards, and guidelines for the management and security of University information to which they have access.
5. Any University entity or employee with operational responsibility to manage a shared data repository is a data custodian.

D. Data trustees and their functional areas are identified in the Data Trustees and Functional Areas Table.

E. This policy creates two operational committees to assist with data governance.
1. Data Management Advisory Committee (DMAC)
a. The DMAC facilitates the coordination of data management efforts to assure the informational quality, effectiveness, usability, and strategic value of data across the University.
b. The DMAC includes:
(1) The Associate Provost for Institutional Research & Effectiveness (chair)
(2) Other members as appointed by data trustees and/or the chair
i. The chair may invite data trustees to appoint delegates to represent their functional areas in the DMAC. Delegates must be knowledgeable about their functional area's missions, strategy, administration, operations, and data management practices.
2. Data Security Advisory Committee (DSAC)
a. The DSAC facilitates the coordination of data security efforts across the University.
b. The DSAC includes:
(1) The director of IT Security (chair)
(2) Other members as appointed by data trustees and/or the chair

i. The chair may invite data trustees to appoint delegates to represent their functional areas in the DSAC. Delegates must be knowledgeable about their functional area's missions, strategy, administration, operations, and data management practices.

F. Data governance roles and responsibilities

1. The President
   a. Understand the need for a comprehensive data governance model.
   b. Authorize the creation of a University-wide data governance framework.
   c. Establish and appoint members to the CDG.
2. The Council for Data Governance (CDG)
   a. Monitor and manage this policy and the University's data governance framework.
   b. Identify the University's functional areas and their data trustees.
   c. Ensure that data trustees fulfill their data governance responsibilities according to policy.
      (1) Ensure that data trustees remain accountable for, engaged in, and committed to data quality, effectiveness, usability, strategy, and security.
   d. Resolve disputes of responsibility where data overlaps the functional areas of multiple data trustees.
   e. Oversee the formation and operation of the DMAC and DSAC.
3. Data trustees
   a. Appoint a data steward for each data set entrusted to their care.
   b. Oversee data stewardship efforts for University information entrusted to their care.
   c. Are ultimately accountable for their functional area's compliance with policies, laws, regulations, standards, and guidelines for the appropriate management of University information.
   d. Coordinate the use of University information entrusted to their care in a manner commensurate with the University's missions and strategic goals.
   e. Launch and support initiatives to improve the confidentiality, integrity, availability, and effectiveness of University information across the University and its units.
   f. Appoint delegates to participate in the DMAC and DSAC.
4. Data stewards
   a. Oversee the informational quality, effectiveness, usability, strategic value, and security of the University information within their stewardship.
   b. Establish definitions of the data sets within their stewardship.
   c. Develop and promulgate data management standards and guidelines to ensure the confidentiality, integrity, availability, and usefulness of University information within their stewardship.
   d. Ensure that University information within their stewardship is managed according to legitimate interests and operational requirements and in a manner that ensures the privacy and security of that University information.
   e. Develop and publish standards and guidelines for access to University information from their functional areas.
   f. Review and approve uses or proposed uses of University information within their stewardship.
   g. Authorize the creation of shared data repositories containing University information within their stewardship and assign custodianship responsibilities for those shared data repositories.
   h. Authorize the access of individual end users to University information within their stewardship.
   i. Audit at least annually the authorized access to University information within their stewardship.
5. The Data Management Advisory Committee (DMAC)
   a. Assist the CDG and data stewards in the implementation of the data management aspects of this policy.
   b. Assist data stewards in coordinating initiatives to improve the informational quality, effectiveness, usability, and strategic value of University information across the University and its units.
   c. Aid in the development of standards and guidelines concerning the management of data by the University and its units.
   d. Report to the CDG relevant data management initiatives and recommendations as appropriate.

6. The Data Security Advisory Committee (DSAC)
    a. Assist the CDG and data stewards in the implementation of the risk management aspects of this policy.
    b. Assist data stewards in coordinating initiatives to improve the confidentiality, integrity, and availability of University information across the University and its units.
    c. Aid in the development of standards and guidelines concerning the management of information security and risk by the University and its units.
    d. Report to the CDG relevant security initiatives and recommendations as appropriate.
7. Data custodians
    a. Are assigned management responsibility for the shared data repositories they maintain.
    b. In compliance with data stewards' standards and guidelines, grant and manage end user access to the shared data repositories for which they are responsible.
8. Unit heads
    a. Assume primary policy compliance responsibility for their units.
    b. Thoroughly understand the policies, laws, and regulations impacting University information used within their units.
    c. Implement procedures to comply with data trustees' and data stewards' policies, standards, and guidelines for the University information to which their units have access.
    d. Report to data trustees the unit's compliance with data management requirements at least annually.
    e. Request end user access to University information only in compliance with data stewards' standards and guidelines and only for end users who have a legitimate interest in access.
    f. Ensure that end users are aware of and understand their responsibilities for University information.
9. End users
    a. Understand and adhere to policies, standards, and guidelines for data management.
    b. Recognize the consequences of improper management of University information.
    c. Acknowledge annually through the Secure UD End User Acknowledgement their responsibility to appropriately manage the IT resources in their care.

G. This policy requires adherence to ethical, legal, and professional standards for data management including, but not limited to:
1. Manage University information in accordance with institutional need only.
2. Access and use University information only for legitimate University activities and only according to your authorization to use that information (i.e., no "administrative voyeurism").
3. Disclose University information only in compliance with federal, state, and local laws, University policies, and data stewardship and management rules.
4. Do not facilitate the violation of administrative policies or the circumvention of technical or physical safeguards by others.

Appendix C: University Information Security Policy

The following policy has been reproduced below due to its foundational role in establishing the mandate for information security at the University and creating the Secure UD DGSP.

This policy is currently a draft.

I. Scope of Policy

A. This policy expands upon the data governance framework established by the University Data Governance Policy to address requirements, roles, and responsibilities related to the security of IT resources.

B. Privacy and security practices protect University information and allow the use, access and disclosure of such information in accordance with University missions and applicable laws, regulations, contracts, and/or funding agency requirements.

C. This policy establishes responsibility to manage IT resources in accordance with the security standards and controls set forth in this policy. The confidentiality, integrity and availability of University information must be maintained and protected to support the University's missions and to comply with laws, regulations, and contractual obligations.

D. This policy establishes a University-wide information security framework to:

1. Protect against unintentional, unlawful, or unauthorized disclosure, alteration, or destruction of sensitive information that could potentially result in harm to the University, members of the University community, other organizations, or the nation.
2. Protect against anticipated threats to the security of IT resources.
3. Comply with federal, state and local law, University policies, and agreements that bind the University to implement applicable security controls.

E. This policy applies to all individuals who have access to IT resources used for University purposes and encompasses the safekeeping of University information in any form—including, but not limited to, spoken, printed, audio, video and digital/electronic media—and in all locations—including, but not limited to, in storage media, in e-communications, in the cloud, and on personal devices. Note: for the purposes of this policy, "University purposes" do not include students or employees accessing or updating their individual University information.

II. Definitions

See Appendix F: Glossary (p. 152).

III. Policy Statements

A. All IT resources must be managed in compliance with applicable federal, state, and local laws; University policies; and agreements.

B. University of Delaware Information Technologies (IT) is authorized to develop, promulgate and enforce information security program requirements for the University. These requirements may include policies, procedures, security standards and controls, roles, and responsibilities for the protection of IT resources.

C. All end users must comply with the requirements mandated by this policy, including administrative, operational, and technical security controls.

IV. Policy Standards and Procedures

A. All end users are responsible for protecting IT resources by complying with appropriate administrative, operational, and technical security standards and controls commensurate with the requirements for its classification. The University Information Classification Policy establishes the University information classifications.

B. The Secure UD Data Governance & Security Program (Secure UD DGSP) establishes administrative, operational, and technical mandates for the security and management of IT resources.

C. Exceptions to this policy, including exceptions to the requirements of the Secure UD DGSP, must be justified by operational or technical needs and must be submitted to and approved by unit heads.

D. Roles and responsibilities

1. Data trustees
   a. Define risk tolerance related to security threats to University information entrusted to their care.

b. Are ultimately accountable for the implementation of reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of IT resources within their functional areas.
c. Require annual assessments of security controls within their functional areas and report the results to IT.

2. Data stewards
   a. Require the implementation of reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of IT resources within their stewardship.
3. Information Technologies
   a. Maintain overview responsibility for implementation of this policy.
   b. Establish policy requirements, including security standards and controls, and monitor and enforce compliance.
      (1) Develop a comprehensive security program that includes risk assessments, best practices, education, and training.
      (2) Having IT assume this responsibility does not abrogate the responsibility of individuals and units to comply with policy requirements.
   c. Train and educate the University community on this policy.
   d. Monitor technological developments, trends, and changes in laws and regulations and update this policy as appropriate.
   e. Conduct annual reviews of minimum technical requirements and update this policy, with appropriate review.
   f. Assist units in understanding risk and in identifying and implementing security controls to protect IT resources.
   g. Issue critical security notices to units.
   h. Develop, implement, and maintain University-level security monitoring and analysis.
4. The Data Security Advisory Committee (DSAC)
   a. Assist in the implementation of this policy.
   b. In consultation with the VP & General Counsel, monitor federal, state, and local laws and regulations affecting information security and privacy.
   c. Stay abreast of evolving best practices in information security and privacy in higher education.
   d. Assess risks to University information and recommend updates to this policy, including the Secure UD DGSP, as necessary.
5. Unit heads
   a. Assume primary compliance responsibility for the IT resources under their control.
   b. Identify local support providers and report those individuals or units to IT.
   c. Develop and implement an information security plan for the unit consistent with the requirements of this policy and commensurate with the specific security needs of the unit.
   d. Thoroughly understand the security risks impacting University information under their control. Security risks should be documented and reviewed with the appropriate data steward so that he or she can determine whether greater resources need to be devoted to mitigating these risks. IT can assist unit heads with gaining a better understanding of their security risks.
   e. Ensure the implementation of reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of IT resources within their units.
   f. Approve exceptions to this policy based on operational or technical needs.
   g. Report to data trustees the unit's compliance with information security requirements at least annually.
6. Local support providers
   a. Maintain knowledge of the IT devices for which they are responsible.
   b. Implement, at the direction of the unit head, security controls for the IT devices for which they are responsible.
   c. Understand and document the configurations and characteristics of the IT devices for which they are responsible.
   d. Recommend security controls and practices for the IT devices for which they are responsible.
7. End users
   a. Adhere to unit procedures for implementing security controls.

Appendix D: University Information Classification Policy

The following policy has been reproduced below due to its foundational role in establishing the information classifications for University information.

This policy is currently a draft.

I. Scope of Policy

A. This policy establishes risk-based information classifications to facilitate institution-wide understanding of data-related risks and implementation of security standards and controls as required by the University Information Security Policy.

B. This policy applies to University information in all forms, including physical and digital, and in all locations, including in storage media, in e-communications, in the cloud, and on personal devices. Note: for the purposes of this policy, "University information" does not include an individual's own personal information stored on a computer or device.

II. Definitions

See Appendix F: Glossary (p. 152).

III. Policy Statements

A. University information must be classified according to the University information classifications defined in this policy.

B. University information in all forms and locations must be protected by implementing the administrative, operational, and technical security standards and controls required by its classification.

IV. Policy Standards and Procedures

A. This policy establishes three University information classifications based on confidentiality risks:

1. Level III—High Risk Information
   a. The University is required to implement specific security controls to safeguard the privacy and confidentiality of Level III information as mandated by federal, state and/or local law; University policy; or agreement.
   b. Unintentional, unlawful or unauthorized disclosure of Level III information would have a significant adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation.
   c. Level III information includes, but is not limited to:
      (1) Confidential information.
      (2) Personally Identifiable Information (PII) - An individual's first name or initial and last name in combination with any of the following:
         i. Social Security number,
         ii. Driver's license number or state-issued ID card number,
         iii. Alien registration or government passport number,
         iv. Account number, or credit or debit card number, in combination with any required security code, access code, PIN or password needed to access an account.
      (3) Protected Health Information (PHI/ePHI) as defined in the Health Insurance Portability and Accountability Act (HIPAA).
      (4) Cardholder Data (CHD) as defined by the Payment Card Industry Data Security Standards (PCI-DSS).
      (5) Export controlled data, including research, subject to the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR).
      (6) Sensitive personally identifiable human subject research.
      (7) UDelNet account passwords or encryption keys used to protect access to Level III information.

d. Data stewards and unit heads may require specific University information not classified as Level III information under this policy to be nonetheless managed according to the same security standards and controls as Level III information. For example, data stewards may require that a data set vital to the operational continuity or effectiveness of the University be protected by the additional security standards prescribed for Level III information, even if that data set does not necessarily carry significant confidentiality risks.

2. Level II—Moderate Risk Information
   a. Level II information includes all University information not categorized as either Level III or Level I.
   b. Level II information refers to official internal records that support the day-to-day operation of University units. This data may sometimes be described as "official use only."
   c. Level II information includes, but is not limited to:
      (1) Student education records, not including directory information, subject to the Family Education Rights Protection Act (FERPA).
      (2) Human resources information, such as salary and employee benefits information.
      (3) Non-public personal and financial data about applicants and donors.
      (4) Information received under grants and contracts subject to confidentiality requirements.
      (5) Law enforcement or court records and confidential investigation records.
      (6) Citizenship or immigration status.
      (7) Unpublished University financial information, strategic plans, and real estate or facility development plans.
      (8) Information on facilities security systems.
      (9) Nonpublic intellectual property, including unpublished research data, invention disclosures, and patent applications.
3. Level I—Low Risk Information
   a. Level I information is explicitly or implicitly approved for distribution to all members of the University community and to all individuals and entities external to the University community with no legal, regulatory, contractual, or funding agency restrictions on access or usage.
   b. Unintentional, unlawful, or unauthorized disclosure of Level I information would have limited or no adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation.
   c. Level I information includes, but is not limited to:
      (1) General access data on University websites.
      (2) University financial statements and other reports filed with federal or state governments and generally available to the public.
      (3) Copyrighted materials that are publicly available.
      (4) Directory information under FERPA.

B. Roles and responsibilities
1. Data trustees
   a. Require the appropriate classification of University information entrusted to their care.
2. Data stewards
   a. Classify University information within their stewardship according to the three University information classifications:
      (1) Level III—High Risk Information
      (2) Level II—Moderate Risk Information
      (3) Level I—Low Risk Information
   b. Periodically review and update the classifications of University information within their stewardship.
   c. Report to Information Technologies the classifications of University information within their stewardship..
3. Information Technologies
   a. In collaboration with data stewards, develop and maintain a University data dictionary that describes the sets of University information available for access and the University information classifications assigned to them.

Appendix E: Data Trustees and Functional Areas

The following list is an example of data trustees and functional areas and is intended to supplement the University Data Governance Policy. It is presented for discussion purposes only.

Data Trustee	Functional area and data areas
Associate Provost and Chief of Staff Margaret Bottorff	**Provost Chief of Staff** Provost budget data Provost staff data
Chief Budget Officer Amanda Minner	**Budget** Budget data
Chief Human Resources Officer Darcell Griffith	**Human Resources** Employee biographic/demographic data Employee personnel data Benefits data Compensation data
Chief Investments Officer Keith Walter	**Investments** Investments data
Chief of Police Patrick Ogden	**Police** Law enforcement data
Dean, Alfred Lerner College of Business and Economics Bruce Weber	**Alfred Lerner College of Business and Economics** Alfred Learner College of Business and Economics data
Dean, College of Agriculture and Natural Resources Mark Rieger	**College of Agriculture and Natural Resources** College of Agriculture and Natural Resources data
Dean, College of Arts and Sciences George Watson	**College of Arts and Sciences** College of Arts and Sciences data
Dean, College of Earth, Ocean, and Environment Estella Atekwana	**College of Earth, Ocean, and Environment** College of Earth, Ocean, and Environment data
Dean, College of Education and Human Development Carol Vukelich	**College of Education and Human Development** College of Education and Human Development data
Dean, College of Engineering Babatunde Ogunnaike	**College of Engineering** College of Engineering data
Dean, College of Health Sciences Kathleen Matt	**College of Health Sciences** College of Health Sciences data Protected Health Information (HIPAA)
Deputy Provost for Academic Affairs Lynn Okagaki	**Academic Affairs** Student immigration and visa data Advising data Curriculum data

Data Trustee	Functional area and data areas
Director of Office of Equity & Inclusion and University Title IX Coordinator Susan Groff	**Office of Equity & Inclusion** Equity & inclusion data Title IX investigation data
Director of Intercollegiate Athletics and Recreation Services Christine Rawak	**Athletics** NCAA student athlete data
Director of Internal Audit Kirk Die	**Internal Audit** Audit data
Executive Director for Campus and Public Safety Albert Homiak	**Public Safety** Occupational safety and environmental health data Security camera data Public safety and security data Emergency planning data
Vice President and General Counsel Laure Ergin	**General Counsel** Case files Contracts Miscellaneous legal advice and communications
Vice President and University Secretary Jeffrey Garland	**Board of Trustees** Board of Trustees data Archives data
Vice President for Communications and Marketing Glenn Carter	**Communications and Marketing** Communications and marketing data
Vice President for Development and Alumni Relations James Dicker	**Development** Alumni/donor data Gift data Prospect data Gift planning data Alumni association data
Vice President for Enrollment Management Christopher Lucier	**Enrollment** Undergraduate biographic/demographic data Student academic records Student accounting data Financial aid data UD #1 Flex data

Data Trustee	Functional area and data areas
Vice President for Facilities, Real Estate and Auxiliary Services and University Architect Peter Krawchyk	**Facilities** Facilities/management space data Service unit billing Auxiliary operations data Plant operations data Parking operations data Architecture, engineering, and construction data
Vice President for Finance and Deputy Treasurer Gregory Oler	**Finance** General ledger data Capital assets data Purchasing data Equipment inventory data Miscellaneous accounts receivable data Wages, salaries, and withholdings data Treasury services data (banking and tax data) Debt issuance data Insurance claims
Vice President for Information Technologies and Chief Information Officer Sharon Pitt	**Information Technologies** IT data E-communications UD Directory data Learning management system usage data
Vice President for Research, Scholarship and Innovation Charles Riordan	**Research Administration** Sponsored projects (pre-award) Sponsored projects (post-award) Human subjects research Animal research Conflict of interest data Faculty research interests
Vice President for Strategic Planning and Analysis Mary Remmler	**Strategic Planning and Analysis** Strategic planning and analysis data Institutional research data

Data Trustee	Functional area and data areas
Vice President for Student Life José-Luis Riera	**Student Life** New Student Orientation data Housing data Student health and wellness data Student conduct data Career counseling data Mental health counseling data Activities data Academic counseling data Protected Health Information (HIPAA)
Vice Provost for Diversity Carol Henderson	**Diversity** Diversity data
Vice Provost for Faculty Affairs Matthew Kinservik	**Faculty Affairs** Faculty affairs data
Vice Provost for Graduate and Professional Education Ann Ardis	**Graduate and Professional Education** Graduate biographic/demographic data Professional studies biographic/demographic data
Vice Provost for Libraries and Museums and May Morris University Librarian Trevor Dawes	**Library** Library data Museum data

Appendix F: Glossary

Administrative controls—Security controls that focus on the management of risk and IT resources. (*FIPS Publication 200*)

Availability—The timeliness and reliability of access to and use of University information. (*University Information Security Policy*)

Checklist test—A test in which a plan or procedure is reviewed to ensure accuracy and consistency.

Client system—Any IT device that is a desktop computer or laptop computer.

Confidentiality—The preservation of authorized restrictions on University information access and disclosure, including means for protecting personal privacy and proprietary information. (*University Information Security Policy*)

Council for Data Governance (CDG)—The University council responsible for overseeing the appointment and action of data trustees for each of the University's functional areas. It includes the Chief Information Officer, VP & General Counsel, and other members as appointed by the President and/or his or her delegates. (*University Data Governance Policy*)

Critical—Important to the business continuity or operational effectiveness of the unit. Loss of integrity or availability of critical IT resources would have moderate short-term impact on business continuity or operational effectiveness.

Criticality—The combined integrity and availability concerns of University information. Criticality is a reflection of how important data is to business continuity or operational effectiveness.

Data center—A group of networked server systems used for critical business processes involving data processing, storage, and transmission.

Data custodian—A University entity or employee with operational responsibility to manage a shared data repository on behalf of a data steward. (*University Data Governance Policy*)

Data governance—The responsible oversight of the informational quality, effectiveness, usability, strategic value, and security of data throughout its lifecycle. (*University Data Governance Policy*)

Data management—The responsible stewardship of data throughout its lifecycle, including acquisition, utilization, maintenance, access, and protection. (*University Data Governance Policy*)

Data Security Advisory Committee (DSAC)—The University council responsible for coordinating information security and risk management efforts and monitoring and recommending necessary security actions to the University. It is chaired by the director of IT Security and includes delegates as may be appointed from time to time by data trustees and/or the chair. (*University Data Governance Policy*)

Data set—A collection of related University information that supports University missions or activities. (*University Data Governance Policy*)

Data steward—An individual within the University who is the primary institutional authority for a particular data set and who is principally responsible for the management and security of that data set across the institution. (*University Data Governance Policy*)

Data stewardship—The responsible oversight of a data set, including principal responsibility for the establishment of standards and guidelines for appropriately managing and securing that data across the institution. (*University Data Governance Policy*)

Data trustee—An executive officer of the University who has the highest level of strategic planning and policy-setting authority and responsibility for his or her functional area. (*University Data Governance Policy*)

Disruptive event—An event that requires the execution of a plan or procedure to recover from operational loss.

E-communications—The network traffic or files containing users' electronic communications, including telephone conversations, electronic mail or transmission, webpage, or content exchanged with other IP addresses. (*University Acceptable Use of IT Resources Policy*)

Electronic storage media—Any standalone or integrated electronic media that can be used to store data. Includes optical media, magnetic media, disk drives, and flash drives.

End user—Any individual who accesses and/or utilizes IT resources. (*University Data Governance Policy*)

Functional area—One or more units that have primary responsibility for managing a core University mission or business function. (*University Data Governance Policy*)

Integrity—The protection against improper modification or destruction of University information; includes non-repudiation and authenticity. (*University Information Security Policy*)

IT device—Any device involved in the accessing, processing, storage, or transmission of University information and making use of the University IT infrastructure or attached to the University network. These devices include, but are not limited to, desktop computers, laptop computers, personal digital assistants, server systems, network devices such as routers or switches, and printers. (*University Information Security Policy*)

IT resources—The full set of University-owned or -controlled IT devices and data involved in the accessing, processing, storage, and transmission of information. (*University Information Security Policy*)

Incident—Any event that has or is reasonably likely to result in the compromise of the confidentiality, integrity, or availability of an IT resource, including, but not limited to, breaches or loss or theft of devices. (*University Incident Response Policy*)

Legitimate interest—A requirement to access University information commensurate with a end user's conduct of official University activities. (*University Data Governance Policy*)

Level I information—Also called Low Impact information; University information for which unintentional, unlawful, or unauthorized disclosure would have limited or no adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation. (*University Information Classification Policy*)

Level II information—Also called Moderate Impact information; University information for which unintentional, unlawful, or unauthorized disclosure would have a moderate adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation. (*University Information Classification Policy*)

Level III information—Also called High Impact information; University information for which unintentional, unlawful, or unauthorized disclosure would have a significant adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation. (*University Information Classification Policy*)

Local support provider—An individual or unit with primary responsibility for the installation, configuration, security, and ongoing maintenance of an IT device. (*University Information Security Policy*)

Mission critical—Vital to the business continuity or operational effectiveness of the unit. Loss of integrity or availability of mission critical IT resources would have significant short-term impact on business continuity or operational effectiveness.

Mobile device—Any IT device that is a mobile phone or tablet.

Non-critical—Necessary to the business continuity or operational effectiveness of the unit. Loss of integrity or availability of non-critical IT resources would have limited or no short-term impact on business continuity or operational effectiveness.

Operational controls—Security controls that are implemented primarily by people rather than by IT devices. (*FIPS Publication 200*)

Portable device—Any IT device that is a laptop computer, mobile device, or removable electronic storage media.

Privacy statement—A posted notice of website practices for obtaining and using data from visitors to that website. (*University Web Privacy Policy*)

Quality—Accuracy, completeness, and timeliness; reflects the fitness of data for its intended University purposes. (*University Data Governance Policy*)

Recovery point objective—The targeted maximum time period for which data might be lost as a result of a disruptive event before incurring unacceptable consequences associated with a break in business continuity. Simplified: the acceptable extent of data loss due to a disruptive event.

Recovery time objective—The targeted duration of time and degree of business function resumption required following a disruptive event to avoid unacceptable consequences associated with a break in business continuity. Simplified: the acceptable duration of downtime following a disruptive event.

Remote access—Access to an IT resource through an off-network connection.

Risk area—One of 10 broad groups of IT security risks posed to the University.

Risk management objective—One of 25 specific goals for managing and mitigating risk to the University.

Security controls—Administrative, operational, and technical requirements and recommendations for meeting security standards. (*University Information Security Policy*)

Security standards—Requirements for achieving risk management objectives and compliance with laws, regulations, and policies. (*University Information Security Policy*)

Server system—Any IT device that provides application, system, or network services to other information systems.

Shared data repository—A collection of University information to which multiple individuals or entities have access. (*University Data Governance Policy*)

Simulation—A test in which a plan or procedure is executed during a mock disruptive event to ensure its function.

Structured walkthrough—A test in which a plan or procedure is reviewed step by step with the individuals responsible for its execution to ensure accuracy and consistency.

Technical controls—Security controls that are implemented primarily by IT devices according to their hardware, software, and firmware. (*FIPS Publication 200*)

Technology service provider—A University unit or third-party vendor that provides online services for the University. (*University Web Privacy Policy*)

Unit—A University department, school, institute, program, office, initiative, center, or other operating unit. (*University Data Governance Policy*)

Unit head—A University official with the highest level of authority over the day-to-day management or oversight of a unit's operation. (*University Data Governance Policy*)

University activities—Actions, processes, and procedures that support University missions, administration, or operation. For the purposes of policy, University activities do not include an individual's personal scholarship, pedagogy, or academic research.

University-approved—Either: required or permitted by a University contract; or approved by a unit head in the interests of facilitating the unit's administrative, operational, or technical ability to fulfill its missions.

University information—Any information within the University's purview, including information that the University may not own but that is governed by laws and regulations to which the University is held accountable. Encompasses all data that pertains to or supports the administration and missions, including research, of the University. (*University Data Governance Policy*)

University information classifications—The categories of University information that have different security requirements based on their potential impact due to a loss of confidentiality, integrity, or availability. (*University Information Classification Policy*)

Vendor—A cloud service provider; any third party that provides IT services that would otherwise be performed by IT.

Visitor—Any user of a University website. (*University Web Privacy Policy*)

This page intentionally left blank.