Office of Information Technology

Information Security and Assurance Management Program

Fordham University

Information Security and Assurance
3-20-2024

Contents

Revision History

Revision Number	Summary of Revision	Revision Author	Date	Accepted By
1.0	Initial plan	Silvio Balzano	12/21/2016	Jason Benedict
1.1	Revisions were made to the plan based on recommendations made by Gartner. These changes are primarily format-based, including moving the IT organizational chart to the appendix. Some grammatical fixes were made as well.	Silvio Balzano/ Josephine Law	05/01/2017	Jason Benedict
1.1.0	Updated policies section; org charts	Josephine Law	01/14/2020	
1.1.1	Revised Awareness Training (AT) section	Lynne Chernow	01/17/2020	
1.1.2	Added 2020 Status to tables	Josephine Law	01/21/2020	
1.1.3	Updated AT table entries	Lynne Chernow	01/22/2020	
1.2	Updated FY18 Status	Josephine Law	02/11/2020	
1.3	Updated FY2020	Josephine Law	02/21/2020	
1.4	Updated narrative	Josephine Law	03/30/2020	
2.0	FY20 updated	Josephine Law	04/16/2020	Jason Benedict
2.1	Added additional information to the FY20 updates	Josephine Law	06/30/2020	
3.0	Updated to reflect the transition from NIST 800-53 rev 4 to Cybersecurity Framework (CSF)	Josephine Law	10/1/2021	
3.1	Update job descriptions, org charts, and name of the group from University Information Security Office to Information Security and Assurance	Josephine Law	02/09/2022	
3.2	Updated the Information Security and Assurance section	Josephine Law	04/28/2022	
3.2.1	Replaced Fordham IT with Information Technology	Josephine Law	01/28/2023	
3.3	Update job descriptions, org charts, removed references to NIST 800-53, updated definitions, updated IT priorities	Josephine Law	03/20/2024	Shannon Ortiz

Review Frequency

Review Frequency:	Annual
Responsible Person:	Senior Director of IT Security and Assurance
Approved By:	AVP/CISO
Approval Date:	May 1, 2017

Overview

The Fordham University Information Security and Assurance program defines the information security standards and procedures for ensuring the confidentiality, integrity, privacy, security, and availability of all information systems and resources managed by Fordham University and the implementation status as of March 20, 2024. Included are:

- Standards and procedures aligned to NIST
- Roles and responsibilities
- List of policies
- Applicable laws and regulations
- Glossary of terms and acronyms
- Office of Information Technology organizational charts

The Fordham University Information Security and Assurance program supplements the official Security Policies, Standards, Procedures, and Guidelines that Fordham's Office of Information Technology established. The security program aligns with the NIST Cybersecurity Framework. It complies with the regulations and policies set forth by the State of New York, Fordham University, the Federal Information Security Management Act (FISMA), the Family Educational Rights and Privacy Act (FERPA), the General Data Protection Regulation (GDPR), and other regulations.

Scope

The standards and procedures indicated in the Fordham Information Security and Assurance Management Program apply to all IT Resources connecting to the Fordham University network.

Alignment to NIST

Fordham's Information Security and Assurance Office aligns with the NIST Cybersecurity Framework (CSF) 1.1. The NIST CSF is voluntary guidance to help organizations manage and reduce cybersecurity risk. It is organized into five Functions (Identify, Protect, Detect, Respond, and Recover), defined by twenty-three Categories and 108 Subcategories.

CSF is a risk-based approach to managing cybersecurity risk and comprises three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities.

- The Framework Core is a set of cybersecurity activities, desired outcomes, and relevant references common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices to communicate cybersecurity activities and outcomes across the organization from the executive to the implementation/operations levels. The Framework Core consists of five concurrent and continuous Functions (Identify, Protect, Detect, Respond, and Recover). When considered together, these Functions provide a high-level, strategic view of an organization's cybersecurity risk management lifecycle.
- The Framework Profile represents the outcomes based on an organization's business needs selected from the Framework Categories and Subcategories. The Profile aligns standards, guidelines, and practices to the Framework Core in a particular implementation scenario.
- Profiles are used to
    - Identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state),
    - Develop a Profile, ISA reviewed all of the Categories and Subcategories and, based on business drivers and a risk assessment,
    - Determine which are most important.

- Information Security and Assurance added Categories and Subcategories to address the organization's risks, as needed.
- The Current Profile supports prioritizing and measuring progress toward the Target Profile while factoring in other business needs. Information Security and Assurance specifically considered the IT Priorities:
    - Enabling the Future of Teaching and Learning,
    - Expanding Digital Transformation,
    - Empowering the Future of Research,
    - Enhancing the Student Experience,
    - Fostering Innovation in Education and Work, and
    - Creating Strategic External Alliances when prioritizing.
- The Profiles are used to conduct self-assessments and communicate with the Office of Information Technology and business and strategic partners.

Organizational Structure Roles and Responsibilities

Information Security and Assurance

Fordham University created Information Security and Assurance because Information Security is critical to the privacy and integrity of Fordham University community members and its historical, educational, research, and operational missions. Information Security and Assurance, headed by the Chief Information Security Officer (CISO), is responsible for developing and implementing an information security program, including procedures and policies designed to protect University communications, systems, and assets from internal and external threats. Information Security and Assurance sets the overall direction of information security functions relating to Fordham University; these include IT risk management, security policies, security awareness, incident response, and security architecture. Since security risk is a business risk, Information Security and Assurance assesses and works with the strategic components of functional business units and operational security staff across all University IT organizations. Partnering with the business and IT, Information Security and Assurance cultivates relationships with users and department liaisons to set priorities, discuss issues of common concern, and manage expectations.

Key areas of focus for Information Security and Assurance include the security of enterprise-wide applications, communications, networks, computing services, and university-wide data stewardship. Additionally, Information Security and Assurance:

- Promotes the quality and integrity of information security throughout the University,
- Develops information security policy, obtaining ratification of the policy from key constituents, and oversees the implementation of this policy at the University,
- Builds a culture of information security,
- Educates the University concerning the implications of legislative requirements,
- Works closely and collaboratively with the University's Office of Public Safety to enhance the University's physical security and
- Works with the Office of Legal Counsel (OLC) to maintain the privacy of faculty, students, and staff within the University.

The CISO, in alignment with the University's strategic plan, chairs a University-wide Information Risk Management Board (IRMB) that guides on and advocates for information security standards and investments. Information Security and Assurance identifies security goals and objectives and develops

and implements policies, standards, procedures, and guidelines to support the University's strategic direction.

Information Security and Assurance Key Responsibilities and Services:

- Develop and maintain the security architecture,
- Oversee IT security-related risk management,
- Provide security for enterprise-wide applications,
- Handle incident responses,
- Provide a culture of information security throughout the University,
- Develop information security policies,
- Educate the University concerning the implications of legislative requirements,
- Identify security goals and objectives per University priorities,
- Conduct vulnerability assessments, penetration testing, forensics, and code analysis,
- Promote user security awareness,
- Approve security access requests,
- Provide authorizations,
- Manage security implementations,
- Provide ongoing compliance monitoring and
- Monitor network traffic.

Information Security

The security branch of Information Security and Assurance proactively manages the confidentiality, integrity, and availability of information in the custody of or processed by Fordham University. The mission is to protect the University's data and data processing assets. This department guards the network infrastructure, servers, desktops, applications, and University data against theft, misuse, breach, and compromise. To accomplish this, Information Security and Assurance may make use of the following areas of expertise:

- Audit
- Forensic analysis
- Incident response teams
- Security applications and hardware

Information Security and Assurance is responsible for creating, maintaining, deploying, and implementing security policies, procedures, standards, and guidelines. This department also oversees the forensic analysis of security events, leads Fordham's Incident Response Team (IRT) in the event of a security incident, and manages all security applications, hardware, and implementations.

Assurance

Assurance manages overall risks to the University's IT resources. Assurance develops, implements, and maintains a comprehensive Information Security and Assurance Program that incorporates security policy and compliance, security awareness, security risk assessment, and mitigation and information assurance.

Information Security and Assurance continually monitors the risk equation by analyzing IT's infrastructure and recommending the deployment of tools and third-party reviews to report on the status of:

- Risk Assessment
- Business Continuity

- Disaster Recovery
- Data Privacy
- IT Policy

Active monitoring of regulatory and legislative mandates that may apply to Fordham University is integral to the role. This includes creating awareness and documenting the requirements of various legislation of interest to institutes of higher education. Areas of compliance that Information Security and Assurance may become involved include, but are not limited to, Sarbanes Oxley, PCI DSS, GLBA, GDPR, and FERPA.

Key Leadership Roles

The IT leadership team consists of several key members who work together to provide thought leadership, define a security strategy, create a culture of risk awareness and security, and work with diverse operational areas across Fordham to protect what matters most to the Fordham community. Some of these leadership roles are:

Chief Information Officer (CIO)/Vice President, Office of Information Technology

The CIO provides information technology management, development, planning, procurement, and implementation activities to deliver quality information services and products for institutional and educational/academic environments. Provides executive leadership for organizational strategies, including digital, mobile, cloud, online, and collaboration, to reduce operating expenses and grow new markets.

- Creates technology alignment with corporate goals through effective working relationships with senior business leaders and the Board of Trustees
- Provides strategic focus and direction to integrate operational areas with the University's vision and goals:
    - Educate students as global citizens and transformative leaders for justice in the innovation age,
    - Excel across the natural and applied sciences and allied fields to promote social change, equity, and
    - Cultivate a diverse, equitable, inclusive, caring, and connected community that promotes each member's development as a whole person.
- Launches Advanced Analytics and Business Intelligence for critical analysis and decision-making
- Designs Governance and Portfolio Prioritization processes; and
- Delivers cost savings through optimized use of process improvement and sourcing

Chief Information Security Officer (CISO)/Associate Vice President, Office of Information Technology

Reporting to the VP & Chief Information Officer, the Associate VP/CISO is responsible for leading Fordham's Information Security and Assurance office, working with campus leadership to oversee the formation and operations of a university-wide information security capability to achieve a common goal in information security. The CISO is a member of the CIO leadership team and serves a key role in university leadership, working closely with senior administration, academic leaders, and the campus community. As an advocate for the Institution's total information security needs, the CISO is responsible for developing and delivering a comprehensive information security strategy to optimize the University's security posture. The CISO leads the development and implementation of a security program that leverages collaborations and campus-wide resources, facilitates information security governance,

advises senior leadership on security direction and resource investments, and designs appropriate policies to manage IT security risk.

Senior Director, IT Security and Assurance

Reporting to the CISO, the Senior Director of IT Security and Assurance identifies risks, threats, and weaknesses and advises on options for mitigation through research, investigations, and audit. In addition, the Senior Director develops, implements, and maintains a comprehensive assurance program that incorporates security policy, compliance, security awareness, security risk assessment, risk mitigation, and information assurance concerning disaster recovery and business continuity. This key role assists with deploying actions to support mitigation advice and conducting follow-ups to ensure enforcement. The role's information security responsibilities include recommendations for upgrades, repairs, modifications, and replacements of information security and change control procedures, systems, devices, or software. Additionally, the Senior Director designs and implements user security awareness solutions, access requests and authorizations, security implementations, and compliance monitoring. The Senior Director is responsible for developing, publishing, and maintaining information security policies, procedures, and guidelines. Working with executive management, the Senior Director determines acceptable levels of risk for the enterprise and is the senior auditor on IT-based audits directed by the CISO, Internal Audit, or the Office of Legal Counsel. The Senior Director oversees the forensic analysis of security events, leads the Fordham Incident Response Team (IRT) during a security incident, and manages all security applications, hardware, and implementations.

Director, Application and Systems Security

Reporting to the Assistant Vice President of DevOps and secondarily to the CISO, the Director of Application and Systems Security identifies and defines application and system security requirements. The Director recommends and coordinates the implementation of technical controls to support and enforce defined security policies for applications and systems. The Director ensures security is factored into the evaluation, selection, installation, and configuration of hardware, applications, and software. They work with the enterprise information security team to ensure the convergence of business, technical, and security requirements. This role has a strong working relationship with the security operations team to develop and implement controls and configurations aligned with security policies and legal, regulatory, and audit requirements. The Director manages and coordinates operational components of incident management, including detection, response, and reporting for applications and systems.

IT Policy Library

The repository contains the Office of Information Technology's policies, procedures, and guidelines regarding technology resources and services. Office of Information Technology provides resources and services to advance the University's educational, research, and business objectives. Access to or use of IT Resources that interfere with, interrupt, or conflict with these purposes is unacceptable. These documents provide notice of the University's expectations to all who use and manage services, including, but not limited to, computing, networking, communications, application, telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials. Policies include:

- Acceptable Use of IT Infrastructure and Resources
- Account Access Change Control
- Anti-Spoofing
- Antivirus Protection
- Audit and Accountability
- Authorized Access to Electronic Information
- Backup
- Business Continuity and Disaster Recovery
- Change Control
- Cloud Server Technical Control Requirements
- Corporate Accounts
- Data at Rest
- Data Center Sign In/Out
- Data Classification and Protection
- Data Documentation
- Data in Transit
- Disk Encryption
- Dual-Homed Network
- Email Retention
- Emergency Access via Privileged Access Management
- End of Life
- Extensions and Application Auxiliary Services
- Firewall/Access Control List
- Generic Accounts
- Hosting and Sharing Content
- Information Security Breach Response
- Information Security Incident Response
- Internet of Things
- IT Policy on Policies
- IT Resources Relocation
- IT Resources Remote Access
- IT Security
- Limitations on Production Data on Non-Production Environments
- Local Device Backup
- Logging Standards
- Multi-Factor Authentication
- Password Management
- Patch Management
- PCI Hardware Maintenance

- PCI Network Protocol
- PCI Security Testing
- Peer-to-Peer
- Physical Access
- Provisioning and Deprovisioning
- Risk Assessment
- Role-Based Email Accounts
- Secure Data Handling
- Server Certificate Security
- Secure Software Development Life Cycle
- Systems Hardening
- System and Communications Protection
- Temporary Student (TS) Accounts
- Third-Party Data Transfer
- Third-Party Integration
- Third-Party Sensitive Data Handling Inventory
- Vulnerability Management
- Wireless Use
- Web Application Security

Applicable Laws and Regulations

Information Security and Assurance monitors applicable laws, regulations, or directives impacting the Fordham environment. Laws, regulations, or directives (Federal or State) that establish specific requirements for confidentiality, integrity, or availability of data or information include, but are not limited to:

- Clery Act;
- Code of Federal Regulations: 21 CFR Part 11 (FDA);
- Digital Millennium Copyright Act (DMCA);
- Fair and Accurate Credit Transactions Act of 2003 (FACT Act; FACTA), which amended the Fair Credit Reporting Act (FCRA) and amendments thereof, including the Red Flags Rule (Identity Theft Prevention Program);
- Family Educational Rights and Privacy Act (FERPA);
- Federal Information Security Management Act (FISMA) of 2002;
- Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act; GLB Act; GLBA) Safeguards Rule;
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006;
- Freedom of Information Act (FOIA);
- General Data Protection Regulation (GDPR);
- Health Insurance Portability and Accountability Act (HIPAA);
- Higher Education Opportunities Act of 2008 (HEOA) Technology Mandates (Including illegal peer-to-peer file sharing, emergency notification, and distance education student verification);
- Homeland Security Presidential Directive (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection;
- Homeland Security Presidential Directive(HSPD-20), National Continuity Policy;
- Human Subjects Research, including the Federal Policy for the Protection of Human Subjects ("Common Rule");
- International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR);
- National Archives and Records Administration (NARA);
- New York State Information Security Breach and Notification Act;
- New York State Personal Privacy Protection Law;
- OMB Circular A-130 Management130 Management of Federal Information Resources, 2000;
- Payment Card Industry Data Security Standards (PCI DSS);
- Privacy Act of 1974, as amended;
- Sarbanes-Oxley Act of 2002;
- Social Security Act;
- Standard Confidentiality Agreement or Statement

NIST Cybersecurity Framework

NIST's CSF, summarized below, provides a structural foundation for this report. Actionable recommendations captured in this report can also be found in the accompanying Excel spreadsheet entitled *CRISP and CSF with University and IT Goals*. Each recommendation entry contains a notation of the appropriate corresponding NIST functions and categories from the list below.

Function 1: Identity

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts in a way that is consistent with its risk management strategy and business needs.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management

Function 2: Protect

Develop and implement appropriate safeguards to ensure the delivery of critical infrastructure services. The Protect Function supports limiting or containing the impact of a potential cybersecurity event.

Function Unique Identifier	Function	Category Unique Identifier	Category
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Function 3: Detect

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables the timely discovery of cybersecurity events.

Function Unique Identifier	Function	Category Unique Identifier	Category
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes

Function 4: Respond

Develop and implement the appropriate activities regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event.

Function Unique Identifier	Function	Category Unique Identifier	Category
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements

Function 5: Recover

Develop and implement the appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact of a cybersecurity event.

Function Unique Identifier	Function	Category Unique Identifier	Category
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Appendix A - Glossary

Common Terms	Definitions
Accreditation	The official management decision is given by a senior agency official to authorize the operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals based on the implementation of an agreed-upon set of security controls.
Administrative Controls	Refers to policies, procedures, or guidelines that define personnel or business practices in accordance with the organization's security goals. These can apply to employee hiring and termination, equipment and Internet usage, physical access to facilities, separation of duties, data classification, and auditing. Security awareness training for employees also falls under the umbrella of administrative controls.
Authentication	Verifying the identity of a user, process, or device is often a prerequisite to allowing access to resources in an information system.
Availability	Ensuring timely and reliable access to and use of information.
Business Critical	An IT Resource that requires special management attention because of its importance to a particular business entity, its high development, operating, or maintenance costs, or its significant role in the business programs, finances, property, or other resources.
Compensating Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization instead of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53 that provide equivalent or comparable protection for an information system.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Data Owner	An official with statutory or operational authority for specified data and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.
IT Policies	The aggregate of directives, regulations, rules, and practices prescribes how an organization manages, protects, and distributes information.

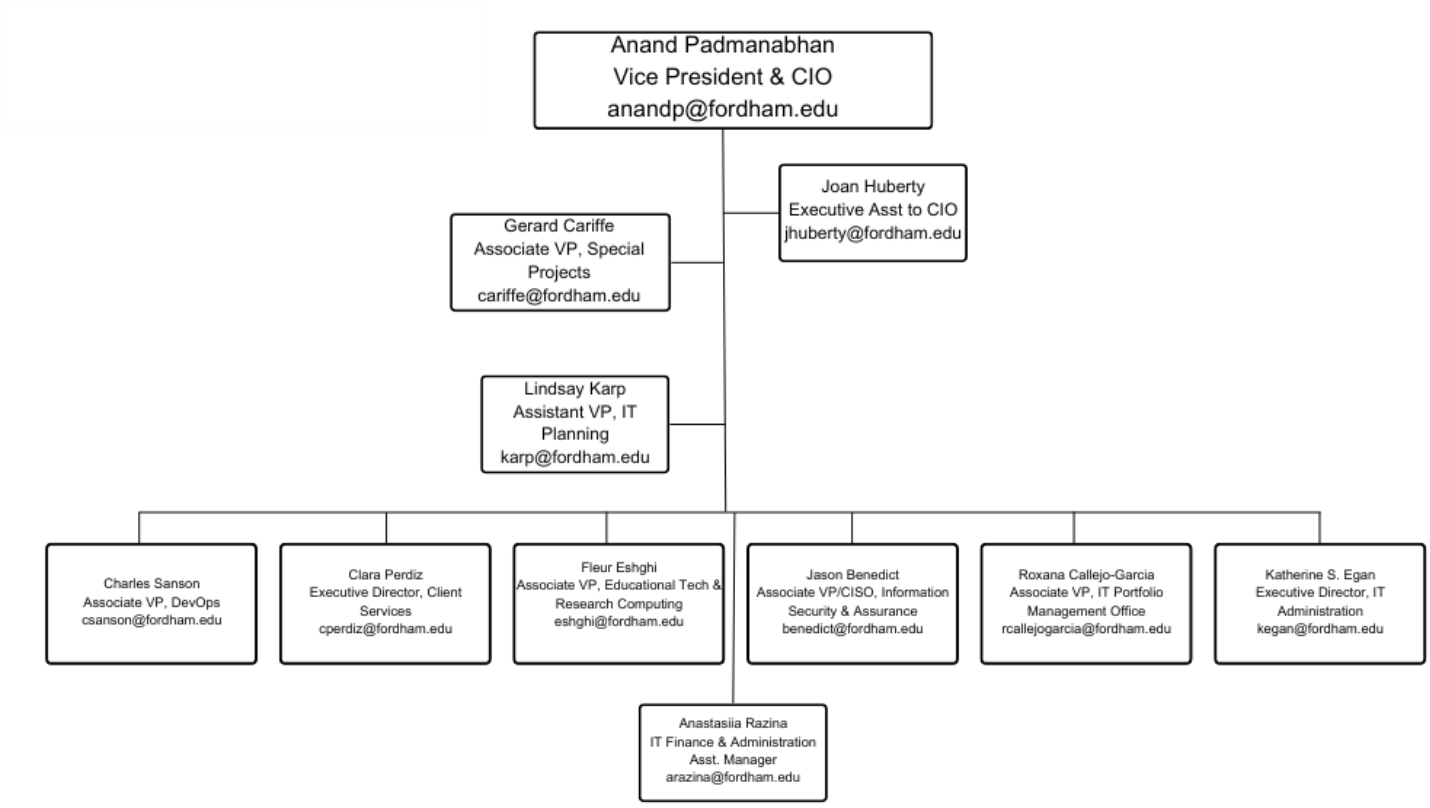
Common Terms	Definitions
IT Resources	Includes computing, networking, communications, application, and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.
Information Security Engineer	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner to ensure that the appropriate operational security posture is maintained for an information system or program.
Integrity	Guarding against improper information modification or destruction includes ensuring information non-repudiation and authenticity.
Mission Critical	An IT Resource that requires utmost attention because of its importance to the University's mission, its high development, operating, or maintenance costs, or its significant role in the administration of agency programs, finances, property, or other resources.
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system are primarily implemented and executed by people (as opposed to systems).
Physical Controls	Describes anything tangible that's used to prevent or detect unauthorized access to physical areas, systems, or assets. This includes things like fences, gates, guards, security badges and access cards, biometric access controls, security lighting, CCTVs, surveillance cameras, motion sensors, fire suppression, and environmental controls like HVAC and humidity controls.
Privacy	Privacy is personal information usually related to personal data stored on computer systems. Maintaining information privacy involves collecting personal information, such as medical, financial, criminal, political, business-related, or website data. Information privacy is also known as data privacy.
Remote Access	Access by users (or information systems) communicating externally to an information system security perimeter.
Risk	The level of impact on operations given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment	Process of taking identified risks and analyzing their potential severity of impact and likelihood of occurrence.
Risk Management	Ongoing management process of assessing risks and implementing plans to address them.
Security Controls	The security controls (i.e., safeguards or countermeasures) for an information system focus on managing risk and information system security, including administrative/managerial controls, physical controls, technical controls, and operational controls.

Common Terms	Definitions
Security Requirements	Integrate information security principles into all aspects of the University's activities. Ensure that reasonable security policies, standards, controls, processes, practices, and procedures are established and maintained to safeguard IT Resources. Follow a risk-based approach to protect the assets' confidentiality, integrity, and availability as business needs and IT Resources change. Operate IT security activities effectively, responsibly, and ethically, complying with all global, federal, state, and local laws and regulations. Protect the IT Resources' confidentiality, integrity, and availability commensurate with their risk and value while maintaining accessibility.
System Owner	The system owner is the individual or group responsible for the procurement, development, integration, modification, operation, maintenance, and retirement of the server, operating system, or other elements that support the application owner in providing services. The System Owner provides the technical infrastructure for system state and data retention backups. If a third party provides these services, the System Owner is responsible for maintaining the relationship with the third party providing the service.
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system are primarily implemented and executed by the information system through mechanisms contained in the system's hardware, software, or firmware components.
User	Individuals who use, access, or otherwise employ, locally or remotely, the University's IT Resources, whether individually controlled, shared, stand-alone, or networked.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that can be exploited or triggered by a threat source.
Vulnerability Assessment	Formal description and evaluation of the vulnerabilities in an information system.

Appendix B – IT Organizational Charts

Below are high-level organizational charts for the Chief Information Officer (CIO) and Information Security and Assurance office.

Office of the CIO



Information Security and Assurance