SOUTHERN ILLINOIS UNIVERSITY
OFFICE OF INFORMATION TECHNOLOGY

Policy of the Information Security Program

Document Number:	ISP-001
Document Owner:	Director of Information Security
Responsible Office:	Office of Information Technology
Version:	1.4
Effective Date:	May 5, 2015
Last Update:	May 27, 2025

(This Page Intentionally Blank)

Table of Contents

Purpose

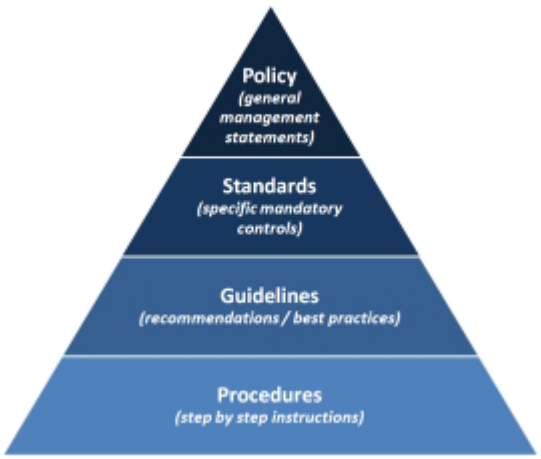
This document establishes the policy for the Information Security Program (ISP) at Southern Illinois University Carbondale (SIU) and is intended to satisfy the requirements as set forth by the Southern Illinois University Board of Trustees Policy, SIU System Information System Plan Charter.

The formation of this policy is driven by many factors, the key one being Risk. This policy sets the ground rules under which SIU shall operate and safeguard its information and information systems to reduce the risk and minimize the effect of security incidents and cyber security threats. Included within this policy are the collective methods, technologies, and processes to help protect the confidentiality, integrity, and availability of computer systems, networks, and data, against cyber-attacks and unauthorized access from both external and internal threats.

Background

Information Documentation Framework

Within the framework of this ISP, SIU will implement numerous **Policies, Standards, Guidelines** and **Procedures** to ensure the security of university information and to comply with the security controls included herein.



Policies are formal, brief, and high-level statements or plans that embraces an organization's general beliefs, goals, objectives, and acceptable procedures for a specified subject area. Policies always state required

actions and may include pointers to **Standards**. Policy attributes include the following:

- Description of mandatory actions, with descriptions of benefits and consequences of non-compliance.
- A description of the desired results, not on means of implementation.
- Further definition provided in **Standards** and **Guidelines.**

Standards are mandatory rules designed to support and conform action(s) to a policy.

- A standard should make a policy more meaningful and effective.
- A standard must include one or more accepted specifications for hardware, software, or behavior.

Guidelines are general statements, recommendations, or administrative instructions designed to achieve the policy's objectives by providing a framework within which to implement **Procedures**.

- A guideline is not mandatory, rather a suggestion of a preference or best practice.
- Because best practices for an industry occasionally change, or are sometimes interpreted differently by individuals, guidelines will likely change more frequently than **Policies** and **Standards**.

Procedures describe the process: who does what, when they do it, and under what criteria. Procedures can be text-based or outlined in a process map. Procedures represent implementation of **Policy** and are typically mandatory actions to include:

- A series of steps taken to accomplish an end goal.
- "How" to protect resources and serve as the mechanism to enforce policy.
- A quick reference in times of crisis.
- Steps to eliminate the problem of a single point of failure.
- Standard Operating Procedures (SOP).

Information Security Control Organization

SIU collects, generates, and stores student, financial, employee and other sensitive information. Most of this information has access restrictions required by legislative and regulatory directives. As the information's trusted custodian, SIU must protect and ensure the Confidentiality, Integrity, and Availability (CIA) of all its information regardless of how it is created, distributed, or stored.

To safeguard the CIA of its information and information systems effectively, SIU has established this enterprise-wide ISP. As part of this program, security controls must be implemented to protect all information assets, including hardware, software, and data at-rest or in-motion. These controls must be designed to ensure compliance with all federal and state legislation, policies, and standards (e.g., by managing risk; facilitating change control; reporting and responding to security incidents, intrusions, or violations; and formulating contracts.)

This policy addresses the reduction in risks to information resources through adoption of preventive measures and controls designed to detect any threats that occur. SIU has established three (3) classes of ISP controls: Management, Operational, and Technical. This structure is consistent with the guidance established by the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, as well as selected components from National Institute of Standards and Technology (NIST), Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*.

NIST SP 800-171 is designed to protect Controlled Unclassified Information (CUI) in nonfederal systems, including universities, which potentially handle federal information through contracts, grants, or research partnerships.

Management controls involve those safeguards and countermeasures that manage the security of the information and information systems, and the associated risk to SIU's assets and operations. There are five (5) families of policy within the Management class that address:

- Security Assessment and Authorization (CA)
- Planning (PL)
- Risk Assessment (RA)
- System and Services Acquisition (SA)

- Program Management (PM)

Operational controls support the day-to-day procedures and mechanisms to protect SIU' information and information systems. There are eight (8) families of policy within the Operational class that address:

- Awareness and Training (AT)
- Configuration Management (CM)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Personnel Security (PS)
- System and Information Integrity (SI)

Technical controls are those security mechanisms employed within an information system's hardware, software, or firmware to protect the system and its information from unauthorized access, use, disclosure, disruption, modification, or destruction. They are used to authorize or restrict the activities of all levels of users within an individual system by employing access based on a least-privileged and need-to-know approach. There are four (4) families of policy within the Technical class that address:

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)
- System and Communications Protection (SC)

Security Categorization

Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires that all federal systems must be associated with a system security level by evaluating the potential impact value (High, Moderate or Low), for each of the three security objectives of confidentiality, integrity and availability (CIA). SIU has pre-determined, using FIPS Publication 199 and

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, all the applicable SIU System Data Classification Levels (DCL) for the various information types processed by SIU information systems. See SIU's Data Classification Policy. This security categorization is the basis for selecting appropriate security controls for SIU information systems as well as assessing the risks to SIU operations and assets.

Methodology

Review

Annually, SIU will perform a review of the current baseline controls established in the SIU ISP. Adjustments, with senior management concurrence, are applied to the ISP to reflect the current information security requirements established by NIST SP 800-171, applicable components of NIST SP 800-53, and any other federal or state law.

- Information assets must reflect the applicable security controls established for the appropriate SIU DCL.
- In exceptional circumstances, deviations from the associated security control of the DCL can be requested with explicit justification in respect to specific mission and business processes, organizational requirements, and environments of operation along with alternate risk mitigations through the Information Security Office to obtain written approval from the SIU Chief Information Security Officer (CISO).
- Data Custodians may choose to evaluate additional security controls based on an assessment of risk and local conditions, including, but not limited to:
    - Specific and credible threat information,
    - Organization-specific security requirements,
    - Cost-benefit analyses, and
    - Special circumstances.

Implement

The implementation of security controls to protect SIU's mission and business processes is tightly coupled to the enterprise architecture and integrated into the System Development Life Cycle (SDLC). Knowledgeable individuals within the organization (e.g., system architects, systems/security engineers, system administrators, physical security experts, personnel specialists) shall determine which personnel, processes, hardware, software, facilities, or environmental components within the defined information system boundary are providing specific security functionality. There should be close coordination and collaboration among organizational personnel to ensure that the needed security functions are allocated to the appropriate systems and supporting infrastructure.

For common security controls, the organization should allocate the controls to entities, either internal or external to the organization, with the responsibility for their development, implementation, and assessment. Certain security controls employed within SIU information systems require that security configuration settings be established during implementation. For many technologies, SIU defines mandatory configuration settings for information technology products that are used within SIU Information Systems to comply with configuration settings-related legislation, directives, and policy requirements. Mandatory security configuration settings shall be enforced across SIU, including all systems that are supporting organizational mission/business processes.

Assess

The security controls must be tested and evaluated prior to system deployment to ensure that the controls are effective. A Security Assessment Plan is developed and executed for each system to test the security controls. This test provides feedback as to the effectiveness of implemented security controls to Data Custodians and System Developers/Maintainers and is one of the factors that may affect the decision to deploy. Satisfactory completion of the Assessment and Authorization (A&A) is an essential milestone for the security authorization of new systems to assure compliance with SIU information security policy and standards as well as providing the desired functionality.

Authorize

Security authorization of a system to process, store, or transmit information is required. This authority to operate is granted by the SIU CIO or their designee and is based on the verified effectiveness of the security controls to SIU policy and standards together with an identified risk to the organization's operation or assets.

Monitor

Periodic or continuous testing and evaluation of security controls in an information system are required on an on-going basis to ensure that the controls continue to be effective in their application. The comprehensive evaluation of security control effectiveness through established verification techniques and procedures is a critical activity conducted by the university or by an independent third party on behalf of the university. The on-going monitoring of security control effectiveness is accomplished in a variety of ways including security reviews, self-assessments, and various audits.

Scope

This policy applies to all SIU information, information systems, information technology activities, and information technology assets owned, leased, controlled, or used by SIU, SIU's agents, contractors, or other business partners on behalf of SIU.

This policy applies to all SIU employees, contractors, sub-contractors, and their respective facilities supporting SIU business missions, wherever SIU data is stored or processed. Some policies are explicitly stated for persons with a specific job function (e.g. the System Administrator); otherwise, all personnel supporting SIU business functions shall comply with the policies. SIU operating departments shall use this policy or may create a more restrictive policy, but not one that is less restrictive, less comprehensive, or less compliant than this policy.

This policy does not supersede any other applicable law or higher-level agency directive, or existing labor management agreement in effect as of the effective date of this policy.

Policy

SIU's policies and controls have a well-defined organization and structure. Security policies and controls are organized into classes and families for ease of use in the control selection and specification process. There are three (3) general classes of security policies and controls (i.e., Management, Operational, and Technical) and seventeen (17) security policy and control families as specified in NIST SP 800-171.

Each family contains security policies and controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each policy and control family. The following table summarizes the classes and families in the security control catalog and the associated family identifiers, as well as the order of the included policies.

Table 1: NIST SP 800-171 Information Security Control Families and Classes

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Organizational Security Program Management	Management

These families are based on the NIST SP 800-171 framework and are tailored to the needs of non-governmental organizations, such as universities. Among the control families, sixteen closely align with the seventeen minimum security requirements for federal information and information systems outlined in FIPS 200. The remaining minimum-security requirement, Contingency Planning, is incorporated into both

System and Communications Protection (SC) and System and Information Integrity (SI) within the NIST 800-171 control families.

The Program Management [PM] family provides organizational-level controls for information security programs, complementing the sixteen families of system-level security controls. These PM controls focus on organization-wide information security needs that are independent of any specific information system and essential for managing security programs. Section 4.2 of this policy fully addresses the PM family of controls.

Security Controls

Security requirements for all information systems shall be used and effectively implemented.

Note: Within some controls the context and scope of "information system" may differ. The applicability of a particular control to an associated information system will be dependent on the DCL of the system and at the discretion of the CISO. Underlying standards, procedures, and guidelines will further define the applicability of a particular information system to a control.

The minimum-security requirements shall include:

Access Control (AC)

Information system access must be limited to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise. Users shall only be authorized to access University computing assets with the necessary privileges and permissions needed to accomplish their jobs. Authorized users will be granted access only after appropriate approval. Processes to govern access based on initial employment and subsequent termination shall be implemented and strictly enforced.

- Unsuccessful Logon Attempts: Information systems shall establish and enforce a set limit of consecutive invalid logon attempts consistent with the system's classification. Access shall be automatically locked when the maximum number of unsuccessful logon attempts have been exceeded.

- Session Lock: A sufficient number of unsuccessful login attempts shall be established and strictly enforced to govern access to information systems.

- Session Termination: Sufficient time limits to govern system inactivity shall be established and strictly enforced to terminate information system sessions.
- Remote Access: External access to information systems will be governed by system classification and authorized based on user roles and responsibilities.

Awareness and Training (AT)

Managers and users of information systems must be made aware of the security risks associated with their activities and of the applicable federal and state requirements related to the security of SIU information systems. Those with significant security responsibilities must be adequately trained to carry out their assigned information security-related duties and responsibilities. Awareness and training programs must be provided to users pertaining to acceptable use of computing resources, how to use information systems, appropriate security safeguards, individual responsibility, recognizing and mitigating cyber security threats, and safe handling of sensitive information.

Acceptable Use Standard

Sensitive Information Standard

Workstation Standard

Audit and Accountability (AU)

Information system audit records must be created, protected, and retained to the extent needed to: (i) enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Security Assessment and Authorization (CA)

As part of the security authorization process production information systems must: (i) be assessed for risk at least every three years or whenever a significant change occurs to the information system; (ii) have plans of action with milestones documented, tracked and closed to mitigate any security control deficiencies identified during an assessment; (iii) be authorized for operation in writing by the Chief Information Security Officer (CISO); (iv) have all external associated information system connections identified and

documented in an Interconnection Security Agreement prior to establishing connectivity to the University network; and (iv) be monitored on an ongoing basis to ensure the continued effectiveness of the security controls.

Configuration Management (CM)

Baseline configurations and inventories of production information systems (including hardware, software, and documentation) must be established and maintained throughout the system's life cycle; security configuration settings for all software employed in information systems must be established and enforced; all changes to production information systems must be identified, documented, and approved prior to being implemented by authorized personnel.

Change Management Policy

Identification and Authentication (IA)

Information system users, processes acting on behalf of users, or devices must be uniquely identified and authenticated prior to access of the information systems. Users shall be assigned individual accounts augmented by strong passwords and use appropriate authentication techniques to ensure proper information system access.

Password Standard

Identity and Access Standard

Identity and Access Procedures

Incident Response (IR)

A documented operational incident handling capability for information systems must be established that includes preparation, detection, analysis, containment, recovery, and user response activities. Incidents must be tracked, documented, and reported to appropriate offices. This document shall be reviewed, updated, and approved annually by the CISO.

Incident Response Standard

Infection Response Procedures

Vulnerability Response Procedures

Maintenance (MA)

Periodic and timely maintenance on organizational information systems must be performed. Sufficient controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance must be established.

Media Protection (MP)

Information system media, both digital (hard drives, removable devices, CDs, DVDs) and non-digital (paper) must be protected by: (i) limiting access to information on information system media to authorized personnel; (ii) sanitizing all digital or destroying digital/non-digital media before disposal or release for reuse; and (iii) protecting information on digital media appropriate to the data classification.

Data Classification Policy

Sensitive Information Standard

Workstation Standard

Physical and Environmental Protection (PE)

Physical access to information systems, equipment, and the respective operating environments must be limited to authorized individuals. This includes the following:

- The physical plant and support infrastructure for information systems.
- Supporting utility ingress into any physical plant and support infrastructure for information systems.
- Providing adequate physical protection of information systems from environmental hazards.
- Requiring physical access control (i.e. locks, proximity card readers, etc.) to facilities containing information systems.
- Providing appropriate environmental controls in facilities containing information systems.

Planning (PL)

A System Security Plan (SSP) document shall be developed for each production information system. The SSP shall be approved in writing by the

CISO and the System Administrator. The SSP shall be reviewed, updated, and re-approved by the same individuals annually or if there is a significant change to the system or threat environment.

Personnel Security (PS)

SIU information systems shall employ personnel security controls consistent with applicable laws, policies, directives, regulations, standards, and guidelines. Procedures shall be developed to guide the implementation of personnel security controls.

- Upon hire and annually thereafter, all information system users shall review and sign an Acceptable Use document outlining accepted University information system use and the consequences of non-acceptable information system use.
- Individuals occupying positions of responsibility within organizations (i.e., including third-party service providers) must be trustworthy and meet established security criteria for those positions.
- Information and information systems must be adequately protected when personnel actions are enacted such as initial employment, terminations, and transfers.
- Formal sanctions for personnel failing to comply with organizational security policies and procedures must be employed.

Risk Assessment (RA)

The risk to university operations (i.e., including mission, functions, image, or reputation), assets, and individuals, resulting from the operation of University information systems and the associated processing, storage, or transmission of organizational information must be assessed and documented. A risk assessment for each production information system shall be performed prior to promoting a new system to the production environment and updated at least every three years thereafter or whenever there is a significant change to the information system, its threat environment, or if a data breach occurs. Each risk assessment shall be approved in writing by the CISO and the System Administrator.

Minimum security controls for each system shall be supplemented, as warranted, based on an assessment of risk and local conditions including SIU-specific security requirements, specific threat information, cost-benefit analysis, or special circumstances.

System and Services Acquisition (SA)

Documented procedures shall be developed and implemented for managing risks from third party products and services' providers. The intent is to establish a method that will be used to evaluate third party services which host SIU information and third-party products which are procured to process SIU information, for information security risks. These procedures shall be consistent with applicable laws, directives, policies, regulations, standards, and guidance.

- Allocation of Resources: SIU shall determine, document, and allocate the resources required to protect the information system as part of its capital planning and investment control process.
- System Development Life Cycle: All identified systems and services for procurement shall be reviewed for support through all security lifecycle activities (Initiation, Acquisition/Development, Implementation/Assessment, and Operations/Maintenance).
- Acquisition Process: Security specifications, either explicitly or by reference, shall be included in information system acquisition contracts based on an assessment of risk and in accordance with applicable regulatory requirements and industry best practices.
- Security Engineering Principles: Architectural designs, software development techniques, and systems engineering principles that promote effective information security within information systems must be employed.

System and Communications Protection (SC)

Documented technical procedures shall be developed and implemented to ensure the protection of SIU information systems and system communications commensurate with each systems' security categorization and to mitigate risk posed by cyber security threats. The intent of this policy is to implement security best practices with regard to system configuration, data communication and transfer. Procedures shall be developed, documented, and implemented to guide the configuration and management of each system. The procedures shall be consistent with applicable laws, policies, regulations, standards, and guidance; and shall be reviewed and updated as necessary.

- Boundary Protection: Communications (i.e., information transmitted or received by SIU information systems) at the external boundaries and

key internal boundaries of the information systems must be monitored, controlled, and protected. Information systems shall connect to external networks or information systems only through centrally managed interfaces consisting of authorized boundary protection devices. A limited number of external network connections shall be authorized to information systems. Information systems at managed interfaces shall deny network communication traffic by default and allow network communication traffic by exception (i.e., deny all, permit by exception). Host-based boundary protection (i.e., host-based firewalls) must be incorporated appropriate to the DCL of the information system. Boundary protection mechanisms shall be used to separate information system components supporting unique business function.

Network Connection Standard

Wifi Standard

System and Information Integrity (SI)

The system and information integrity policy establishes requirements for managing risks from system flaws/vulnerabilities, cyber security threats, malicious code, unauthorized code changes, and inadequate error handling. The intent of this policy is to establish a system and information integrity capability throughout SIU and its business units to help SIU implement security best practices with regard to system configuration, security, and error handling.

- Flaw Remediation: Information system flaws (e.g., security vulnerabilities/exposures, etc.) must be identified, reported, and corrected in a timely manner unless prohibited by extenuating circumstances such as cost, loss of critical functionality, fix availability, etc. All software updates (e.g., patches, service packs, hot fixes, etc.) related to flaw remediation must be tested for effectiveness and potential side effects on SIU information assets before installation. Flaw remediation must be incorporated into the SIU configuration management process and centrally managed. Automated mechanisms shall be used to determine the state of information systems with regard to flaw remediation and to update information system components accordingly. Measures must be taken to limit the time between flaw identification and flaw remediation.

- Malicious Code Protection: Protection from malicious code threats must be provided at appropriate locations within organizational

information systems. Malicious code protection mechanisms must be updated when new releases are available in accordance with SIU configuration management policy and procedures. Periodic scans of information systems and real-time scans of files downloaded, opened, or executed will be performed. Malicious code protection mechanisms will be centrally managed and automatic updates applied consistent with the SIU configuration management process.

- Information System Monitoring: Enterprise-wide intrusion detection/prevention systems and technologies shall be implemented and maintained to monitor inbound and outbound communication. Security alerts shall be expeditiously acted upon including appropriate remediation steps.

- Security Alerts, Advisories, and Directives: Information system and cyber security alerts and advisories issued shall be monitored and appropriate action taken in response.

Additionally, contingency plans for emergency response, backup operations, and disaster recovery for production information systems must be documented, maintained, and tested annually to ensure the availability of critical information resources and continuity of operations in emergency situations. This document shall be reviewed, updated, and approved annually by the CIO, CISO, and pertinent System Administrator.

Organizational Security Program Management (PM)

Organizational security program management controls are required of SIU (including colleges, offices, and departments), SIU agents, contractors, sub-contractors or other business partners performing work on behalf of SIU and that apply to their respective facilities that support SIU business missions, wherever SIU data is stored or processed. These security requirements focus on University-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. These controls are subject to the approval, evaluation, review, monitoring, and correction processes for information systems, but are implemented separately from and are inherited by information systems. Minimum security controls include:

Information Security Program Plan

The CIO or CISO shall review (at least annually) and update as needed this ISP to ensure that it minimally contains:

- An overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.
- Sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended.
- Roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- Approval by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), and assets.

Senior Information Security Officer

The SIU CIO shall appoint a CISO with the mission and resources to coordinate, develop, implement, and maintain this ISP.

Information Security Resources

SIU Data Custodians shall, at a minimum:

- Ensure that all capital planning and investment requests include the resources needed to implement the elements of this information security program and documents all exceptions to this requirement.
- Record the resources required. SIU Data Custodians shall use a business case methodology to record the resources required.
- Ensure that information security resources are available for the expenditure as planned.

Plan of Action and Milestones Process

SIU Data Custodians shall implement the SIU CISO-specified process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions

(from identification of needed action through assessment of implementation) to mitigate risk to organizational operations and assets.

Information System Inventory

SIU Data Custodians shall develop and maintain an inventory of information systems.

Enterprise Architecture

A SIU enterprise architecture shall be developed, and maintained, by the SIU CIO, with consideration for information security and the resulting risk to organizational operations and assets. Contractors of SIU and Business Partners shall design, develop, implement, and operate SIU related information systems in accordance with the SIU enterprise architecture.

Risk Management Strategy

SIU Data Custodians shall:

- Develop a comprehensive strategy to manage risk to organizational operations and assets associated with the operation and use of information systems.
- Implement that strategy consistently across their organization and in compliance with this ISP.

Security Authorization Process

SIU Data Custodians shall:

- Manage (i.e., document, track, and report) the security state of organizational information systems through the appropriate security authorization processes as defined in this ISP.
- Fully integrate the security authorization processes into their risk management program.

Business Process Definition

SIU Data Custodians shall:

- Define business processes with consideration for information security and the resulting risk to organizational operations and assets.
- Determine information protection needs arising from the defined business processes and revise the processes as necessary, until the risk of the process execution is within acceptable levels determined by the SIU CISO.

Information Security Workforce

An information security workforce development and improvement plan shall be developed to define the knowledge and skill levels required to perform information security functions, ensure that qualified personnel are hired, and provide adequate and appropriate training to information security staff.

Contacts with Security Groups and Associations

SIU shall establish and institutionalize contact with appropriate security groups and associations within the security community to facilitate ongoing security education and training, maintain currency with recommended security practices, techniques, and technologies; and share current security-related information including threats, vulnerabilities, and incidents.

Testing, Training, and Monitoring

SIU shall develop and maintain a process to ensure that organizational plans for conducting security testing, training, and monitoring are developed and maintained, and continue to be executed in a timely manner. These plans shall be reviewed for consistency in accordance with organizational risk strategy.

Roles and Responsibilities

The following entities have responsibilities related to the implementation of this program policy.

Chief Information Officer (CIO)

The CIO has the overall responsibility for the implementation of a University-wide ISP, as required by Southern Illinois University Board of Trustees policy, for the purposes of compliance with applicable federal and state laws.

The CIO is responsible for the following:

- Ensuring that SIU has trained personnel sufficient to assist in complying with the requirements of this policy and related procedures, standards and guidelines.
- Ensuring that the SIU CISO reports annually to the SIU CIO on the effectiveness of the SIU ISP, including progress of remedial actions.
- Ensuring there is an appropriate level of protection for all SIU information resources, whether retained in-house or under the control of contractors, including the establishment of operational, management and technical safeguards.
- Assisting University Stakeholders in understanding their security responsibilities and ensuring that they incorporate an acceptable level of protection for all SIU IT Systems.
- Providing Executive oversight of the SIU ISP, as well as University-wide security directives.
- Designating a Chief Information Security Officer (CISO).
- Training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and
- Assisting senior SIU administration concerning their responsibilities regarding information and information systems that support operations and assets under their realm of responsibility.

Chief Information Security Officer (CISO)

The SIU CISO is responsible for the following activities:

- Authorizing, in writing, the acceptance of risk to operate each production information system in support of the University's mission.
- Developing, implementing, and administering the SIU ISP, as well as University-wide security directives.
- Developing and maintaining this policy, information security procedures, and control techniques to address federal and state requirements.

- Providing information security protections commensurate with this policy, the SIU ISP and federal and state regulations.
- Developing and implementing an information system security training and orientation program.
- Developing, evaluating and providing information about the SIU ISP, and communicating SIU ISP requirements and concerns to SIU management and personnel.
- Ensuring that pertinent security guidelines and procedures are developed, reviewed, implemented, and revised within applicable colleges, offices, and departments.
- Maintaining documentation used to establish appropriate systems security level designations for decentralized systems within SIU.
- Providing leadership & participating in incident response and reporting information security incidents in accordance with reporting procedures developed and implemented federal, state, and SIU requirements.
- Mediating and resolving systems security issues across the University.
- Assuring that SIU colleges, offices, and departments are adequately informed, supported, and trained.
- Assuring that SIU professional IT staff develop local systems security; and
- Researching state-of-the-art systems security technology and disseminating information material in a timely fashion.

Information Technology (IT) Professionals

IT Professionals are responsible for the following activities:

- Assisting the CISO in ensuring that their college, office, or department adheres to laws, directives, regulations, policies, standards, and SIU ISP requirements.
- Serving as a point of contact within their respective college, office, or department for information security issues; and

- Participating in the technical development and certification of applicable security standards, guidelines, and procedures within their respective college, office, or department.

Data Custodian

Data Custodians are responsible for the following activities:

- Assessing the risk to the information and information systems over which they have responsibility.
- Ensuring, through system certification, that the SIU information systems over which they have responsibility are developed, implemented, operated, and documented according to the requirements of this policy.
- Certifying that SIU information systems fully comply with SIU ISP requirements; and
- Ensuring appropriate security measures and supporting documentation are maintained.

System Administrator

System Administrators are responsible for the following activities:

- Verifying that system security requirements of their systems are being met.
- Establishing and communicating the security safeguards required for protecting systems based on the sensitivity levels of the information; and
- Periodically reviewing and verifying that all users of their systems are authorized and are using the required systems security safeguards, in compliance with the SIU ISP and all related standards, guidelines, and procedures.

System Developer/Maintainer

System Developers/Maintainers are responsible for the following activities:

- Developing and implementing the ISP requirements throughout the SDLC; and

- Planning and implementation for the on-going maintenance of the information system, including updates, upgrades, and patches in accordance with the SDLC and this policy.

SIU/Business Partner/Contractor Employees

SIU / Business Partner / Contractor employees have the responsibility to ensure the protection of SIU information (data) and information systems by complying with the ISP requirements maintained in this policy. Use of University-owned or leased equipment and resources to accomplish work-related responsibilities will always have priority over personal use. In order to avoid capacity problems and to reduce the susceptibility of organization information technology resources to computer viruses and cyber-attacks, employees shall comply with the following requirements:

- Personal files obtained via the Internet may not be stored on individual PC hard drives or on LAN file servers.
- Official video and voice files may not be downloaded from the Internet except when they will be used to serve an approved organization function; and
- Internet and email etiquette, customs and courtesies shall be followed when using University-owned or leased equipment or resources.

Users

Users, or “end users”, have the responsibility to ensure the protection of SIU information (data) and information systems by complying with the ISP requirements maintained in this policy. Users shall attend or participate in required information security and functional training. In addition, SIU employee-users shall adhere to the duties, requirements, and responsibilities as determined by their position, Board of Trustees policy, University policy, and this ISP.

Definitions

Application

An application is a software program or suite of programs that provides an information management, retrieval or display function for more than one individual. For the purposes of the password policy standard, application generally refers to AIS and Banner, including the underlying Oracle

databases, as well any other enterprise level application in support of SIU business processes.

Change Management

Process of recording, evaluating, approving, planning, and overseeing the implementation of a change in a controlled and efficient manner.

Change

Any modification to an existing system/service, maintenance of an existing system/service or a project to install a new or upgraded system/service.

This includes but is not limited to application installations and upgrades, hardware installations and upgrades, operating system upgrades, configuration changes, web page modifications, network installations and upgrades, and patch installations.

It does not include files written by the computer user, other data files, email messages and similar files provided they do not include any executable instructions or otherwise modify systems or operating software.

Data Custodian

Employee of the University who has administrative and/or operational responsibility over information assets.

Fix

A change to a system to rectify an identified failure to function as required. From the point of view of Change Management, there is little fundamental distinction between Enhancement and Fix.

Similarly, changes can be major (for example implementing a new release of a corporate system) or minor. Again, the scale of the change does not fundamentally affect the process; however, changes significant enough to be formally project managed will thereby satisfy the Change Management Policy.

Infrastructure

Infrastructure refers to IT resources and systems including operating systems, computer hardware and networks provided and supported by IT for use across the university.

Information System

An information system is a discrete set of information resources and components organized expressly for the collection, creation, storage, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems typically include hardware, software, infrastructure, users and the underlying data.

Maintenance

Maintenance refers to routine updates to an administrative process on existing IT resources and systems that carry a minimal level of risk and do not result in disruption of operation.

Passwords

Passwords are short sequences of letters, numbers, and symbols that are entered to verify the user's identity to a system, which then allows access to secure data or other resources. The role of a password is to prevent unauthorized access to data just as a key prevents unauthorized access to a house or apartment.

Production

Any current system/service that is utilized in support of the mission of the university, without which university business would be severely impacted.

Compliance

Violations of this Standard may result in suspension or loss of the violator's use privileges, with respect to Institutional Data and University owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the University. Civil, criminal and equitable remedies may apply.

References

FISMA Act of 2002, Public Law (P.L.) 107-347

FIPS Publication 199

FIPS Publication 200

NIST SP 800-18

NIST SP 800-23

NIST SP 800-30

NIST SP 800-47

NIST SP 800-53 Rev. 5

NIST SP 800-171 Rev. 3

Authority

Southern Illinois University Board of Trustees Policy, SIU System Information Security Plan.

Southern Illinois University Carbondale Policy, Information Security Charter.

Management Commitment

This policy is intended to represent SIU management's commitment to instituting a framework with which to operate all SIU computing assets with minimal risk to the mission of the University.

Approved By	Title	Date
	Acting Director of Information Security	05/27/2025

Revision History

Version	Description	Revision Date	Reviewed By
1.0	Standard was approved by CIO.	07/01/2015	Director of Information Security
1.1	Reviewed. Reformatted title page, fixed broken links, and removed outdated definitions.	08/22/2019	Director of Information Security
1.2	Reviewed. Added language/links specific to Identity and Access Management. Corrected hyperlinks to reference new OIT policies page.	02/19/2020	Director of Information Security
1.2	Reviewed and approved by CIO.	02/20/2020	Director of Information Security
1.2	Updated embedded title to properly display on a webpage.	03/04/2020	Director of Information Security
1.2	Corrected broken link to the Network Connection Standard	12/15/2020	Director of Information Security
1.2	Reviewed, no changes.	06/08/2021	Director of Information Security
1.3	Clarified sections of and added language regarding cyber security. Corrected minor grammatical and formatting errors and inconsistencies.	08/05/2021	Director of Information Security
1.3	Reviewed, no changes	05/11/2022	Acting Director of Information Security and Associate Director, PMO.
1.3	Reviewed, no changes	05/12/2023	Interim Director of Information Security
1.3	Reviewed, no substantive changes Corrected some grammatical and formatting issues. Included the IAM standards and procedures as part of the (IA) family instead of standalone.	05/17/2024	Interim Director of Information Security
1.4	Reviewed, made changes in incorporate more clearly the guidance and framework of	5/272/2025	Interim Director of Information Security

	NIST 800-171. Additionally made some update in regards to references to types of SIU staff. Combined Contingency Planning (CP) into the SI family per 800-171 framework. Updated logo in header		