Office of the Chancellor
Pennsylvania State System of Higher Education
Procedures and Standards for University Operations

Procedure/Standard Number 2020-47

State System Information Technology (IT) Security Programs and Assessments

Approved by: _____ Chancellor **Date**: 8-5-2020

History: N/A **Revised:** N/A

Related Policies, Procedures or Standards: N/A

Key Words/Categories: Cybersecurity, Assessment, Gramm-Leach-Bliley Act, CIS Controls, Information Technology Security, IT Risk Management

Additional References: OOC and University Information Technology Acceptable Use Policies, OOC Policy Number 2011-608 *Policy on Data Classification*

I. Introduction

This Procedure and Standard provides guidance on the development and adherence to University Information Security Programs and a common system-wide methodology for annual information technology security self-assessments. The methodology will ensure acceptable self-assessments are conducted in a meaningful and recurring timeframe and covers the requirements set forth in applicable federal and state regulations. Compliance with this Procedure and Standard will ensure consistent protocols and IT risk management practices are in place for data and IT resources.

This document describes the elements pursuant to which the State System intends to:

1. Ensure proper internal procedures are in place for the security, confidentiality, integrity, and availability of IT resources
2. Proactively protect against any anticipated threats or hazards to IT resources or the unauthorized access to or use of IT resources
3. Identify opportunities to strengthen the cybersecurity posture of the State System through collaboration and strategic investments

This Procedure and Standard is to be used in conjunction with any institutional policies and procedures that may be required pursuant to federal and state laws and regulations, including, without limitation, Gramm-Leach-Bailey Act (GLBA), Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry (PCI).

II. Definitions

1. **CIS Controls:** Security actions used to assess and improve an organization's information security architecture.

2. **Defense-in-Depth Security Architecture:** A set of security controls and best practices that provides a multi-layered security posture for information technology resources such that if one layer fails, additional layers are in place to mitigate threats.

3. **Implementation Group:** Self-assessed categories for organizations based on relevant cybersecurity attributes and is used for prioritize CIS control utilization.

4. **Information Technology Security**: Activities used to prevent, detect, and mitigate risks to information technology resources.

5. **Information Technology Security Assessment**: A systematic process of reviewing and documenting an institution's information security risks in order to determine compliance, identify opportunities of improvement, detect areas of risk, and establish safeguards, related to information security.

6. **Information Technology (IT) Resources:** Assets including, but not limited to, State System/university owned or operated hardware, software, telecommunications, and other technology assets issued by the State System or a university.

7. **IT Risk Management:** A process of identifying risk to an organization's IT resources and taking the appropriate steps to reduce the risk to an acceptable level.

8. **Safeguard:** A set of activities or actions to prevent or mitigate a risk to IT resources.

III. Scope

This Procedure and Standard applies to all State System universities and the Office of the Chancellor.

IV. Procedure/Standard

1. **University Information Technology Security Program**
   A recognized information technology (IT) security program should be designed and approved by a formal university governance committee for each university. To ensure the objectives of the IT security program is aligned with the university's and the State System's information technology security strategy, the IT security program should be reviewed on an annual basis by the university governance committee.

   The IT security program should prioritize the development, management, and continuous improvement of information technology security processes and procedures that focus on the protections of student data and IT resources managing the student data.

Each university IT security program is to be documented and governed through a formal Information Technology Security University Policy that should contain, at a minimum, guidance for the following:

- Description of the university's information security program including scope and objectives
- Security roles & responsibilities
- Annual security awareness training
- Annual cyber risk assessments
- Data classification and protections
- Access control

Universities are to develop or update a position description that identifies a coordinator of the university IT security program that will be responsible for fulfilling the requirements set in this Procedure and Standard and to coordinate and assist the university's IT security program. The position description can be for a new position or as an amendment to an existing position.

Following the guidance detailed in this section and utilizing the recommendations detailed in Appendix A *Recommended State System Information Technology (IT) Security Program Foundational Controls* and Appendix B *Recommended State System Information Technology (IT) Security Program Position Duties [Template]* provides elements to be included in an IT security srogram framework for universities.

2. **State System Defense-in-Depth Security Architecture Principles**
   A defense-in-depth security architecture establishes five tenets that each IT Security Program can use as guiding principles for their program.

   i. Offense informs defense - Use of shared knowledge to learn and adapt.
   ii. Prioritization - Focus on controls that mitigate immediate risks.
   iii. Measurements and metrics – Established standardized performance metrics for reporting across the State System.
   iv. Continuous diagnostics and mitigation – Established processes and procedures for continued monitoring and improvement of the security architecture.
   v. Automation – Automate reliable and scalable security metrics and data for real-time information.

3. **Information Technology Security Framework and Assessment**
   The Center for Internet Security (CIS) provides security standards and best practices through the utilization of CIS controls and benchmarks that are used to measure gaps and capabilities of information technology security programs.

   The State System will utilize the CIS controls as the baseline information security standard for protecting IT resources. Information technology security assessments, to be performed on an annual basis, and are to be conducted utilizing the CIS tool 'CIS-CSAT'. Annual assessment timeframes will be communicated by the Office of the Chancellor to the universities. Refer to Appendix C *Recommended Timeline* for general timeline information.

The State System is to follow CIS assessment guidelines that focus on ensuring the CIS controls are properly in place to mitigate information technology security threats and strengthen the State System's defense-in-depth security architecture through each university's IT security program.

Universities may conduct additional information technology security assessments that supplement the self-assessment or are required due to regulations, audit findings, or other requirements.

The State System Universities are encouraged to leverage resources provided through the Multi-State Information Sharing and Analysis Center (MS-ISAC) and universities are recommended to have an active membership to the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) to access additional information security resources.

4. **Foundational Controls and Implementation Group Baseline**
   CIS controls are categorized through Implementation Groups (IG) developed by CIS. Each university is to evaluate the three IGs and based on the university's resources, are recommended to develop a security plan to meet the appropriate IG that is achievable with available resources within their IT security program.

   University IT security programs are recommended to prioritize a number of State System Information Technology Security Program Foundational Controls. Refer to the Appendix A *Recommended State System Information Technology (IT) Security Program Foundational Controls* for further guidance.

   Concurrently to working towards and maintaining the State System Information Technology Security Program Foundational Controls, if proper resources are available, university IT security programs are recommended to prioritize achieving the "Foundational" Implementation Group ("IG2") maturity as the baseline and to focus defense-in-depth security architecture programs towards developing and managing all CIS controls and sub-controls within the IG2.

5. **Information Technology Risk Management Strategy**
   State System universities, in collaboration with their IT security program, are recommended to develop a comprehensive information technology (IT) risk management strategy with a focus on 1) framing risks; 2) assessing risks; 3) responding to risks; and 4) monitoring risks that are identified in information security assessments and ongoing defense-in-depth security architecture programs.

   Universities are recommended to use the following risk control strategies to guide and reduce identified risks.

   - Avoidance: To eliminate the conditions that allow the risk to be present at all, most frequently by dropping the project or the task.
   - Acceptance: To acknowledge the risk's existence, but to take no preemptive action to resolve it, except for the possible development of contingency plans should the risk event come to pass.
   - Mitigation: To minimize the probability of a risk's occurrence or the impact of the risk should it occur.

- Deflection: To transfer the risk (in whole or part) to another organization, individual, or entity.

6. **Risk Reporting and Governance**
   It is recommended each State System university, in collaboration with their IT security program, maintain an internal IT risk management governance review process which defines roles and responsibilities, including accountability for each risk identified and procedures for determining the appropriate risk mitigation strategy in subsection 5 (Information Technology Risk Management Strategy) or safeguard. It is recommended that stakeholders from diverse program areas (IT, legal, academics, administration, etc.) be involved in the governance review process.

   A communications plan should be adopted as part of the governance review process that will ensure all appropriate stakeholders are notified of risks and the risk control strategies that may impact their program area.

V. Roles and Responsibilities

To ensure consistent management of the annual information technology security assessments, consideration should be given to identify a single point of contact at each State System university to facilitate the assessment procedures. The following roles and responsibilities are provided as recommended best practices; each university may substitute the following based on business requirements, capabilities, and other factors.

1. **University Chief Information Technology Officers (CITOs) / IT Shared Services Director or designee**

   - Establish and maintain an IT security program
   - Facilitate the annual information technology security self-assessment
   - Ensure corrective action plans and safeguards are established to address information security gaps identified in annual assessment
   - Report assessment findings to appropriate stakeholders

2. **State System Chief Information Officer (CIO) or designee**

   - Establish an annual cycle for completion of the information security self-assessments for universities and OOC
   - Ensure immediate corrective action plans and safeguards are established to address information technology security gaps identified in annual assessment
   - Report assessment findings to appropriate stakeholders
   - Compile the State System annual information technology security self-assessments to identify common approaches and strategies for future information security collaboration and shared investments

VI. Resources

1. Consumer Financial Protection Bureau, Gramm-Leach-Bliley Act: https://www.consumerfinance.gov/policy-compliance/guidance/gramm-leach-bliley-act/
2. Center for Internet Security https://www.cisecurity.org/

3. CIS Controls/NIST Cybersecurity Framework Mapping https://www.cisecurity.org/white-papers/cis-controls-v7-1-mapping-to-nist-csf/
4. Multi-State Information Sharing & Analysis Center (MS-ISAC): https://www.cisecurity.org/ms-isac/
5. Research & Education Networks Information Sharing & Analysis Center (REN-ISAC): https://www.ren-isac.net/
6. Federal Student Aid Cybersecurity: https://ifap.ed.gov/fsa-cybersecurity-compliance

VII. **Implementation**

This Procedure and Standard is effective immediately.

Appendix A

Recommended State System Information Technology (IT) Security Program Foundational Controls

The following CIS Controls are recommended to be in place for all universities within the State System as a result of the *GLBA Requirements for Higher Education Institutions 2019 – 001* audit finding. Once mitigated, universities should expand to cover all twenty (20) CIS controls.

Integrating these controls will provide an elementary defense-in-depth security architecture, enabling the State System to proactively protect State System IT resources. Each university is encouraged to evaluate their security architecture and IT security program for areas of improvement with a focus on integrating and enhancing the following controls.

CIS Control	Control Name	Mapped to 2019-01 Audit Finding
CIS Control 1	Inventory and Control of Hardware Assets	16 CFR 314.4 b. Info systems, including network and software design, info processing, storage, transmission, disposal.
CIS Control 2	Inventory and Control of Software Assets	16 CFR 314.4 b. Info systems, including network and software design, info processing, storage, transmission, disposal.
CIS Control 3	Continuous Vulnerability Management	16 CFR 314.4 c. Detecting, preventing, and responding to attacks, intrusions, or other system failures.
CIS Control 4	Controlled Use of Administrative Privileges	16 CFR 314.4 c. Detecting, preventing, and responding to attacks, intrusions, or other system failures.
CIS Control 5	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	16 CFR 314.4 b. Info systems, including network and software design, info processing, storage, transmission, disposal.
CIS Control 8	Malware Defenses	16 CFR 314.4 c. Detecting, preventing, and responding to attacks, intrusions, or other system failures.
CIS Control 10	Data Recovery Capabilities	16 CFR 314.4 b. Info systems, including network and software design, info processing, storage, transmission, disposal. c. Detecting, preventing, and responding to attacks, intrusions, or other system failures.
CIS Control 13	Data Protection	16 CFR 314.4 b. Info systems, including network and software design, info processing, storage, transmission, disposal. c. Detecting, preventing, and responding to attacks, intrusions, or other system failures.
CIS Control 17	Implement a Security Awareness and Training Program	16 CFR 314.4 a. Employee training and management.

Appendix B

Recommended State System Information Technology (IT) Security Program Position Duties [Template]

It is recommended State System universities to have an established information technology (IT) security program and appropriate human resources to complete the requirements and responsibilities set in this Procedure and Standard. The Office of the Chancellor provides the following position duties as guidance for university human resources department. Each university should evaluate these recommendations and make the appropriate determination when developing internal position descriptions in consultation with university and OOC stakeholders.

- Responsible for creating, defining, and managing the information technology (IT) security program based upon industry established best practices at their respective university
- Establish and manage a formal IT Risk Management Program based upon the CIS Framework
- Responsible for monitoring and complying with the information technology security program area portion of compliance and regulations that are applicable to the university such as PCI, FERPA, GLBA, HIPAA, GDPR, and others that may apply
- Responsible for managing a Security Awareness Training Program to educate end-users of common threats
- Review and approve security policies, controls, and cyber incident response planning and communicate all to university personnel
- Schedule periodic security audits
- Review investigations after breaches or incidents, including impact analysis and recommendations for avoiding similar vulnerabilities
- Brief the CITO and executive team on status and risks, including taking the role of champion for the overall strategy and necessary budget
- Creating and implementing a strategy for the deployment of information security technologies

Appendix C

Annual Timeline

Activity	Timeline	Responsible Party
Assessment & Remediation Planning Process	January – March	Universities / IT Shared Services
Systemwide Summary & Recommendations	March – April	OOC
Discuss Priorities for Next Cycle	April – May	Universities / IT Shared Services
Annual Assessment & Remediation Checkpoints	June	Universities / IT Shared Services
Complete Self-Assessment & Remediation	June – November	Universities / IT Shared Services
Assessment & Remediation Reports Complete	December	Universities / IT Shared Services