

Policy Number/Title:	7.1.01 Information Security - Master Policy
Effective Since:	12/16/2020
Last Revision Approved:	04/29/2020
Responsible Office:	Computing and Information Technology.

1. Scope:

This policy applies to all Winthrop University faculty, staff, students, and user of information assets or systems.

2. Definitions:

Business Unit: A logical element or segment of a company (such as accounting, production, marketing) representing a specific business function, and a definite place on the organizational chart, under the domain of a manager. Also called department, division, or a functional area.

Guidance: Guidance refers to best practices and industry standards that have been used as a guide to develop the security policies and the policy supplements.

Information security liaison: Official responsible for carrying out the “Chief Information Officer” responsibilities within the agency under the Federal Information Security Management Act (FISMA) and serving as the primary liaison between the DIS office of the Chief Information Security Officer and the agency’s authorizing officials, information system owners, and information system security officers.

Information Security Plan: the collection of procedures and other guidance developed by state government agencies to implement the SC DIS Information Security Program within the agency

Risk posture: Risk posture identifies the specific threats that the agency faces and quantifies the risks associated with each of those threat events materializing.

SC DIS–South Carolina Division of Information Security

SC DIS Information Security Program–the collection of policies, procedures, and other guidance published on the SC DIS website (dis.sc.gov).



Control, Information Security: refers to any process or technology intended to reduce a security risk.

Policy exemptions: Scenarios which require exemption from the existing provisions of the Security policy are called policy exemptions.

3. Policy:

Information Security Program Planning

3.1 Information Security Plan

3.1.1 Winthrop University shall develop and communicate an information security plan that underlines security requirements, the security management controls, and common controls in place for meeting those requirements.

3.1.2 Winthrop University's information security plan shall identify and assign security program roles, responsibilities and management commitment, and ensure coordination among the University's business units, as well as compliance with the information security plan.

3.1.3 Winthrop University shall ensure coordination among the University's business units responsible for the different aspects of information security (i.e., technical, physical, personnel, etc.)

3.1.4 The Winthrop University Board of Trustees shall authorize the development of an information security plan.

3.1.5 The information security plan shall be approved by executive leadership.

3.1.6 Winthrop University shall review the information security plan on at least an annual basis.

3.1.7 Winthrop University shall update the information security plan to address changes and problems identified during plan implementation or security control assessments.

3.1.8 Winthrop University shall protect the information security plan from unauthorized disclosure and modification.

3.2 Information Security Resources



3.2.1 Winthrop University shall consider resources needed to implement and maintain the information security plan in capital planning and investment requests.

3.3 Plan of Action and Milestones (POAM) Process

3.3.1 Winthrop University shall implement a process for ensuring that plans of action and milestones for the information security program and associated information systems are developed and maintained.

3.3.2 Winthrop University shall review plans of action and milestones for consistency with the University's risk management strategy and priorities for risk response actions.

3.4 Information Security Measures of Performance

3.4.1 Winthrop University shall develop, monitor, and report on the results of information security measures of performance, as directed or guided by the SC Division of Information Security and SC Enterprise Privacy Office.

Information Security Organization (Roles and Responsibilities)

3.5 Information Security Authority

3.5.1 Winthrop University's executive leadership shall ensure that the University's senior leadership group are given the necessary authority to secure the operations and assets under their control.

3.5.2 Winthrop University shall appoint an information security liaison with the mission and resources to: coordinate, develop, implement, and maintain an information security plan.

3.6. Information Security Workforce

3.6.1 Winthrop University shall establish an information security workforce and professional development program appropriately sized to the University's information security needs.

3.7 Role-based Security Training

3.7.1 Winthrop University shall provide role-based information security training to personnel with assigned information security roles and responsibilities.

Policy Management (Plan of Action)

3.7 Procedure Development



3.7.1 Winthrop University shall adopt a risk-based approach to identify State and Winthrop University-specific information security objectives, and shall develop information security procedures in alignment with the identified security objectives.

3.7.2 Winthrop University shall allocate the appropriate subject matter experts to the development of State and Winthrop University-specific information security procedures.

3.7.3 Winthrop University shall approach independent external (third party) specialists to assist in the development of information security policies in cases where it is established that the required skills do not exist within the University and are not available within any other state government agency.

3.7.4 Winthrop University shall work in collaboration with other states, Federal government, and external special interest groups in cases where procedures directly or indirectly affect interfacing activities with them.

3.7.5 Information security procedures that are developed at Winthrop University shall contain the following information, as appropriate:

- (a) Revision history
- (b) Introduction
- (c) Preface
- (d) Ownership, roles, and responsibilities
- (e) Purpose
- (f) Policy statements
- (g) Policy supplement
- (h) Guidance
- (i) Definitions

3.7.6 Scenarios which cannot be effectively addressed within the constraints of Winthrop University's information security procedures, should be identified as exceptions:

- (a) Exceptions shall be evaluated in the context of potential risk to Winthrop University as a whole;
- (b) Exceptions that create significant risks without adequate compensating controls shall not be approved; and
- (c) Exceptions shall be consistently evaluated in accordance with the University's risk acceptance practice.



3.7.7 The University shall review each draft procedure with stakeholders who shall be impacted by the procedure, to ensure that the procedure is enforceable and effective.

3.7.8 The University shall identify gaps within the procedures that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps.

3.7.9 The University shall develop and implement a communication plan to disseminate new procedures or changes to existing procedures.

3.7.10 The University shall review procedures on an annual basis to ensure that procedures are up-to-date and aligned with the State's risk posture.

3.8 Procedure Review and Approval

3.8.1 A procedure governance committee shall be established for the purpose of review and approval of procedures.

3.8.2 Procedure exemptions shall be explicitly approved by the procedure governing committee.

3.8.3 Procedure approval history shall be documented in detail.

3.9 Procedure Implementation

3.9.1 The University shall implement mechanisms to help ensure that information security procedures will be available to the University's personnel on a continuous basis and whenever required.

3.9.2 The University shall require employees to review and acknowledge understanding of information security procedures prior to allowing access to sensitive data or information systems.

3.10 Controls Deployment

3.10.1 The University shall adopt a risk-based approach to prioritize deployment of controls.

3.10.2 The University shall allocate the appropriate subject matter experts to the deployment of State and University-specific information security controls.

3.10.3 The University shall approach independent external (third party) specialists to assist



in the deployment of information security controls in cases where it is established that the required skills do not exist within the University and are not available within any other state government agency.

3.10.4 Controls which cannot be deployed due to the University's resource or other constraints must be reported to the office of the State Chief Information Security Officer.

3.10.5 The University shall review each control with stakeholders who shall be impacted, to ensure that the control is enforceable and effective.

3.10.6 The University shall identify gaps within the controls that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps.

3.10.7 The University shall develop and implement a communication plan to disseminate new controls or changes to existing controls.

3.10.8 The University shall review controls on an annual basis to ensure that they are up-to-date and aligned with the State's risk posture.

4. Procedures:

This section was intentionally left blank.

5. Resources:

NIST SP 800-53 Revision 4: PM 2 Senior Information Security Officer

NIST SP 800-53 Revision 4: PM 13 Information Security Workforce

NIST SP 800-53 Revision 4: AT 3 Role-based Security Training

NIST SP 800-100: 2.2.3.1 Agency Head

NIST SP 800-53 Revision 4: PM 1 Information Security Program Plan

NIST SP 800-53 Revision 4: PM 3 Information Security Resources

NIST SP 800-53 Revision 4: PM 4 Plan of Action and Milestones Process

NIST SP 800-53 Revision 4: PM 6 Measures of Performance



6. History of Revisions:

12/16/2020	Minor Revisions
04/29/2020	Policy first established

7. Approvals:

Responsible Officer Signature/Date:

Vice President/Senior Administrator Signature/Date:

President Signature/Date: