AURORA
UNIVERSITY

POLICY: INFORMATION SECURITY

DOCUMENT #:	ITS-POL-0001
EFFECTIVE:	05-26-2022
OWNER:	ITS

CONTENTS

1.0 INTRODUCTION

The purpose of this policy is to assist the institution in its efforts to fulfill its fiduciary responsibilities relating to the protection of information assets and comply with regulatory and contractual requirements involving information security and privacy. This policy framework consists of eighteen (18) separate policy statements, with supporting Standards documents, based on guidance provided by the National Institute of Standards and Technology (NIST) Special Publication 800-171.

Although no set of policies can address every possible scenario, this framework, taken as a whole, provides a comprehensive governance structure that addresses key controls in all known areas needed to provide for the confidentiality, integrity and availability of the institution's information assets. This framework also provides administrators guidance necessary for making prioritized decisions, as well as justification for implementing organizational change.

2.0 PURPOSE

The purpose of this Information Security Policy is to clearly establish Aurora University role in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives enables Aurora University to implement a comprehensive system-wide Information Security Program.

3.0 SCOPE

The scope of this policy includes all information assets governed by the institution. All faculty, staff, student workers and service providers who have access to or utilize assets of the institution, including data at rest, in transit or in process shall be subject to these requirements. This policy applies to:

- All information assets and Information Technology (IT) resources operated by the institution;
- All information assets and IT resources provided by the institution through contracts, subject to the provisions and restrictions of the contracts; and
- All authenticated users of Aurora University information assets and IT resources.

4.0 IMPLEMENTATION

Aurora University needs to protect the availability, integrity and confidentiality of data while providing information resources to fulfill the institution's mission. The Information Security Program must be risk-based and implementation decisions must be made based on addressing the highest risk first.

Aurora University's administration recognizes that fully implementing all controls within the NIST Standards is not possible due to institution limitations and resource constraints. Administration must implement the NIST standards whenever possible, and document exceptions in situations where doing so is not practicable.

5.0 ROLES AND RESPONSIBILITIES

Aurora University has assigned the following roles and responsibilities:

1) Chief Information Officer or designee: The Chief Information Officer or designee is accountable for the implementation of the Information Security Program including:

    a) Security policies, standards, and procedures

    b) Security compliance including managerial, administrative and technical controls

    The Chief Information Officer is to be informed of information security implementations and ongoing development of the Information Security Program design.

2) Information Security Committee: The group is responsible for the design, implementation, operations and compliance functions of the Information Security Program for all Aurora University constituent units. The committee is comprised of Chief Information Officer, Chief Operations Officer, Emergency Preparedness Director and functions as the Information Security Program Office.
3) Information Security Officer (designated as the individual): GreyCastle Security is supportive and performs as the Information Security Officer for Aurora University. GreyCastle alongside Aurora University's Chief Information Officer are responsible for the development, implementation and maintenance of a comprehensive Information Security Program for Aurora University. This includes security policies, standards and procedures which reflect best practices in information security.

6.0 INFORMATION AND SYSTEM CLASSIFICATION

Aurora University must establish and maintain security categories for both information and information systems. For more information, reference the Data Classification Policy.

7.0 PROVISIONS FOR INFORMATION SECURITY STANDARDS

The Aurora University Security Program is framed on National Institute of Standards and Technology (NIST) and controls implemented based on SANS Critical Security Controls priorities. Aurora University must develop appropriate control standards and procedures required to support the institution’s Information Security Policy. This policy is further defined by control standards, procedures, control metrics and control tests to assure functional verification.

The Aurora University Security Program is based on NIST Special Publication 800-171. This publication is structured into 18 control groupings, herein referred to as Information Security Standards. These Standards must meet all statutory and contractual requirements.

7.1 ACCESS CONTROL (AC)

Aurora University must limit information system access 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.

7.2 AWARENESS AND TRAINING (AT)

Aurora University must: (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, directives, policies, standards, instructions, regulations, or procedures related to the security of institution information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

7.3 AUDIT AND ACCOUNTABILITY (AU)

Aurora University must: (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity on protective enclave systems, specific to confidential data and confidential networks, at a minimum; and (ii) ensure that the actions of individual information system users can be uniquely traced for all restricted systems.

7.4 ASSESSMENT AND AUTHORIZATION (CA)

Aurora University must: (i) periodically assess the security controls in institution information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in institution information systems; (iii) authorize the operation of the institution’s information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

7.5 CONFIGURATION MANAGEMENT (CM)

Aurora University must: (i) establish and maintain baseline configurations and inventories of institution information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in institution information systems.

7.6 CONTINGENCY PLANNING (CP)

Aurora University must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for the institution's information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

7.7 IDENTIFICATION AND AUTHENTICATION (IA)

Aurora University must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Aurora University information systems.

7.8 INCIDENT RESPONSE (IR)

Aurora University must: (i) establish an operational incident handling capability for institution information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate institution officials and/or authorities.

7.9 MAINTENANCE (MA)

Aurora University must: (i) perform periodic and timely maintenance on institution information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

7.10 MEDIA PROTECTION (MP)

Aurora University must: (i) protect information system media, both paper and digital; (ii) limit access to information-on-information system media to authorized users; and (iii) encryption, where applicable, (iiii) sanitize or destroy information system media before disposal or release for reuse.

7.11 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

Aurora University must: (i) limit physical access to information systems, equipment and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

7.12 PLANNING (PL)

Aurora University must develop, document, periodically update and implement security plans for institution information systems that describe the security controls in place or planned for the information systems as well as rules of behavior for individuals accessing the information systems.

7.13 PERSONNEL SECURITY (PS)

Aurora University must: (i) ensure that individuals occupying positions of responsibility within the institution are trustworthy and meet established security criteria for those positions; (ii) ensure that institution information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with Aurora University security policies and procedures.

7.14 RISK ASSESSMENT (RA)

Aurora University must periodically assess the risk to institution operations (including mission, functions, image, or reputation), institution assets, and individuals, resulting from the operation of institution information systems and the associated processing, storage or transmission of institution information.

7.15 SYSTEM AND SERVICES ACQUISITION (SA)

Aurora University must: (i) allocate sufficient resources to adequately protect institution information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third- party providers employ adequate security measures, through federal and state law and contract, to protect information, applications and/or services outsourced from the institution.

7.16 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

Aurora University must: (i) monitor, control and protect institution communications (i.e., information transmitted or received by institution information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions; and (ii) employ architectural designs, software development techniques, encryption, and systems engineering principles that promote effective information security within institution information systems.

7.17 SYSTEM AND INFORMATION INTEGRITY (SI)

Aurora University must: (i) identify, report and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within institution information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

7.18 PROGRAM MANAGEMENT (PM)

Aurora University must implement security program management controls to provide a foundation for the institution's Information Security Program.

8.0 ENFORCEMENT

Aurora University may temporarily suspend or block access to any individual or device when it appears necessary to do so in order to protect the integrity, security or functionality of institution and computer resources.

Any personnel found to have violated this procedure may be subject to disciplinary action, up to and including termination of employment or enrollment.

9.0 PRIVACY

Aurora University must make every reasonable effort to respect a user's privacy. However, personnel do not acquire a right of privacy for communications transmitted or stored on institution resources.

Additionally, in response to a judicial order or any other action required by law or permitted by official institution policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the institution, the Chief Information Officer, or an authorized agent, may access, review, monitor and/or disclose computer files associated with an individual's account.

10.0 EXCEPTIONS

Exceptions to the policy may be granted by the Chief Information Officer, or the Chief Operations Officer. To request an exception, submit an Information Security Exception request to the Information Services Department.

11.0 DISCLAIMER

Aurora University disclaims any responsibility for and does not warrant information and materials residing on non-Aurora University systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of Aurora University.

12.0 REFERENCES

- NIST SP 800-171
- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- Illinois State Information Security Breach and Notification Act
- FIPS-199
- PCI DSS 3.1

13.0 RELATED POLICIES

- Aurora University Data Classification Policy
- Data Classification Procedure
- Acceptable Use Policy

14.0 RESPONSIBLE DEPARTMENT

Information Technology Services

15.0 POLICY AUTHORITY

This policy is issued by the Chief Information Officer for Aurora University

16.0 REVISION HISTORY

Version	Date	Author	Revisions

1.0	5-19-2022	GreyCastle Security	Initial Draft
1.1	5-26-2022	Aurora University Team	Approval/Effective

17.0 APPROVALS

Executive	**Chief Information Officer**
Name Jeff King	Name Hurstel Howard
COO	CIO
05/24/2022	5/26/2022
Signature Jeff King	Signature Hurstel Howard