POLICY STATEMENT 120 STANDARD 1
ROLES AND RESPONSIBILITIES

POLICY DIGEST

Monitoring Unit: Office of Information Technology
Initially Issued: October 17, 2022
Last Revised: none

I. PURPOSE

As an institution of higher education, Louisiana State University at Eunice (“University” or “LSU Eunice”) is charged with maintaining systems and data for administrative and academic purposes. These assets are critical to the mission of the University, and the security of these systems and datasets must be managed with a formalized Information Security Program.

The purpose of this standard is to describe the specific roles and responsibilities in the Information Security Program at LSU Eunice.

II. DEFINITIONS

Asset. A resource, process, product, information infrastructure, etc. whose loss or compromise could intangibly affect its integrity, availability, or confidentiality, or it could have a tangible dollar value. The loss or compromise of an asset could also affect an entity’s ability to continue business. Examples of assets including, but are not limited to,equipment, software, algorithms, and data.

Information Security Program. The collection of administrative, physical, and technical safeguards implemented to mitigate the risks to the integrity, availability, and confidentiality of information technology assets.

Responsibility. The job functions and associated activities performed in a particular operation or process as a function of a role.

Role. A defined position assumed by employees at an entity.

Standard. Standards are defined actions and/or rules that provide support and direction for compliance with policies.

III. STANDARDS

Each of the following roles must exist as part of the Information Security Program at LSU Eunice. Each role must be assigned to a specific position held by individuals and have the associated responsibilities, related to Information Security Program, as defined below.

A. University Administration Officials – Administration Officials consist of senior level positions within Business Affairs, Academic Affairs, and the Office of Information Technology along with the University Chancellor. These officials are also referred to as Data Trustees for the purposes of Data Governance. Responsibilities for these roles include:

1. Budget sufficient resources to fund an ongoing Information Security Program that will address risk remediation, implementation of industry standard Information Technology (IT) security best practices and standards, and compliance activities that reduce overall risk to an acceptable level.

2. Enforce policies, procedures, standards, and practices within LSU Eunice.

3. Enforce appropriate corrective and disciplinary actions in the event of noncompliance with all information security policies and standards.

4. Appoint Data Stewards for each subject are domain within LSU Eunice.

B. Department Head of Information Technology – In addition to the responsibilities under the role of University Administration Officials, this role has the following responsibilities:

1. Lead the planning and implementation of strategic and core IT initiatives on LSU Eunice pertaining to information security, finance, human resources, student information, budget and planning, data analytics, and telecommunication services.

2. Direct the development and implementation of IT policies and proceduresfor LSU Eunice.

3. Serve as a resource for communicating information technology policies,procedures, and practices to campus departments and senior LSU Eunice administrators.

4. Designate an individual to serve as the Information Security Officer.

5. Approve LSU Eunice Information Security Program.

C. Information Security Analyst – The Information Security Analyst establishes the overall information security strategy and program to ensure confidentiality, integrity, and availability of information assets at the University. The Information Security Analyst's responsibilities include, but are not limited to:

1. Develop, implement, and administer the Information Security Program which also incorporates information security risk management.

2. Develop and maintain the information security strategy, policies, procedures, and controls to satisfy regulatory requirements, as well as campus policies and contractual agreements.

3. Understand University's strategic plans, vital academic activities, and business functions for the purpose of creating balance between information security and core functions of the University.

4. Maintain current knowledge of applicable regulatory and compliance issues related

to information security and privacy.

5. Develop, manage, and communicate policies to direct security functions around information technology assets including systems under development, networks, applications, and voice and data communications that are consistent with applicable regulatory and compliance requirements.

6. Provide periodic monitoring, reviewing, and updating the Information Security Program to include a full annual program review.

7. Coordinate and approve the use of any external resources involved insecurity testing (i.e., penetration tests, vulnerability scans).

8. Develop and report business-relevant metrics to measure the efficiency and effectiveness of the Information Security Program.

9. Ensure implementation of the data classification schemes defined at the institution.

10. Facilitate appropriate resource allocation and increase the maturity of the security program.

11. Provide subject matter expertise on a broad range of information security standards and best practices.

12. Design security standards for IT initiatives, including the evaluation of enterprise architecture, hardware, software, and technical controls.

13. Coordinate training and oversee the workforce with significant responsibilities for information security.

14. Develop, implement, and ensure compliance with an information security training program for all applicable parties, including employees.

15. Provide oversight of Supplier/Vendor Risk Management activities involving information technology assets.

16. Provide leadership and participate in incident response procedures.

17. Manage all reporting and communications pertaining to information technology incident response (e.g., coordinating communications after suspected breaches of confidential LSU Eunice data).

D. Data Analyst – The Data Analyst is responsible for creative value from the institution's data assets. The Data Analyst is responsible for the following:

   1. Establish and maintain a data governance framework.

   2. Evangelize the culture of use of data-informed decision making.

   3. Promote the use of data as an institutional asset and the ethical use of data.

   4. Mitigate data risk.

5. Align a data strategy to the institutional strategic plan.
6. Align data governance with laws, rules, and regulations.
7. Create data literacy programs.
8. Operationalize data policies, procedures, standards, and practices.

E. Information Security Team – the information security team comprises multiple positions that aim to protect institutional systems, services, and data against unauthorized use, disclosure, modification, damage, or loss. Information SecurityTeam is responsible for:

1. Analyze and investigate reported incidents of technology abuse and security incidents.
2. Monitor the network for security traffic anomalies and implement remediation actions.
3. Actively scan the network to identify vulnerability devices and recommend mitigation/remediation steps.
4. Develop enterprise-level strategies for patching and endpoint security.
5. Utilize security policies, processes, technologies, and awareness to provide a secure IT environment.
6. Conduct security reviews of systems, processes, and data.
7. Advise and provide recommendations to campus entities responsible for compliance with regulatory compliance frameworks.
8. Serve as a point of contact for institutional IT security-related incidents (e.g., data breaches, malicious activity, copyright infringement, etc.).

F. IT Security Analyst – security analysts monitor LSU Eunice IT assets to ensure the safe and secure operation for the network and respond to information security- related incidents and inquiries using established information security tools, processes, and procedures. Security analysts are responsible for:

1. Gathering and analyzing materials about information systems to provide recommendations to security team’s leadership to improve compliance and achieve enhanced posture of data and information systems security.
2. Ensuring security program operations and controls are being consistently assessed and implemented across the University.
3. Assessing requirements for updates to security procedures based on changes in business functions and/or processes, and the emergence of vulnerabilities and threats.
4. Providing guidance to the Departmental Technology Support Professionals regarding the implementation of security controls, resolution of security vulnerabilities, and compliance with information security requirements and controls.

5. Implementing incident response procedures as laid out by the enterprise incident response plan.

G. Data Functional Owner – Data functional owners are organizational representatives who have planning and decision-making responsibilities for data, related to their functional area. They are members of the academic or functional areas of the University (e.g., Registrar, Director, Associate Director, Assistant Director, Associate/Assistant Dean, or equivalent) and are appointed by Data Trustees. The responsibilities for this role include:

1. Oversee data access, data quality, and data integrity.

2. Define user security roles.

3. Coordinate efforts with information security team to Identify, assess, and evaluate risks to the institutional data.

4. Ensure that are data are maintained and used in compliance laws, rules, and regulations.

5. Promote data security awareness to the community.

6. Ensure metadata is created for data related to their functional area.

7. Authorize usage of data.

H. Data Steward – Data stewards are operational managers in a functional area with day-to-day responsibilities for managing business processes and establishing business rules for production transaction systems and associated datasets. A data steward normally reports to a Data Functional Owner. Data steward’s responsibilities include:

1. Accountable for data access, data quality, and data integrity processes.

2. Provide content expertise for the meaning and usage of data (e.g., defining metadata, implementing data quality, defining usage restrictions, etc.).

3. Educate Data Consumers on the data (e.g., compliance issues and best practices in using the data).

4. Provide input on the creation of security roles and role-level security.

5. Review and validate user access, at least annually.

I. Data Custodian – Data Custodians are information technology staff with day-to- day responsibilities for the capture, maintenance, and dissemination of data. In some cases, there may be multiple Data Custodians for a given dataset. The responsibilities include:

1. Ensure the Master Access Plan (MAP) is implemented, and processes are auditable.

2. Provide day-to-day security administration and request fulfillment.

3. Maintain access and audit records.

4. Communicate appropriate use, and consequences of misuse, to users who access the systems.
5. Create, distribute, and follow-up on security violation reports.
6. Monitor the use, security, and transmission of data.
7. Ensure designs for new technologies are consistent with the MAP.
8. Implement and administer controls and procedures to manage application and information security risks in coordination with Data Stewards.
9. Provide reports on actual accesses to be reviewed and validated by DataFunctional Owner(s) at least annually.
10. Coordinate with Information Security Team to respond to any unauthorized use and/or disclosure of data.

J. Data Consumer – a data consumer is any employee, contractor, or third-party agent of the University who is authorized to access LSU Eunice information systems and data to perform their assigned duties or to fulfill their role in the community. The responsibilities include:

1. Adhere to policies, guidelines, and procedures for the protection of data.
2. Report actual or suspected breaches in the confidentiality, integrity, or availability of data to a manager, Information Security Team, and/or Office of Information Technology.
3. Request appropriate access to applications and data through established security processes.
4. Maintain adequate operational controls to ensure data protection.
5. Maintain data confidentiality.
6. Access and use only the data that is authorized by Data Stewards, in the manner authorized.

IV. REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	2/25/2022	Initial Draft	OIT