POLICY STATEMENT 120 STANDARD 2
SEGREGATION OF DUTIES

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.

As a fundamental principle of an Information Security Program, segregation of duties (SOD) is necessary to reduce the opportunity for unauthorized, unethical, illegal, and/or unintentional modification or misuse of information assets and fundamentally reduces the risk of loss of confidentiality, integrity, and availability of data.

The purpose of this standard is to describe the principles of segregation of duties as it relates to 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.

Principle of Least Privilege. The principle requires that a user/system is only granted the least level of access for the least amount of time necessary to perform their job and/or duties.

Segregation of Duties. Segregation of Duties (SOD) is the act of dividing duties and responsibility among various individuals to reduce the possibility of unauthorized, unethical, illegal, or unintentional modification or misuse of information system resources.

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

III. STANDARDS

A. LSU Eunice must segregate duties and areas of responsibility for any process or action that affect assets. The primary categories of activity and responsibility are outlined below.

1. Process/action development/initiation - It is the responsibility of setting a process in motion (e.g., creating/submitting/initiating forms, requests, etc.).

2. Process/action approval – Process approval is the responsibility of allowing an initiated process to continue to completion.

3. Asset processing - Asset processing is the act of fulfilling the business transaction (e.g., granting system/data level access, account reimbursement) as well as creating and maintain the records of the transaction.

4. Process/action review - The review refers to a managerial review function over a particular business process to ensure that proper segregation of duties is occurring.

B. No one person should have responsibility to complete two or more of the activities outlined above. In the event this is not feasible due to business constraints, appropriate segregation of duties mitigating controls must be implemented.

C. Segregation of Duties (SOD) Controls – Control mechanisms that enforce SOD and/or mitigate a lack of SOD can include, but are not limited to:

1. All access to information systems should be limited to prevent any one individual from having sole ownership of a system.

2. A system access request procedure for access to information systems should exist and be maintained.

3. Managers, supervisors, and employees must adhere to the security principle of least privilege and should only request access that is needed to perform their job duties.

4. Managers and supervisors should only approve access that has been deemed necessary for the employee to perform their job duties.

5. Managers and supervisors should review all employees' access levels, at least annually, to ensure each employee has the appropriate level of access.

6. System owners should maintain and update guidelines when approving or denying access to an information system.

7. Supervisors, system owners, and the University reserve the right to deny or remove access to an information asset at any time if the access requested is deemed inappropriate for the user's job role or if the access held is no longer required for the user's job.

8. Employees cannot authorize processes that result in their own personal gain.

9. All approved transactions must adhere to the University policies, existing laws, regulations, and compliance requirements.

10. All individuals responsible for assignment and supervision of employees that carry out fiscal activities should appoint and document authorized approvers of all financial transactions.

11. Audit trails must exist that enable the re-creation of the transaction flow from the point of origination to its current state. Adequate audit trails should provide the initiator of the transaction, data and time of entry, type of entry, data fields, etc.

12. Managerial reviews should be periodically performed through observation and inquire to detect errors and irregularities.

13. Appropriate reports and/or alerts must be established in business-critical systems that highlight potential SOD violations and they must be reviewed and addressed by the relevant functional unit.

IV. REVISION HISTORY

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