POLICY NUMBER 65.3
SECURITY OF COMPUTING RESOURCES

POLICY DIGEST

Monitoring Unit: Information Technology
Initially Issued: November 4, 2020
Last Revised: None

I. PURPOSE

This statement outlines the role and authority of the Office of Information Technology (OIT) in supporting and upholding the security and integrity of the Louisiana State University at Eunice (the University) information technology (IT) environment.

IT has become critical in support of most, if not all of LSU Eunice operations, which has resulted in a very complex and diverse technology environment. Data is continuously being stored, accessed, and manipulated electronically which increases the risk of unauthorized access, disclosure, or modification of data.

Institutions of higher education are subject to various regulatory requirements designed to protect the privacy of education records, financial information, medical records, and other personal information maintained by LSU Eunice relative to its students and employees. Further, LSU Eunice seeks to maintain as confidential certain research data, intellectual property, and other proprietary information owned, licensed, or otherwise maintained or used by the University. Systems that are not properly secured are subject to misuse and/or unauthorized access. Everyone associated with providing and using information technology services should be diligent in their protection of data, use of computing resources, administration and maintenance of systems, response to security threats, and compliance with other University policies and directives. Information related to intrusions, attempted intrusions, unauthorized access, misuse, or other abnormal or questionable incidents should be quickly reported to the Office of Information Technology so the event can be recognized, mitigated, and hopefully avoided elsewhere.

II. GENERAL POLICY

LSU Eunice functional units utilizing computing resources are responsible for managing and maintaining the security of the data, computing resources, and protected information. This requirement is especially important for those computing resources that support or host critical business functions or protected information.

The Office of Information Technology has the authority to:

A. develop and implement policies necessary to minimize the possibility of unauthorized access to protected information and the University's information technology

infrastructure;

B. consult and educate user(s) and functional unit(s) relative to their individual and collective responsibilities to protect data and secure computing resources; and

C. take reasonable actions to mitigate incidents or concerns relating to security of data or computing resources. This includes establishing guidelines, procedures, standards, and security resources, conducting security audits, and providing consulting services to functional unit(s) for all LSU Eunice computer systems or other computing resources.

User(s) within functional unit(s) are required to report any suspected or known security breaches or flaws relating to the security of University computing resources to the Office of Information Technology. OIT will forward information to the Office of Student Affairs if/when the responsible individual is determined to be a past or current student. OIT will assess reported breaches and flaws and provide advice as to an appropriate response. A failure to report suspected or known security breaches or flaws is cause for disciplinary action, including termination of employment. Users should immediately discontinue any use of computing resources or practice that could reasonably lead to a security breach.

The Office of Information Technology has the authority to assume control over the response to any suspected or known security breach or flaw involving LSU Eunice's information technology infrastructure, data, and computing resources regardless of the functional unit involved. Appropriate remedies may be taken to secure computing resources and mitigate any unauthorized use, disclosure, or access to data, including the removal of devices to a secure facility and denying access to computing resources and/or data. OIT may draw upon the experience, expertise, and resources of other University functional units when necessary and as appropriate.

III. PROCEDURES

Intrusion attempts, security breaches, and other security related incidents or flaws perpetrated against or involving computing resources either attached to an LSU Eunice operated network or in a functional unit shall be reported immediately to the Office of Information Technology. This is critical for systems supporting vital functions and/or hosting institutional or protected information. User(s) within functional unit(s) must:

A. Report any security breaches in order to obtain advice and assistance,

B. Report any systematic unsuccessful attempts (i.e. log in attempts, probes, or scans), and

C. When feasible, send detailed reports to OIT as soon as the situation is detected.

Upon receiving a report, IT staff will respond according to OIT standard operating procedures.

In order to protect University data and systems, as well as to protect threatened systems external to the University, OIT may place limits or restrictions on technology services provided on or from any computing resources.

A. Limitations may be implemented using of policies, standards, and/or technical methods, and could include (but may not be limited to) usage eligibility rules, password

requirements, or restricting or blocking certain protocols or use of certain applications known to cause security problems.

B. Restrictions may be deployed permanently based on continuing threat or risk after appropriate consultation with affected constituents, or they may be deployed temporarily, without prior coordination, in response to an immediate and serious threat.

C. Restrictions deployed temporarily will be removed when the risk is mitigated to an acceptable level, or when the effect on University functions caused by the restriction approaches or exceeds risk associated with the threat.

In order to protect University data and systems, as well as to protect threatened systems external to the University, OIT may unilaterally direct that a specific computing resource be isolated from University, campus, or external networks, given:

A. Information reasonably points to the system as having been compromised.

B. There is ongoing activity associated with the system that is causing or will cause damage to other University computing resources or data, or to systems of other internal or external users, or where there is significant risk of such damage occurring.

C. All reasonable attempts have been made to contact the responsible functional unit management, or contact has been made, but the functional unit managers are unable to or choose not to resolve the problem in a reasonable time.

Isolation is removed when the risk is mitigated to an acceptable level, or when loss of access or function caused by the isolation approaches or exceeds risk associated with the threat, as determined between the responsible functional unit and the staff of OIT.

All security breaches, incidents, or concerns should be reported immediately to it@lsue.edu and/or the Office of Information Technology.