POLICY STATEMENT 122 STANDARD 1
SECURITY ASSESSMENT

POLICY DIGEST

Monitoring Unit: Office of Information Technology
Initially Issued: December 12, 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 acceptable use of these systems and data sets must be managed with a formalized Information Security Program.

A major element of protecting the University's Information Technology (IT) assets is managing risks that result from vulnerabilities and threats to the confidentiality, integrity, and availability of data and information systems. One of the primary methods of identifying these risks involves the coordination of performing security assessments of LSU Eunice's technology environment.

The purpose of this standard is to describe security assessment standards as they pertain to LSU Eunice network.

II. DEFINITIONS

Common Vulnerability Scoring System (CVSS). CVSS is the industry standard framework using scores ranging from informational, low, medium, high, and critical severity used to determine vulnerability's criticality in security assessment.

Threat. Threat is a possible danger that might exploit a vulnerability to breach security and therefore cause potential damage or exposure to information systems, data, and/or supporting technology.

Vulnerability. Vulnerability is a weakness which can be exploited by a threat actor, such as a hacker, to perform unauthorized actions on an information system.

III. STANDARDS

A. Assessment Timing

1. System security assessments shall be completed any time there are significant changes to information assets that would affect its risk posture.

2. Assets that store, process, and/or transmit private and/or confidential data, security assessments shall be conducted as required by any applicable federal or state laws, regulations, and/or compliance requirements.

3. System security assessments shall be performed on any new system prior to it being exposed through LSU Eunice network firewall.

4. Internal vulnerability scans must be performed by LSU Eunice Office of Information Technology (OIT) on a weekly basis, on any system that has access to non-LSU Eunice network (i.e., external/internet access). Systems without internet access must be scanned on a regular basis, as applicable.

5. Internal security assessments that simulate an event involving the user community (e.g., tabletop exercises, self-phishing exercises, etc.) shall be performed by OIT at least twice a year.

6. OIT will engage with qualified third parties in external security assessments for the University infrastructure at least once every two years, or for specific systems, as needed.

7. All efforts must be made to ensure that security assessments (internal or external) shall not be scheduled to coincide with any critical University business processes.

B. Assessment Entity

1. Internal security assessments can be performed on the University systems by any of the following entities:

   a. OIT

   b. LSU Internal Audit

2. External security assessments can be performed by any qualified third-party entity with the approval from the IT Security Administrator and in coordination with the Office of Information Technology.

C. Assessment Scope

1. Security assessments (internal or external) shall have documented assessment scope which must include, at minimum:

   a. Systems involved

   b. Assessment technique and tools used

   c. Expected assessment duration

   d. Conditions governing the assessment

D. Assessment Approvals

1. Any security assessment (internal or external) performed at LSU Eunice must have approval from the IT Security Administrator. University Administration Officials may also be involved in the approval process or will be informed of the assessment based on the assessment scope.

E. Assessment Tools and Technologies

1. Security assessments (internal or external) shall not employ any tools or technology that could adversely impact a University system and/or application. This includes, but not limited to,

   a. Revealing confidential information through public channels in plain text.

   b. Stopping services and/or applications on systems

   c. Disabling security software

2. Assessment Reporting and Retention

   a. Remediation and mitigation of discovered vulnerabilities shall be prioritized based on the CVSS vulnerability scores.

   b. Reports of external assessment or specific section of the reports of external assessment must be shared with relevant departments/units of campus as well as appropriate University Administration Official.

   c. All assessment reports must be retained for a period of three (3) years.

IV. REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	04/20/2022	Initial Draft	OIT