Vulnerability Management (LP7.7)

LANDER UNIVERSITY POLICY

2/23/2026

1 Purpose

Vulnerability management is an essential component of information security programs and critical for Lander University to address responsibly in compliance with federal and state laws and policies. The purpose of this policy is to establish a structured, repeatable, and measurable vulnerability management program that enables timely identification, remediation, and reporting of vulnerabilities in university information systems and infrastructure. This process supports the confidentiality, integrity, and availability of university data, and aligns with recognized best practices and applicable state regulatory expectations for system and information integrity.

2 Scope

This policy applies to all information systems and networked devices owned, managed, or operated by the University and its departments, including but not limited to servers, workstations, network appliances, cloud services, and virtual systems. The policy also applies to all faculty, staff, students, affiliates, prospective students, contractors, sub-contractors, and others who are authorized to interact with the University systems and processes.

3 Key Principles

3.1 Vulnerability Assessment & Scanning

3.1.1 The University will perform regular vulnerability scans of information systems and network assets using automated tools approved by ITS.

3.1.2 Scans will be scheduled at least monthly for critical systems and quarterly for all other assets, with additional scans following significant configuration changes, software releases, or incident response activities.

3.1.3 The University will analyze vulnerability scan reports and results from security control assessments and remediate identified vulnerabilities in accordance with IT risk assessments and severity.

3.1.4 Only privileged and authorized individuals have privileged access to vulnerability scanning tools and vulnerability reports. Centrally managed vulnerability assessment solutions will be utilized; use of any other network-based tools to scan or verify vulnerabilities must be approved, in writing, by the CIO.

3.2 Patch Management & Flaw Remediation

3.2.1 Applicable security patches from vendors must be reviewed, tested, and deployed according to severity and risk exposure (e.g., critical and high 15 days or less).

3.2.2 The University will establish a formal process to test and patch software and firmware updates related to flaw remediation for effectiveness and identification of potential impact prior to implementation.

3.2.3 Systems will be evaluated to ensure patches or mitigations do not negatively impact system integrity or availability.

3.2.4 The University will install latest stable versions of applicable security software and firmware updates.

3.2.5 The University will conduct external penetration testing exercises on an annual basis by an independent third-party penetration team to identify, report, and correct information system flaws.

4 Information System Monitoring

4.1 The University will monitor network assets and key information systems to detect attacks and indicators of potential attacks as well as unauthorized local, network, and remote connections.

4.2 The University will heighten the level of information system monitoring activity whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.

5 Roles and Responsibilities

5.1 Information Technology Services (ITS)

The development, implementation and execution of the vulnerability management process is the responsibility of ITS-Information Security in collaboration with network and assigned IT staff, plus other impacted units as directed by the CIO.

5.2 System/Service Owners

5.2.1 Ensure that vulnerabilities identified in systems under their control are assessed and remediated within established timelines.

5.2.2 Provide justification and mitigation strategy to ITS where remediation cannot meet target timelines.

5.2.3 Account for risk and operational needs in remediation decisions.

5.3 Security Operations & Compliance

5.3.1 Review vulnerability metrics and remediation status regularly.

5.3.2 Coordinate technical and procedural updates to this policy as required.

6 Enforcement

6.1 Non-compliance with this policy may result in restrictions on system access, changes in role responsibilities, and in severe or repeated cases may trigger disciplinary action in accordance with university personnel and student governance procedures.

7 Review Cycle

7.1 This policy will be reviewed at least annually or when significant changes occur in threat landscape, technology use, or applicable regulation. Internal and external audit findings shall be considered in the review process.

8 Policy Revision History

- First draft of policy submitted by the Chief Information and Technology Officer on 2/23/2026.
- Policy prepared for review and provisional publishing approval by the Policy Coordinator on 2/23/2026.
- Prepared for Board of Trustees Policy Committee: Pending.
- Reviewed by Board of Trustees Policy Committee: Pending.
- Lander University Board of Trustees review: Pending.