Vulnerability Management Standard Operating Procedure (SOP)

Executive & Audit-Ready Operational Standard

Organization: Sundance Networks

Effective Date: 2025

Approved By: Executive Management

This document defines the authoritative vulnerability management process used by Sundance Networks to identify, assess, remediate, govern, and evidence security vulnerabilities across managed environments.

Table of Contents

1. Purpose

This SOP establishes a formal, repeatable vulnerability management process to reduce risk, support regulatory compliance, and demonstrate due diligence.

2. Scope

This procedure applies to all systems, applications, infrastructure, cloud services, and third-party components managed by the organization.

3. Governance & Accountability

Information Security owns the program. IT Operations executes remediation. Executive Management approves risk acceptance.

4. Asset Coverage

All managed assets must be inventoried, assigned ownership, and classified by business criticality.

5. Vulnerability Identification

Identification occurs via scanning tools, patch systems, advisories, audits, penetration tests, and incident response.

6. Risk Assessment & Prioritization

Vulnerabilities are prioritized based on severity, exploitability, exposure, and business impact.

7. Remediation Standards

Remediation includes patching, upgrading, hardening, service removal, or replacement under change management.

8. Remediation Timelines

Critical: 7 days; High: 30 days; Medium: 60 days; Low: 90 days. Exceptions require approval.

9. Zero-Day & Emergency Vulnerabilities

Actively exploited vulnerabilities trigger immediate mitigation and accelerated remediation.

10. Outdated or Unsupported Software

Business-required outdated software requires documented justification, compensating controls, and a replacement timeline.

11. Compensating Controls

Controls include segmentation, restricted access, monitoring, MFA, and backup validation.

12. Risk Acceptance & Exceptions

All exceptions require executive approval, expiration dates, and periodic review.

13. Validation & Verification

Remediation is validated through rescanning or configuration review prior to closure.

14. Documentation & Evidence

All records and evidence are retained per record retention requirements.

15. Metrics & Continuous Improvement

Metrics such as SLA adherence and recurring findings are reviewed regularly.

16. Audit & Compliance Alignment

Aligned to SOC 2 (CC3, CC7) and ISO/IEC 27001 technical vulnerability management controls.

17. Enforcement

Non-compliance is escalated to management for corrective action.

Approval & Adoption

This SOP is formally approved and adopted as the official vulnerability management procedure of Sundance Networks.

Name	Title	Signature	Date