VULNERABILITY MANAGEMENT POLICY

PURPOSE

In accordance with industry best practices and applicable compliance regulations, the provider has implemented a range of Information Security policies and procedures to protect the confidentiality, integrity, and availability (CIA) of critical client data, computing resources, and business interests. This Vulnerability Management Policy defines the process for identifying, assessing, prioritizing, and remediating security vulnerabilities across the provider's systems and infrastructure.

POLICY STATEMENT

The provider IT department must establish and maintain a vulnerability management program that ensures:

- Regular identification of security vulnerabilities
- Assessment of the severity and potential impact of identified vulnerabilities
- Prioritization of remediation activities based on risk
- Timely remediation of vulnerabilities
- Verification of successful remediation
- Reporting of vulnerability status to management

---

1. VULNERABILITY IDENTIFICATION

The provider IT department must use industry-standard tools and methods to identify vulnerabilities, including:

- Automated vulnerability scanning tools
- Monitoring of vendor security advisories
- Review of threat intelligence feeds
- Participation in relevant security communities

Systems subject to scanning include:

- Servers and cloud infrastructure supporting the FDD platform
- Workstations and administrative systems
- Network devices
- The data acquisition device and any other integrated hardware
- Applications and APIs

2. VULNERABILITY ASSESSMENT AND PRIORITIZATION

Identified vulnerabilities must be evaluated to determine:

- Severity (e.g., using CVSS scoring or vendor ratings)
- Impact on confidentiality, integrity, and availability
- Exposure to external or internal networks
- Presence of known exploits
- Operational dependencies

Based on this assessment, vulnerabilities must be prioritized for remediation as follows:

- **Critical:** Immediate remediation required
- **High:** Remediation as soon as practical
- **Medium:** Remediation on next scheduled maintenance cycle
- **Low:** Address as part of long-term improvements

3. REMEDIATION REQUIREMENTS

The provider IT department must remediate vulnerabilities by:

- Applying patches or updates
- Reconfiguring systems or network settings
- Disabling vulnerable services
- Implementing compensating controls if remediation is not immediately possible

Systems with **critical** vulnerabilities must be addressed as a top priority.

If a vulnerability cannot be remediated promptly:

- A documented risk acceptance or mitigation plan must be approved by management
- Compensating controls must be implemented to reduce risk

4. VERIFICATION

After remediation, the provider IT department must:

- Re-scan systems to verify the vulnerability has been resolved
- Confirm no new issues were introduced
- Document remediation results

Verification steps must be retained for audit purposes.

5. REPORTING

The provider IT department must maintain records of:

- Identified vulnerabilities
- Assessment and prioritization decisions
- Remediation activities
- Verification results

Management must receive periodic reports summarizing vulnerability status, outstanding issues, and remediation timelines.

6. RESPONSIBILITIES

Provider IT Department

- Conducts vulnerability scanning
- Assesses and prioritizes vulnerabilities
- Performs and verifies remediation
- Communicates risks to management
- Maintains documentation

Management

- Reviews and approves risk acceptance decisions
- Allocates resources to support remediation
- Ensures compliance with policy requirements

All Employees

- Must not bypass or disable security controls
- Must report suspicious activity or potential vulnerabilities
- Must support remediation efforts where applicable