

Vulnerability Management Policy

IronHub Inc

August 2026

Contents

1 Purpose and Scope	2
2 Background	2
3 Policy	2
3.1 Vulnerability Scanning	2
3.2 Penetration Testing	2
3.3 Severity Classification and Remediation SLAs	3
3.4 Patch Management	3
3.5 Vulnerability Tracking and Reporting	4
3.6 Configuration and Change Monitoring	4
4 Enforcement	4

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC7.1, CC7.2

Table 2: Document history

Date	Comment
Apr 21 2026	Initial document

1 Purpose and Scope

- a. The purpose of this policy is to establish a systematic approach to identifying, assessing, prioritizing, and remediating security vulnerabilities in IronHub's systems, applications, and infrastructure.
- b. This policy applies to all production systems, applications, cloud infrastructure, network devices, and endpoints within IronHub's information security program.
- c. This policy applies to all employees, contractors, and vendors responsible for the administration or security of IronHub's systems.

2 Background

- a. Unmanaged vulnerabilities represent one of the most common vectors for security incidents. A structured vulnerability management program reduces the attack surface and ensures that known weaknesses are addressed before they can be exploited.

3 Policy

3.1 Vulnerability Scanning

- a. All production systems and infrastructure must be scanned for vulnerabilities on a regular basis:
 - i. **External-facing systems** must be scanned at least **monthly** using automated vulnerability scanning tools.
 - ii. **Internal systems and infrastructure** must be scanned at least **quarterly**.
 - iii. **Critical systems** (those hosting sensitive or personal data, or classified as High availability) must be scanned at least **monthly** regardless of exposure type.
 - iv. Scans must be performed by or under the supervision of the Information Security Manager (ISM) or a designated security engineer.
- b. Vulnerability scan results must be reviewed by the ISM within 5 business days of scan completion.

3.2 Penetration Testing

- a. IronHub must conduct external penetration testing of its production environment at least **annually**, performed by a qualified third-party security firm or internal security team.

- b. Penetration test reports and findings must be reviewed by the ISM and Leadership Team. Findings must be tracked to remediation.
- c. Penetration testing must also be conducted before major product releases or significant infrastructure changes.

3.3 Severity Classification and Remediation SLAs

- a. Identified vulnerabilities must be classified using the CVSS (Common Vulnerability Scoring System) or an equivalent industry-standard framework:

CVSS	Severity	Remediation SLA
9.0–10.0	Critical	7 days
7.0–8.9	High	30 days
4.0–6.9	Medium	90 days
0.1–3.9	Low	180 days or next planned maintenance window

- a. Remediation SLAs begin from the date the vulnerability is confirmed and assigned to an owner.
- b. Vulnerabilities that cannot be remediated within the defined SLA must be escalated to the ISM and documented with:
 - i. Business justification for the delay.
 - ii. Compensating controls implemented to reduce risk.
 - iii. A revised remediation date approved by the ISM or Leadership Team.

3.4 Patch Management

- a. Security patches must be applied in accordance with the remediation SLAs defined above.
- b. The following patch prioritization rules apply:
 - i. Operating system and critical application patches rated Critical or High must be applied within the SLA regardless of scheduled maintenance windows.
 - ii. Patches for Medium and Low vulnerabilities may be batched and applied during scheduled maintenance windows.
 - iii. Emergency patches may be applied outside of maintenance windows following the Emergency Change process defined in the System Change Policy.

- c. Patch application must be tested in a non-production environment before deployment to production, except for emergency patches where risk of delay exceeds risk of deployment.

3.5 Vulnerability Tracking and Reporting

- a. All identified vulnerabilities must be logged in a vulnerability register maintained by the ISM. The register must include: system affected, vulnerability description, CVSS score, severity, assigned owner, remediation status, and target remediation date.
- b. The ISM must report on vulnerability management status to the Leadership Team on a **quarterly** basis, including open vulnerability counts by severity, SLA compliance rates, and overdue items.
- c. Vulnerabilities that are accepted rather than remediated must be formally approved by the ISM and documented in the vulnerability register with compensating controls and a review date.

3.6 Configuration and Change Monitoring

- a. IronHub must implement automated configuration monitoring to detect unauthorized changes to system configurations that may introduce new vulnerabilities.
- b. Any unauthorized configuration change must be investigated as a potential security incident in accordance with the Security Incident Response Policy.

4 Enforcement

- a. System owners are responsible for remediating vulnerabilities within their systems by the defined SLA. Failure to remediate within SLA must be escalated to the ISM.
- b. Violations of this policy may result in disciplinary action up to and including termination.