Security Incident Response Policy

IronHub Inc

August 2026

Contents

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC7.3, CC7.4, CC7.5

Table 2: Document history

Date	Comment
Jun 1 2022	Initial document
Nov 28 2024	Updated document structure

1 Purpose and Scope

1.1 Purpose

This Security Incident Response Policy establishes controls to ensure the timely detection and response to security incidents and vulnerabilities. It provides clear guidelines for incident reporting, classification, investigation, resolution, and communication.

1.2 Scope

This policy applies to all users of IronHub's information systems, including employees, contractors, and external parties with system access. All users must adhere to this policy to maintain the security and integrity of IronHub's information assets.

2 Background

IronHub is committed to detecting and mitigating information security risks to protect employees, customers, and partners. Security incidents, including data breaches, must be promptly addressed to minimize damage and legal exposure. This policy ensures a structured approach to incident management.

3 Policy

3.1 Reporting Incidents

- All users must report suspected or confirmed security incidents within 24 hours to the Information Security Manager (ISM) via email at `support@theironhub.com`.
- Failure to report security incidents will result in disciplinary action.

3.2 Incident Handling

- All security incidents must follow the defined incident management procedures.
- Incident response procedures must be reviewed and updated annually.
- Incident response testing must be conducted at least twice per year.
- Incident logs must be reviewed monthly to assess response effectiveness.

3.3 Data Preservation

- Evidence related to security incidents (e.g., logs, files, system snapshots) must be preserved for investigation and potential legal proceedings.

4 Procedure for Establishing Incident Response System

4.1 Designation of Roles

- The ISM is responsible for overseeing incident response procedures.
- A rotating on-call schedule must be defined for incident response.
- Key stakeholders from Engineering, Legal, HR, and C-Suite teams must be assigned as management sponsors.

4.2 Communication Channels

- A dedicated security incident email inbox must be monitored for reports.
- An incident ticketing system must be used for tracking incidents.
- Updated contact details for the on-call ISM must be maintained.

4.3 Training and Awareness

- All employees must complete security incident response training twice annually.
- Incident response procedures must be accessible to all users.

5 Procedure for Executing Incident Response

5.1 Incident Identification

- Users must report incidents within 24 hours to their manager, who must escalate it to the ISM.
- Reports must include:
  - Incident description
  - Date, time, and location
  - Reporting person
  - Evidence and affected systems

5.2 Incident Investigation

- Within 48 hours, the ISM must conduct an initial investigation and assign a severity level:
  - **High**: Major impact on operations or regulatory compliance.
  - **Medium**: Significant impact on business units or service delivery.

  - **Low**: Security policy violation with minimal business impact.

5.3 Criteria and Response Times for Client Notification

- Clients must be notified of incidents based on the classification:
  - **High Severity:** Clients must be notified within 24 hours of incident confirmation.
  - **Medium Severity:** Clients must be notified within 48 hours of incident confirmation.
  - **Low Severity:** Clients must be notified within 72 hours if their data or operations are affected.
- Notifications must include:
  - Summary of the incident
  - Impact assessment
  - Mitigation steps taken
  - Further actions required, if any

5.4 Regulatory and Legal Notification

- In the event of a personal data breach (unauthorized access to, disclosure of, or loss of personal information), the ISM must assess regulatory notification obligations immediately.
- Applicable data protection authorities must be notified within **72 hours** of becoming aware of the breach, where required by applicable law (e.g., GDPR, PIPEDA, or other applicable privacy regulations).
- If notification is not made within 72 hours, a written explanation for the delay must be provided to the relevant authority.
- Affected data subjects must be notified without undue delay if the breach is likely to result in a high risk to their rights and freedoms.
- All regulatory notifications must be documented, including the decision rationale if notification was deemed unnecessary.

5.5 Cyber Insurance Notification

- When any senior executive officer becomes aware of a cyber incident or any event that may reasonably give rise to an insurance claim, IronHub's cyber insurer must be notified as soon as reasonably practicable. For cyber incidents, notification may be made by calling the insurer's 24/7 cyber incident response line.

- In the event of cyber crime (e.g., funds transfer fraud, social engineering) or a cyber extortion demand, the incident must also be reported to appropriate law enforcement authorities as soon as reasonably practicable.
- **Ransom payments must not be made without the cyber insurer's prior written agreement.** No costs, ransom payments, or settlement commitments may be made without the insurer's prior written consent, except that necessary costs incurred within the first **72 hours** of discovering a cyber event may be authorized without prior written consent. Any third-party vendors engaged within this 72-hour window must be drawn from the insurer's approved claims panel providers.
- The ISM is responsible for maintaining current contact details for the cyber insurer's claims manager and incident response line, and for ensuring these are accessible during an incident.

5.6 Incident Containment and Resolution

- The ISM, in consultation with management, determines appropriate containment and remediation actions.
- If the incident is categorized as High or Medium, a communications plan must be developed in collaboration with HR, Legal, and C-Suite.
- The ISM must ensure preservation of forensic evidence for law enforcement if required.
- Actions taken to mitigate the incident must be logged, including:
  - Description and severity
  - Root cause
  - Mitigation steps
  - Disclosure recipients (e.g., customers, vendors, regulators)

5.7 Post-Incident Review

- A post-mortem analysis must be conducted within **5 business days** of incident closure to identify root causes and improvements.
- The post-mortem must document:
  - Timeline of events
  - Root cause analysis
  - Containment and remediation actions taken
  - Gaps identified in detection or response
  - Action items with owners and due dates

- Lessons learned must be shared across the organization within 10 business days of closure.
- The CEO may escalate serious incidents to external authorities, including law enforcement and regulatory bodies.

5.8 Incident Response Testing

- The incident response plan must be tested at least **annually** via a tabletop exercise involving key stakeholders from Engineering, Legal, HR, and the C-Suite.
- Test results, findings, and action items must be documented and used to update the incident response plan within 30 days of the exercise.
- Ad hoc or simulated incident exercises (e.g., phishing simulations, breach scenarios) are encouraged throughout the year in addition to the formal annual exercise.

5.9 User Notifications and Remediation

- Users must be informed of incidents affecting them.
- Additional training must be provided if necessary.
- Disciplinary actions must be taken if malicious intent is detected.