Incident Response Plan (IRP) Policy

Version Date: Aug 2nd 2025

1. Purpose

The purpose of this policy is to establish a structured approach to managing security incidents that affect the HR2000 platform. It aims to minimize the impact of security breaches, ensure rapid response, protect customer data, and maintain trust and compliance.

2. Scope

This policy applies to all:

- Components of the product (application, database, cloud infrastructure, APIs)
- Employees, contractors, and third-party service providers
- Incidents involving data breaches, system compromise, malware, DDoS attacks, unauthorized access, or any abnormal behaviour indicating a potential security event

3. Incident Response Objectives

- Detect and confirm security incidents quickly
- Contain and mitigate the impact
- Eradicate the root cause and recover operations
- Communicate effectively with stakeholders and customers
- Prevent recurrence through post-incident review and improvement

4. Definitions

- Security Incident: Any attempted or actual unauthorized access, use, disclosure, modification, or destruction of information or system resources.
- Event: A deviation from normal operations that may indicate a security issue.
- Incident Response Team (IRT): A cross-functional team responsible for managing the incident.

5. Roles and Responsibilities

Role	Responsibilities
Incident Response Team (IRT)	Coordinates incident response activities
CISO / Security Manager	Leads the incident response process and ensures policy execution
DevOps / IT Team	Assists in technical investigation and remediation
Legal & Compliance	Manages regulatory reporting and legal risk
Communications Lead	Handles customer and public notifications
All Employees	Report suspected incidents immediately

6. Incident Response Lifecycle

6.1 Preparation

- Maintain an up-to-date incident response plan and team contact list
- Conduct training and simulation exercises annually
- Ensure monitoring, logging, and alerting systems are in place

6.2 Detection & Analysis

- Detect anomalies through automated alerts, monitoring tools, or user reports
- Classify the incident severity (Low / Medium / High / Critical)
- Collect evidence (logs, screenshots, packet captures)

6.3 Containment

- Short-term containment: Isolate affected systems immediately
- Long-term containment: Apply patches, disable accounts, block IPs
- Ensure data integrity and prevent spread of the issue

6.4 Eradication

- Identify root cause (e.g., unpatched vulnerability, misconfiguration)
- Remove malware, close vulnerabilities, revoke compromised credentials
- Validate system integrity before restoration

6.5 Recovery

- Restore affected systems to full operation
- Monitor systems for signs of reinfection or re-compromise
- Re-enable services with continuous observation

6.6 Post-Incident Review

- Conduct a "lessons learned" session within 7 days
- Document findings, timeline, actions taken, and recommendations
- Update policies, procedures, and controls based on findings

7. Communication Plan

- Internal Notifications: Immediate alert to IRT and executives
- Customer Notifications: Within 72 hours if personal data is compromised (as per PDPA laws)
- Regulatory Reporting: As required by law or contractual obligation
- Public Statements: Handled by Communications Lead in coordination with Legal

8. Incident Severity Classification

Severity	Description	Example
Low	No impact to customer data or services	Failed login attempts
Medium	Minor impact, isolated system	Malware detected and quarantined
High	Affects service availability or internal systems	DDoS, partial outage
Critical	Major data breach or full SaaS downtime	Ransomware, data exfiltration

9. Documentation and Reporting

All incidents must be documented, including:

- Incident description and timeline
- Affected systems and data
- Actions taken and outcomes
- Final resolution and lessons learned

Records are retained for at least 3 years or as required by law.

10. Policy Review

This policy will be reviewed annually, or sooner if:

- There are significant system changes
- A critical incident occurs
- Regulatory requirements are updated

11. Compliance and Violations

Failure to report or appropriately handle security incidents may result in disciplinary action, including termination or legal consequences.

HR 2000 SDN BHD (475163-M)