Version Date: Aug 2nd 2025

1. Purpose

This policy establishes the risk management framework for HR2000's platform. It ensures that all significant risks to the operation, security, legal compliance, and continuity of the SaaS system are effectively identified, assessed, managed, and monitored.

2. Scope

This policy applies to all components of the system including:

- Application software
- Infrastructure and hosting services
- Third-party integrations
- Customer data and access
- Development and operations (DevOps) processes

It covers all employees, contractors, and third parties involved in the development, maintenance, and operation of the system.

3. Risk Management Objectives

- Protect customer data and system assets from threats and vulnerabilities
- Ensure compliance with regulatory and contractual obligations
- Reduce the likelihood and impact of incidents
- Promote informed decision-making and accountability
- Ensure business continuity and disaster recovery preparedness

4. Risk Management Process

The risk management process follows 5 core steps:

4.1 Risk Identification

Risks are identified through:

- Threat modelling during software design
- Regular security assessments and audits
- Incident reports and lessons learned
- Regulatory and legal updates
- Vendor risk assessments

4.2 Risk Assessment

Each risk is evaluated based on:

- Likelihood of occurrence (Low, Medium, High)
- Impact on operations, data security, compliance, and reputation (Low, Medium, High)

4.3 Risk Treatment

Risk mitigation strategies include:

- Avoidance (e.g., not adopting risky tech)
- Reduction (e.g., implementing controls)
- Transfer (e.g., insurance, outsourcing)
- Acceptance (e.g., if risk is low and controlled)

Risk treatment plans must be documented with assigned ownership and deadlines.

4.4 Risk Monitoring and Review

- Risk registers are reviewed at least quarterly.
- High-impact risks are monitored continuously.
- Internal and external audits will validate the effectiveness of risk controls.

4.5 Communication and Reporting

- Risk status reports are submitted to executive management quarterly.
- Significant risks are escalated immediately.
- Employees are briefed on risk management responsibilities annually.

5. Roles and Responsibilities

Role	Responsibilities
Risk Manager / CISO	Maintains the risk framework, conducts assessments, and reports on risk posture
Engineering / DevOps	Implements technical controls and mitigates system-related risks
Compliance Officer	Ensures regulatory and contractual compliance
Management	Makes risk-based decisions and provides oversight
All Employees	Report risks and comply with controls

6. Policy Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination or legal action. All employees and partners must acknowledge and agree to this policy.

8. Review and Updates

This policy will be reviewed annually or upon significant changes to the product architecture, threat landscape, or legal environment.

HR 2000 SDN BHD (475163-M)