

INFORMATION SECURITY POLICY

Stake

Key Information	
Approving Official(s)	Head of IT Security
Responsible Office	Head of IT Security - Compliance Team – HR
Effective Date	30 May 2025
Next Review Date	30 May 2026

This policy is established to ensure alignment with **ISO/IEC 27001:2022** and the applicable clauses and controls:

- ☐ **Clause 4.2** – *Understanding the needs and expectations of interested parties*
- ☐ **Clause 5.1** – *Leadership and commitment*
- ☐ **Clause 5.2** – *Information security policy*
- ☐ **Clause 6.1.3** – *Information security risk treatment*
- ☐ **Clause 7.4** – *Communication*
- ☐ **Clause 8.1** – *Operational planning and control*
- ☐ **Clause 9.1** – *Monitoring, measurement, analysis and evaluation*
- ☐ **Clause 10.1** – *Nonconformity and corrective action*
- ☐ **Control A.5.1** – *Policies for information security*
- ☐ **Control A.5.2** – *Information security roles and responsibilities*
- ☐ **Control A.5.23** – *Information security for use of cloud services*
- ☐ **Control A.5.28** – *Secure coding*
- ☐ **Control A.5.29** – *Security testing in development and acceptance*
- ☐ **Control A.5.32** – *Change management*
- ☐ **Control A.5.36** – *Compliance with policies, rules and standards for information security*
- ☐ **Control A.5.37** – *Documented operating procedures*

Table of Contents

1. Purpose
2. Scope
3. Governance
4. Information Security Objectives
5. Roles and Responsibilities
6. Core Security Principles
 - ☐ a. Access Control
 - ☐ b. Data Protection
 - ☐ c. Incident Management
 - ☐ d. System Development & Change Control
 - ☐ e. Monitoring & Auditing
7. Third-Party Risk Management
8. Training and Awareness
9. Policy Review and Maintenance
10. Approval

1. Purpose

1.1 Medium Rare / Stake (“the Company”) is committed to protecting its information assets, systems, and services.

1.2 This Information Security Policy establishes a structured framework for protecting information assets, maintaining the confidentiality, integrity, and availability of data, and ensuring compliance with ISO/IEC 27001:2022.

2. Scope

This policy applies to all employees, contractors, and authorized third-party service providers accessing or managing the Company’s technology systems, data, or infrastructure. This includes customer and corporate information, systems supporting operations, technology platforms, and cloud services.

3. Governance

Medium Rare / Stake retains full accountability for ensuring adherence to defined security and privacy standards. Contracts with providers include enforceable obligations covering data protection and incident response.

4. Information Security Objectives

The objectives of this policy are to safeguard all sensitive and regulated data, ensure uptime and resilience of platforms, clearly define and enforce responsibilities, and maintain compliance with ISO 27001:2022.

5. Roles and Responsibilities

Role	Responsibilities
Security Officer	Enforcement of technical and operational controls
Operations Team	Implementation of operational security practices

Service Providers	Secure provision of IT services, infrastructure, and development
All Personnel	Compliance with security policies and incident reporting

6. Core Security Principles

a. Access Control Role-based access is enforced. Multi-factor authentication (MFA) is mandatory for administrative accounts. Access rights are regularly reviewed.

b. Data Protection Data is encrypted in transit and at rest. Secure data deletion is enforced.

c. Incident Management An incident response plan is maintained. Vendors are contractually required to report incidents immediately. Escalation and notification processes are defined. Company manages all information security incidents.

□ Key Principles:

- **Identification & Reporting:** Incidents are identified through proactive logging and monitoring systems, as well as through direct reporting by personnel. All confirmed or suspected security incidents are reported to the IT & Security Team and documented.
- **Structured Response:** An Incident Response Plan (IRP) defines roles, responsibilities, and procedures for incident identification, containment, eradication, and recovery.
- **Plan Validation:** The IRP undergoes regular testing via drills and annual reviews.

d. System Development & Change Control A secure software development lifecycle (SDLC) is enforced. All code changes are reviewed and tested before deployment. Production environments are segregated from development.

e. Monitoring & Auditing All critical systems are monitored. Logs are collected and retained. Regular vulnerability scanning and independent security assessments are conducted.

f. Business Continuity and Disaster Recovery

The Company maintains overarching Business Continuity and Disaster Recovery capabilities to ensure the resilience and availability of critical operations and systems:

- **Business Continuity:** A high-level Business Continuity Plan outlines how essential business functions are sustained or resumed during disruptions. This includes continuity objectives and general responsibilities, with further detail defined in supporting documentation.
- **Disaster Recovery:** A Disaster Recovery Plan exists to guide the restoration of IT systems, platforms, and data following significant incidents. This includes defined roles, high-level recovery strategies, and reference to system-specific recovery procedures.
- **Testing and Assurance:** Business continuity and disaster recovery capabilities are periodically tested and reviewed to ensure effectiveness and alignment with organisational needs.
- **Responsibilities:** The IT & Security Team oversees the management and coordination of continuity and recovery planning. Operational teams and service providers are required to support recovery objectives as defined in their respective responsibilities.

7. Third-Party Risk Management

Third-party agreements include data protection, audit rights, and breach notification clauses. Service providers undergo security due diligence during onboarding and are reviewed annually.

The organisation shall conduct due diligence reviews of all critical third-party service providers to ensure security requirements are met.

8. Training and Awareness

All staff complete security training at onboarding and annually. Roles with elevated access receive enhanced training. Awareness initiatives are conducted regularly.

9. Policy Review and Maintenance

This policy is reviewed annually or following significant changes to systems, operations. Updates are approved by senior management and communicated throughout the organisation.

Policy Name: Information Security

Effective Date: 30 May 2025

Version 1.0