

Information Security Policy

1. Introduction

1.1 Purpose

This Information Security Policy (the "Policy") outlines the framework for managing and protecting the confidentiality, integrity, and availability of information assets owned or controlled by Grace Bay B.V. (the "Company"). The Policy is designed to mitigate risks associated with data breaches, unauthorized access, and operational disruptions in the online gambling industry. It promotes a culture of security awareness and ensures the protection of player data, financial information, gaming systems, and other sensitive assets. By implementing this Policy, the Company aims to maintain trust with players, comply with applicable laws and regulations, and align with industry best practices for information security management systems (ISMS).

1.2 Scope

This Policy applies to all information assets, including digital and physical data, systems, and processes used in the Company's operations. It encompasses:

- All employees, contractors, consultants, vendors, and third-party service providers who have access to the Company's information.
- All forms of data, including player personal information (e.g., identification details, payment information, gaming history), proprietary software, transaction records, and intellectual property.
- IT infrastructure, including networks, servers, applications, and endpoints.
- Physical and virtual environments where information is stored, processed, or transmitted.

The Policy covers all aspects of the Company's B2C gaming activities, including online platforms, mobile applications, and associated services.

1.3 Objectives

- **Confidentiality:** Ensure that sensitive information is accessible only to authorized individuals.
- **Integrity:** Protect information from unauthorized modification or destruction.
- **Availability:** Guarantee that information and systems are available when needed to support business operations.

- **Compliance:** Adhere to relevant legal, regulatory, and contractual obligations, including data protection laws, anti-money laundering (AML) requirements, and industry standards for fair gaming.
- **Risk Management:** Identify, assess, and mitigate security risks to minimize potential impacts on the business and stakeholders.

1.4 Regulatory and Standards Alignment

The Company is committed to complying with applicable international standards and regulations, including but not limited to data protection frameworks, AML directives, and gaming-specific guidelines. This includes ensuring fair play through certified random number generators (RNGs) and integrating security with responsible gaming practices.

Non-compliance with this Policy may result in disciplinary actions, legal consequences, or reputational damage.

2. Definitions

For clarity, the following terms are defined:

- **Information Assets:** Any data, hardware, software, networks, or processes that have value to the Company.
- **Sensitive Information:** Includes personally identifiable information (PII) of players, financial data, gaming algorithms, and trade secrets.
- **Security Incident:** Any observed or suspected event that could compromise the security of information assets, such as unauthorized access, data loss, or malware infection.
- **Access Controls:** Mechanisms to restrict access to information based on roles and necessities.
- **Encryption:** The process of converting data into a coded format to prevent unauthorized access.
- **RNG:** Random Number Generator, a system used to ensure randomness and fairness in games, subject to independent certification.

3. Governance and Responsibilities

3.1 Information Security Governance

Executive Management shall oversee the implementation, review, and continuous improvement of this Policy, with support from designated personnel as needed.

3.2 Roles and Responsibilities

- **Executive Management:** Provide leadership and resources for information security initiatives; approve the Policy and ensure its alignment with business objectives.
- **Designated Information Security Responsible:** Develop, implement, and monitor security practices; conduct risk assessments; report on security performance to management; handle integration with regulatory requirements such as AML/KYC processes and player protection measures.
- **All Employees and Contractors:** Adhere to security procedures, report incidents promptly, and participate in training programs. They are responsible for protecting information in their custody.

Third-party vendors must sign agreements that include security obligations aligned with this Policy.

4. Risk Management

The Company shall implement a risk management process:

- **Risk Identification:** Identify threats and vulnerabilities through assessments and threat intelligence.
- **Risk Assessment:** Evaluate risks based on likelihood and impact, prioritizing those affecting player data, financial integrity, or gaming fairness.
- **Risk Treatment:** Develop and implement mitigation plans, such as controls or acceptance of residual risks.
- **Monitoring and Review:** Review risks periodically or after significant changes.

Tools like penetration testing, vulnerability scanning, and third-party audits may be used to validate controls.

5. Asset Management

- **Inventory:** Maintain an inventory of information assets, classifying them by sensitivity (e.g., public, internal, confidential, restricted).
- **Ownership:** Assign owners to assets who are responsible for their protection and management.
- **Handling Procedures:** Define rules for secure handling, storage, transmission, and disposal of assets, including secure deletion of data no longer needed.

6. Human Resources Security

- **Pre-Employment:** Conduct background checks and require non-disclosure agreements (NDAs) for roles with access to sensitive information.
- **Training and Awareness:** Provide security training, including topics like phishing awareness, data privacy, and responsible gaming.
- **Termination:** Revoke access immediately upon termination and reinforce ongoing obligations.

7. Physical and Environmental Security

- **Asset Protection:** Safeguard physical hardware and devices against theft, damage, or unauthorized access through secure storage practices, device encryption, and remote wipe capabilities.
- **Environmental Controls:** Protect assets from environmental hazards using uninterruptible power supplies (UPS), redundancy measures, and monitoring tools where applicable.
- **Remote and Cloud-Based Assets:** Apply equivalent protections to virtual or third-party hosted environments, including contractual requirements for data centers to maintain physical security standards such as access controls and surveillance.

8. Communications and Operations Management

8.1 Network Security

- Implement firewalls, intrusion detection/prevention systems (IDS/IPS), and secure configurations to protect networks.

- Use virtual private networks (VPNs) for remote access and segment networks to isolate sensitive systems.

8.2 System Acquisition, Development, and Maintenance

- Ensure security is integrated into system development, including secure coding practices.
- Require independent certification for RNGs and gaming software to ensure integrity and fairness.

8.3 Supplier Relationships

- Assess third-party risks and include security requirements in contracts, such as data processing agreements.

8.4 Backup Management

- Perform backups of critical data, store them securely, and test restoration procedures.

9. Access Control

- **User Access Management:** Grant access based on the principle of least privilege and need-to-know, using role-based access controls (RBAC).
- **Authentication:** Enforce strong passwords, multi-factor authentication (MFA), and session timeouts.
- **Privileged Access:** Monitor and log access by administrators.
- **Player Access:** Implement KYC verification to prevent unauthorized users (e.g., minors) and integrate with responsible gaming tools.

10. Cryptography

- Use industry-standard encryption for data in transit and at rest.
- Manage cryptographic keys securely.

11. Information Security Incident Management

- **Incident Response Plan:** Establish a plan for detecting, reporting, responding to, and recovering from incidents.

- **Reporting:** Require immediate internal reporting of incidents; escalate to management and, where required, to authorities or affected parties (e.g., data breach notifications).
- **Post-Incident Review:** Analyze incidents to identify root causes and update controls.
- **Business Continuity:** Develop plans to ensure minimal disruption, including disaster recovery for gaming operations and player fund protection.

12. Compliance

- **Monitoring and Measurement:** Use logging and monitoring tools to track security effectiveness.
- **Audits:** Conduct audits as needed.
- **Legal Compliance:** Stay informed of changes in laws and update the Policy accordingly.

13. Policy Review and Enforcement

- This Policy shall be reviewed periodically or following material changes in operations, technology, or regulations.
- Enforcement mechanisms include monitoring, investigations, and sanctions for violations.
- The Policy is effective as of 10/11/2025 and applies to all relevant parties.

Approval

Approved by:

Date: