

Information Security Policy

-Edge Five Entertainment B.V.

1. Purpose

This Information Security Policy sets out the principles and guidelines to ensure the confidentiality, integrity, and availability of all sensitive information processed by Edge Five Entertainment B.V. It aims to protect against unauthorized access, data breaches, and other security threats as required by the Curaçao Gaming Control Board (GCB).

2. Scope

This policy applies to all employees, contractors, third-party service providers, and any other individuals who have access to the company's information systems, networks, and data.

3. Key Principles

- **Confidentiality:** Ensure that sensitive information is only accessible to authorized individuals.
- **Integrity:** Protect the accuracy and completeness of information.
- **Availability:** Ensure that information is available when needed by authorized users.

4. Security Measures

- **Data Encryption:** All sensitive data must be encrypted in transit (e.g., TLS 1.2/1.3) and at rest (e.g., AES-256) to prevent unauthorized access.
- **Access Control:** Implement Role-Based Access Control (RBAC) and the Principle of Least Privilege (PoLP) to limit data access based on job function.
- **Multi-Factor Authentication (MFA):** Required for all critical systems and administrative accounts.
- **Network Security:** Use firewalls, intrusion detection systems (IDS), and secure VPNs to protect internal networks.
- **Physical Security:** Secure physical access to servers and data centers with biometric or card-based access control systems.

5. Data Protection

- **Data Minimization:** Only collect and retain the minimum amount of data necessary for business operations.
- **Data Backup and Recovery:** Implement regular data backups, with offsite storage, and test recovery procedures periodically.
- **Data Retention and Disposal:** Define retention periods for different data types and ensure secure disposal of outdated data.
- **Personal Data Protection:** Ensure compliance with GDPR and other relevant data protection regulations.

6. Incident Response

- **Detection and Reporting:** Implement real-time monitoring for suspicious activities and establish clear incident reporting procedures.
- **Containment and Eradication:** Immediately isolate affected systems and remove threats.
- **Recovery and Analysis:** Recover systems to a secure state and conduct root cause analysis to prevent recurrence.
- **Post-Incident Review:** Regularly update incident response plans based on lessons learned.

7. Compliance and Audits

- **Internal Audits:** Conduct regular internal audits to ensure compliance with GCB requirements and internal policies.
- **Third-Party Assessments:** Engage independent auditors for periodic security assessments.
- **Regulatory Reporting:** Submit required security and compliance reports to the GCB on a regular basis.

8. Continuous Improvement

- **Training and Awareness:** Provide ongoing security training for employees and contractors.
- **Technology Upgrades:** Regularly assess and implement new security technologies as needed.
- **Policy Review and Updates:** Review this policy annually or as required by changes in GCB regulations.

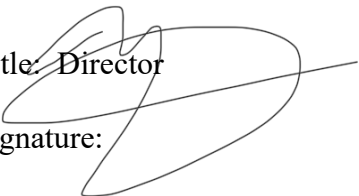
9. Policy Review

- This policy will be reviewed and updated annually or as required by changes in GCB regulations.

Approved by:

Name: MICHAELIDIS NIKOS

Title: Director

Signature: 

Date: May 8, 2025