

GENERAL CYBER & INFORMATION SECURITY POLICY

ISLAND LUKKLY B.V.

Effective Date: 13.05.2025

Last Updated: 29.09.2025

Approved by: Executive Management

1. INTRODUCTION

1.1. Information and information assets are vital resources for ISLAND LUKKLY B.V. and must be safeguarded by putting in place suitable controls to lower the risks associated with using them.

1.2. This document also demonstrates Management's commitment to create a transparent security policy and its dedication to putting ISLAND LUKKLY B.V.'s Information Security Management System into place and keeping it up to date through continuous improvements.

1.3. To adhere to relevant laws, regulations, directives, and industry standards.

2. PURPOSE AND SCOPE

2.1. The purpose of this Policy is to establish a comprehensive framework for safeguarding information assets, systems, and player data at Island Lukkly B.V. The Policy applies to all employees, contractors, and third parties who process or have access to Company data, regardless of the system or platform. It ensures compliance with applicable laws, including the National Ordinance on Games of Chance (LOK), the Curaçao Gaming Authority (CGA) and Gaming Control Board (GCB) guidance, the General Data Protection Regulation (GDPR), and international standards such as ISO/IEC 27001, ISO/IEC 22301, and PCI DSS v4.0.

3. INFORMATION SECURITY OBJECTIVES

3.1. To safeguard the information and system assets of ISLAND LUKKLY B.V., ensuring confidentiality, integrity, and availability of the company's data, thereby protecting its reputation.

3.2. To adhere to relevant laws, regulations, directives, and industry standards.

3.3. To strengthen the security culture among employees, customers, and other stakeholders through ongoing cybersecurity and awareness initiatives.

3.4. To boost competitive advantage by securely enabling the development and delivery of new products and services.

3.5. To align the company's security practices with its overall business strategy.

4. ACCESS CONTROL AND IDENTITY MANAGEMENT

4.1. Access to Company systems is strictly controlled according to the principle of least privilege. All administrative accounts and remote access require multi-factor authentication. User accounts are created, modified, and terminated following the Company's joiner-mover-leaver process to ensure timely adjustments to access rights. Privileged accounts are reviewed quarterly, and their use is continuously monitored. Shared accounts are prohibited, and password reuse is not permitted. Non-compliance with these rules will be treated as a breach of security policy.

5. POLICY STATEMENTS

5.1. ISLAND LUKKLY B.V. is **certified under PCI DSS v4.0**, which provides a robust framework for securing payment card data and associated environments.

5.2. In addition, the company uses internationally recognized best practices, such as those from ISO/IEC 27001, ISO/IEC 22301, and ISO/IEC 20000, as references to strengthen its security posture, though it does not currently hold certifications under these frameworks.

Note: ISLAND LUKKLY B.V. is not certified in these additional standards but uses them as guidance for enhancing internal processes.

5.3. All ISLAND LUKKLY B.V. personnel, contractors, and third-party service providers are required to comply with this policy and any supporting procedures, standards, or regulatory requirements.

5.4. This policy has been reviewed and approved by Executive Management and is communicated to all relevant stakeholders.

6. DATA ENCRYPTION AND CRYPTOGRAPHY

6.1. All sensitive information, including player data, financial data, and authentication credentials, is encrypted in transit using TLS 1.2 or higher and at rest using AES-256 or equivalent. Encryption keys are securely managed in accordance with industry best practices, stored in hardware security modules (HSM) or equivalent, and rotated at least annually. Obsolete protocols such as SSL or TLS versions lower than 1.2 are disabled across all systems.

7. VENDOR AND THIRD-PARTY MANAGEMENT

7.1. Before engaging with third-party providers, the Company performs security due diligence to ensure that vendors meet the same security standards required internally. Contracts with third-party providers include mandatory Data Processing Agreements (DPA) and security schedules to govern the handling of personal data. Vendors providing critical services are reviewed annually, and their compliance with security obligations is subject to audit by Island Lukkly B.V.

8. DATA CLASSIFICATION AND ASSET MANAGEMENT

8.1. All information assets are classified as Confidential, Internal, or Public. An inventory of assets is maintained, listing owners, classification levels, and applicable security measures. Confidential

and payment-related data may not be stored or transmitted without encryption. Employees are prohibited from transferring Company or player data through unapproved or unsecured channels.

8.2 This policy applies to:

- (a) All ISLAND LUKKLY B.V. staff (employees, contractors, consultants)
- (b) All information systems, infrastructure, and digital assets owned or managed by the company
- (c) Any third-party entity that processes or manages data on behalf of ISLAND LUKKLY B.V.

9. LOGGING, MONITORING, AND VULNERABILITY MANAGEMENT

9.1. Island Lukkly B.V. maintains a centralised logging and monitoring framework to ensure the integrity and security of its information systems.

9.2. All critical systems, including player account management, payment platforms, and administrative portals, generate security logs that capture authentication attempts, privilege changes, and financial transactions.

9.3. These logs are collected in a central Security Information and Event Management (SIEM) system, which is actively monitored to detect anomalies and potential security breaches.

9.3.1. Operational logs are retained for a minimum of 1 (one) year to support ongoing monitoring and investigations, while regulatory logs, including access records and incident traces, are retained for at least 5 (five) years in compliance with Curaçao Gaming Authority (CGA) and Gaming Control Board (GCB) requirements.

9.4. Suspicious or abnormal activities identified through log analysis are escalated immediately to the Information Security Officer (ISO) for investigation and remediation.

9.5. In addition to monitoring, Island Lukkly B.V. has established a structured vulnerability management program to proactively identify, assess, and remediate security weaknesses:

9.5.1. Vulnerability scans are performed at least monthly on all critical infrastructure and applications.

9.5.2. Any critical vulnerabilities identified must be remediated within 7 (seven) days, and high-severity vulnerabilities within 30 (thirty) days.

9.5.3. The Company commissions an independent external penetration test of its environment on an annual basis to validate the resilience of its security controls, while an internal penetration test is conducted at least every 2 (two) years.

9.6. All findings from vulnerability assessments and penetration tests are documented in a central register, tracked until closure, and reported to senior management and the Board as part of the Company's ongoing information security governance process.

10. BUSINESS CONTINUITY AND DISASTER RECOVERY

10.1. Island Lukkly B.V. maintains a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) that ensure the timely restoration of critical services in case of disruption. The Recovery Time Objective (RTO) for critical systems is set at 24 hours, and the Recovery Point Objective (RPO) at one hour. Both BCP and DRP are tested at least once per year, and the results are documented and presented to senior management and regulators upon request.

11. TRAINING AND AWARENESS

11.1. All employees undergo mandatory information security training as part of their onboarding process and must complete refresher training annually. Regular phishing simulations and awareness campaigns are conducted to reinforce vigilance. Failure to comply with information security requirements, including failure to report incidents or suspected breaches, may result in disciplinary measures.

12. REFERENCE DOCUMENTS

PCI DSS v4.0 (Certified Standard)

ISO/IEC 27001:2022 - Information Security Management (reference only)

ISO/IEC 22301:2019 - Business Continuity Management (reference only)

ISO/IEC 20000:2018 - IT Service Management (reference only)

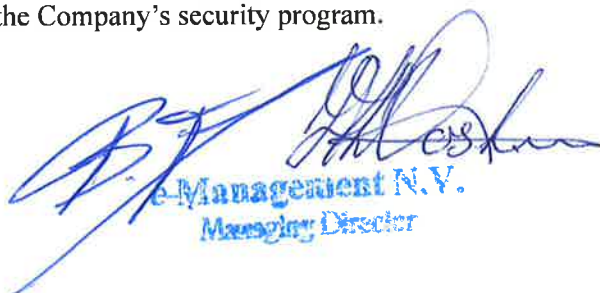
GDPR (Regulation (EU) 2016/679) and Applicable Curaçao data protection regulations

Applicable Curaçao data protection and cybersecurity regulations

International best practices and regulatory guidance where applicable

13. GOVERNANCE

Island Lukkly B.V. maintains a clear governance structure to ensure accountability and oversight of information security. The Information Security Officer (ISO) is responsible for implementing this Policy, monitoring compliance, and coordinating the Company's overall security framework. In addition to daily operational oversight, the ISO prepares a comprehensive quarterly report for the Board of Directors. This report includes a summary of all security incidents and their resolution status, the results of vulnerability assessments and penetration testing, records of staff training and awareness activities, and an outline of planned improvements to the Company's security posture. The Board reviews these reports to ensure that appropriate resources and measures are allocated to address identified risks. This governance process ensures that information security remains a standing agenda item at the highest level of management and that continuous improvement is embedded in the Company's security program.



e-Management N.V.
Managing Director