

Information Security Policy

OF

LUCKYROO N.V.

As of: 1 September 2025

Approved by:

Morganite Corporate Services B.V.

Director of:

LuckyRoo N.V.



A handwritten signature in black ink is positioned to the left of a circular corporate seal. The seal features the Morganite logo (a stylized 'M' inside a square) and the text 'MORGANITE CORPORATE SERVICES B.V.' around the perimeter. Below the signature and seal, a horizontal line extends across the page.

Information Security Policy	1
1. Preliminary Declarations	3
2. Scope of Enforcement	3
3. Foundational Security Principles	4
4. Protective Mechanisms and Administrative Controls	4
Defense of Technical Infrastructure	4
Governance of Identities and Privileges	4
Secure Management of Data Assets	4
Application Integrity and Device Safeguards	5
Oversight, Monitoring, and Assurance	5
Governance of Third-Party Relationships	5
5. Obligations of Personnel	5
6. Response to Incidents and Security Events	5
7. Identification and Management of Risks	6
8. Compliance and Enforcement	6
9. Commitment to Continuous Enhancement	6
10. Supervisory Structure and Corporate Governance	6

1. Preliminary Declarations

LUCKYROO N.V., incorporated under the laws of Curaçao with its registered office at 1, Abraham de Veerstraat, Willemstad, Curacao (registration number 163606), administers digital gaming platform betwinner.llc. The Company is duly licensed by the Curaçao Gaming Authority under license OGL/2024/1371/0694, in accordance with the National Ordinance on Offshore Games of Hazard (Landsverordening buitengaats hazardspelen, P.B. 1993, no. 63).

Because the Company constantly processes and transmits sensitive information, including customer identity details, payment transaction data, and operational records of confidential nature, the protection of such assets must be carried out with the highest level of diligence and professional care.

This Policy has been created to provide a structured and consistent framework for safeguarding the Company's information resources. It is intended to preserve confidentiality, accuracy, and reliability, while simultaneously ensuring the uninterrupted and secure provision of gaming services. The adoption of this Policy demonstrates conformity with applicable laws and recognized international standards and reinforces the Company's reputation as a responsible and trustworthy operator within the gaming industry.

2. Scope of Enforcement

This Policy applies comprehensively to every person and entity working with or on behalf of the Company. It covers employees, consultants, contractors, service providers, and any other external partners. Its scope is not limited to individuals but extends equally across all forms of technology, including servers, software, network infrastructures, cloud-based solutions, and backup and recovery systems.

The Policy governs every form of information asset processed or stored by the Company. This includes customer identity and account information, details of financial transactions, official regulatory submissions, compliance-related records, and system-generated operational logs. All vendors and strategic partners are bound by these requirements, ensuring that the same standards of protection are observed within and beyond the internal boundaries of the Company.

3. Foundational Security Principles

The Company's security framework is rooted in several core principles that define its overall approach. Privacy of information is paramount and personal data must remain protected from unauthorized disclosure at all times. Such protection is achieved through a combination of restricted access rights, strong authentication procedures, and the use of advanced encryption. Integrity of information must also be preserved so that data remains accurate, trustworthy, and unaltered by unauthorized action.

Reliability of services is treated as essential to both operations and customer trust, which is why redundant systems, rigorous backup arrangements, and carefully tested recovery

procedures are maintained. Responsibility for protection is regarded as a shared duty; everyone handling information is expected to recognize their role in preserving security, thereby ensuring accountability across the organization. Finally, all security measures are aligned with applicable laws, local regulations, and international standards to guarantee compliance, transparency, and continued legitimacy of the Company's operations.

4. Protective Mechanisms and Administrative Controls

Defense of Technical Infrastructure

The Company employs a comprehensive, layered security architecture to shield its platforms from potential threats. This approach incorporates firewalls, intrusion prevention and detection systems, distributed denial-of-service defenses, and strict reliance on encrypted channels for the transmission of both gaming traffic and payment-related data.

Governance of Identities and Privileges

Access rights are managed under the principle of least privilege. This means that every individual is provided with only the minimum level of access required to perform their responsibilities. Strong authentication processes are enforced, user sessions are continuously monitored, and permissions are reviewed on a regular basis. When an employee or contractor leaves the Company or changes their role, access rights are revoked without delay.

Secure Management of Data Assets

Data classified as sensitive is always encrypted, whether stored or transmitted. When appropriate, personal identifiers are masked or pseudonymized in order to reduce the risk of exposure should unauthorized access occur.

Application Integrity and Device Safeguards

Applications and gaming software are developed in strict conformity with secure coding practices. They undergo frequent independent testing, including penetration tests, security scans, and code reviews, in order to identify vulnerabilities. Devices connecting to Company systems are subject to endpoint protection controls and are managed under approved mobile device policies to ensure that only secure equipment is used.

Oversight, Monitoring, and Assurance

The Company maintains comprehensive monitoring systems that operate continuously to identify unusual or suspicious activity. Security logs are centralized and retained securely, where they are reviewed on a regular basis. Internal audits and formal assessments are scheduled to confirm that controls remain effective and appropriate.

Governance of Third-Party Relationships

Before engaging with suppliers or service providers, the Company conducts thorough due diligence. All third parties are required to commit contractually to compliance with the Company's standards, and their adherence is periodically reassessed to ensure alignment with internal requirements.

5. Obligations of Personnel

Safeguarding the information resources of the Company is a shared responsibility of all employees and contractors. Every individual must complete required training in cybersecurity, anti-fraud measures, and regulatory obligations. Any weaknesses or suspicious activities must be reported immediately through established reporting channels.

Positions involving access to highly sensitive information are subject to background checks. The use of personal devices or unauthorized software for corporate activities is not permitted under any circumstances. Only Company-issued and administratively managed devices are authorized for use when accessing internal systems.

6. Response to Incidents and Security Events

The Company maintains a comprehensive incident response framework that ensures prompt detection, containment, and investigation of any suspected or confirmed breach. Root causes are analyzed with care, and mitigation steps are applied to prevent similar incidents from occurring in the future.

When required, regulators, affected customers, and business partners are informed in a timely and transparent manner. Service restoration procedures are implemented immediately to reduce disruption, while the lessons learned from the incident are incorporated into updated security processes.

7. Identification and Management of Risks

Risk management is treated as an ongoing process within the Company. Regular reviews, independent audits, and certification programs are used to identify and assess vulnerabilities. Risks are logged in a centralized register, prioritized by probability and potential impact, and addressed through corrective actions.

The Company remains vigilant regarding emerging risks such as cybercrime, fraud, and misuse of gaming systems. This forward-looking approach ensures preparedness against both existing and evolving threats.

8. Compliance and Enforcement

Compliance with this Policy is mandatory for all staff and partners. Employees who violate its provisions may face disciplinary consequences, including dismissal. Partners or vendors

who fail to comply risk termination of agreements and may be reported to the appropriate regulatory authorities.

Because adherence to security practices is a prerequisite for maintaining the Company's gaming license, compliance with this Policy is not optional but a fundamental condition of employment and partnership.

9. Commitment to Continuous Enhancement

This Policy is reviewed regularly, at minimum once per year, and amended whenever new technologies, regulatory changes, or security events make such updates necessary. All modifications are formally documented and communicated throughout the Company.

The Company treats security as a constantly developing discipline. Investments are directed toward new tools, advanced training initiatives, and adaptive security practices. Through these measures, the Company seeks to maintain resilience, strengthen defenses, and preserve the confidence of stakeholders.

10. Supervisory Structure and Corporate Governance

Responsibility for the ultimate oversight of this Policy lies with the Board of Directors. The Chief Technology Officer is responsible for day-to-day administration, ensuring that adequate procedures, resources, and strategies are in place to uphold the highest standards of protection.

Independent external audits are performed periodically to validate compliance and confirm to regulators, stakeholders, and customers that the Company operates with integrity, transparency, and the strongest possible security standards.