

INFORMATION SECURITY POLICY

Version: 1.0

Effective Date: September 15, 2025

Information is one of the Company's most critical assets. We rely on physical resources and information technology (IT) systems to store, manage, process, and share information in the course of providing online gaming services, ensuring regulatory compliance, and supporting our internal business functions. Protecting these assets is essential to maintain trust, safeguard our operations, and preserve the integrity of our business.

In particular, it uses the following terms:

“**We**”, “**Company**”, “**Us**”, and “**Our**” when referring to the WUNGroup B.V., a limited liability company incorporated in Curaçao under the company number 160576, with registered business address at Chuchubiweg 17, Willemstad, Curaçao.

1. INTRODUCTION AND PURPOSE

1.1. By adopting this Information Security Policy, the Company affirms its commitment to safeguarding all information assets against unauthorized access, disclosure, alteration, and destruction.

1.2. The Company acknowledges its obligations under the Curaçao Gaming Authority (CGA) requirements, the Central Bank of Curaçao and Sint Maarten guidelines, and internationally recognized standards such as ISO/IEC 27001.

1.3. The objective of this Policy is to ensure confidentiality, integrity, and availability of information systems and data while supporting lawful and responsible iGaming operations.

2. SCOPE

2.1. This Policy applies to all employees, contractors, consultants, temporary staff, interns, volunteers, third-party service providers, and any other individual or entity granted access to Company systems, information assets, or facilities.

2.2. This Policy extends to all forms of information, including but not limited to electronic records, paper-based documents, verbal communications, images, audio and video recordings, and any other medium used to create, store, process, or transmit information.

2.3. This Policy applies to all Company assets, including hardware, software, networks, databases, cloud services, mobile devices, and physical infrastructure used for the processing, storage, or transmission of information.

2.4. This Policy governs all business functions and operations, including but not limited to online gaming services, payment processing, customer support, marketing activities, financial management, human resources, and regulatory reporting.

2.5. This Policy applies in all environments where Company information is accessed, processed, or transmitted, including remote work locations, third-party hosted systems, and cross-border data transfers.

2.6. Compliance with this Policy is mandatory, forms part of the contractual obligations of all relevant stakeholders, and shall be enforced through continuous monitoring, regular audits, and disciplinary or contractual measures where required.

3. GOVERNANCE AND RESPONSIBILITIES

3.1. The Board of Directors provides strategic oversight, ensures alignment of this Policy with the Company's objectives, and approves any amendments or updates.

3.2. The Chief Executive Officer (CEO) is ultimately accountable for the protection of information assets and for ensuring that sufficient resources are allocated to implement this Policy effectively.

3.3. The Chief Technology Officer (CTO) is responsible for establishing, implementing, and monitoring the information security framework, reporting on risks and incidents to the Board, and ensuring compliance with regulatory requirements.

3.4. The IT and Security Team is responsible for deploying, maintaining, and monitoring technical and physical security controls, incident detection and response measures, and regular vulnerability assessments.

3.5. The Compliance Team is responsible for integrating information security into corporate governance, conducting periodic audits, and ensuring that all practices comply with applicable laws, regulations, and licensing obligations.

3.6. Department Heads are responsible for implementing this Policy within their respective business units, ensuring that employees and contractors comply with the established controls, and reporting any security concerns to the Compliance Officer or other designated governance body responsible for information security.

3.7. All Employees, Contractors, and Third Parties granted access to Company systems or information are required to comply with this Policy, participate in mandatory training programs, promptly report any suspected or actual security incidents, and support the Company's commitment to safeguarding information.

3.8. Failure to comply with the obligations set out in this Policy may result in disciplinary measures, termination of employment or contract, and, where applicable, legal action.

4. BASIC PRINCIPLES FOR INFORMATION SECURITY

4.1. The Company shall protect all critical information and technology assets against potential cybersecurity, physical, and operational threats, ensuring confidentiality, integrity, and availability at all times.

4.2. The Company shall ensure that all employees, contractors, and third parties who have access to Company systems or sensitive information receive mandatory security awareness training, maintain appropriate levels of knowledge, and apply such knowledge to protect Company assets.

4.3. The Company shall implement adequate technical, organizational, and procedural controls based on risk assessments, ensuring that security mechanisms are proportionate to identified threats and vulnerabilities.

4.4. The Company shall maintain and continuously improve prevention, detection, response, analysis, recovery, and investigation capabilities to ensure effective management of security incidents.

4.5. The Company shall establish a process of continuous review and improvement of its information security framework, taking into account changes in technology, emerging threats, and evolving regulatory requirements.

4.6. The Company shall ensure strict compliance with all applicable laws, regulations, licensing requirements, and contractual obligations relating to information security and data protection.

4.7. All employees, contractors, and third parties shall acknowledge that safeguarding Company information is a shared responsibility, and they shall act in accordance with the principles set out in this Policy.

5. MANAGING INFORMATION

5.1. The Company shall establish and maintain clear standards for information classification and handling, ensuring that all information assets are assigned an appropriate classification level based on sensitivity, confidentiality, and regulatory requirements.

5.2. All employees, contractors, and third parties shall handle information strictly in accordance with its classification level and shall apply the prescribed safeguards for storage, transmission, sharing, and disposal.

5.3. The Company shall maintain a Records Retention Schedule that defines the minimum and maximum retention periods for each category of information and prescribes the method of secure disposal, archiving, or permanent preservation.

5.4. All employees and contractors shall comply with the Records Retention Schedule and shall not retain or destroy information outside of the prescribed requirements.

5.5. Information Asset Owners shall ensure that information assets under their control are properly classified, documented, protected, and regularly reviewed for accuracy and compliance.

5.6. All employees, contractors, and third parties acknowledge that unauthorized alteration, destruction, or disclosure of information assets is strictly prohibited and may result in disciplinary, contractual, or legal action.

6. INFORMATION SECURITY CONTROLS AND RISK MANAGEMENT

6.1. The Company shall identify, assess, and manage information security risks through a structured and documented risk management process.

6.2. Risk assessments shall be conducted at least annually, and additionally following significant changes to infrastructure, operations, technology, or applicable regulations.

6.3. The Company shall implement controls designed to prevent, detect, and mitigate information security risks, including but not limited to:

- a) cyber threats such as malware, phishing, denial of service, and ransomware;
- b) risks associated with system incompatibility, outdated software, and lack of updates;
- c) risks arising from adoption of new technologies, including data migration and system integration;
- d) risks caused by poor data quality, inaccuracies, or errors in decision-making;
- e) risks related to unauthorized access, weak authentication, or misuse of physical facilities.

6.4.4. The Company shall classify risks into digital, operational, and physical categories, ensuring that appropriate mitigation measures are applied to each class.

6.5. All employees, contractors, and third parties shall promptly report any identified or suspected risks, vulnerabilities, or weaknesses to the Information Security Team.

6.6. The Chief Technology Officer, together with the Compliance Officer, shall review the Risk Register, evaluate mitigation measures, and submit periodic reports to the Chief Executive Officer (CEO).

6.7. The Company acknowledges that residual risks may remain despite the implementation of controls, and it shall take all reasonable steps to ensure that such risks are reduced to an acceptable level.

7. ACCESS CONTROL

7.1. Access to Company systems, applications, and information shall be granted strictly on a “need-to-know” and “least privilege” basis, and only to individuals with a legitimate business requirement.

7.2. All user accounts shall be unique, assigned to a single individual, and protected with strong authentication. Multi-factor authentication (MFA) shall be mandatory for all administrative, privileged, or sensitive accounts. Sharing of credentials is strictly prohibited.

7.3. Access rights shall be reviewed regularly, at least quarterly, to ensure alignment with current roles and responsibilities. All access shall be promptly revoked upon termination, resignation, role change, or when no longer required for business purposes. Temporary access shall be limited in scope and duration and documented for auditing purposes.

7.4. Employees, contractors, and third parties shall immediately report any suspected or actual unauthorized access to the Information Security Team. The Company shall maintain and review audit logs of access to critical systems and sensitive data to detect and respond to security anomalies.

7.5. Any violation of access control requirements shall be treated as a serious security incident and may result in disciplinary action, termination of contract, or legal consequences.

8. TRAINING AND AWARENESS

8.1. All employees, contractors with access to Company systems or information, shall complete mandatory information security, data protection, and records management training upon induction and at least once every two years thereafter.

8.2. The Company shall conduct ongoing awareness campaigns to reinforce secure behaviours, inform personnel of emerging threats, and provide guidance on applying information security controls in daily operations.

8.3. Employees, contractors, and third parties with privileged or sensitive roles shall receive specialized training appropriate to the level of access and responsibility assigned to them.

8.4. All personnel shall acknowledge their understanding of the Policy and accept responsibility for compliance with security procedures and reporting obligations.

9. DATA PROTECTION AND PRIVACY

- 9.1. All personal and sensitive data shall be collected, processed, stored, and transmitted in accordance with applicable data protection laws, regulations, and licensing requirements.
- 9.2. Sensitive information shall be protected using strong encryption both in transit (e.g., TLS/SSL) and at rest (e.g., AES-256 or equivalent).
- 9.3. Data retention periods shall be enforced according to the Records Retention Schedule, and expired data shall be securely deleted, anonymized, or archived as required.
- 9.4. Any transfer of data to third parties shall be governed by contractual obligations and technical safeguards ensuring compliance with this Policy and applicable laws.
- 9.5. Employees, contractors, and third parties shall immediately report any suspected or actual data breaches or violations of data protection requirements to the Information Security Team.

10. NETWORK AND SYSTEM SECURITY

- 10.1. The Company shall implement appropriate technical measures, including firewalls, intrusion detection/prevention systems (IDS/IPS), and anti-malware solutions, to protect all networks and systems.
- 10.2. Systems, applications, and devices shall be kept up to date with security patches and updates, applied promptly following vendor release.
- 10.3. The Company shall conduct periodic penetration testing and vulnerability assessments to identify and remediate security weaknesses.
- 10.4. Logging and monitoring of critical systems shall be maintained to detect, investigate, and respond to suspicious activities.

11. INCIDENT MANAGEMENT

- 11.1. All employees, contractors with access to Company systems or information, shall immediately report any suspected or actual security incidents, including unauthorized access, data breaches, system failures, or operational disruptions, to the Information Security Team.
- 11.2. The Company shall maintain a documented Incident Response Plan (IRP) that defines roles, responsibilities, and procedures to ensure prompt detection, investigation, containment, remediation, and root cause analysis of all security incidents.
- 11.3. Significant incidents, including those affecting customer data, financial systems, or regulatory compliance, shall be escalated to senior management and reported to the Curaçao Gaming Authority within the required regulatory timeframes.
- 11.4. Lessons learned from incidents shall be documented, analyzed, and incorporated into preventive measures, policies, and controls to minimize the likelihood of recurrence and strengthen the overall security posture.
- 11.5. The Company shall review incident trends periodically and adjust security measures, training, and controls as necessary to address emerging threats and vulnerabilities.

12. BUSINESS CONTINUITY AND DISASTER RECOVERY

12.1. The Company shall maintain a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to ensure resilience of critical operations in the event of disruption.

12.2. Critical systems and data shall be backed up regularly, and recovery procedures shall be tested periodically for effectiveness.

12.3. Plans shall be reviewed and updated at least annually or upon significant organizational, operational, or technological changes.

13. COMPLIANCE AND MONITORING

13.1. The Company shall conduct regular internal audits and reviews to ensure compliance with this Policy, applicable laws, regulations, and licensing requirements.

13.2. Independent external audits may be performed to verify the effectiveness of the information security framework and demonstrate regulatory compliance.

13.3. Non-compliance with this Policy, whether by employees, contractors, or third parties, may result in disciplinary measures, termination of employment or contract, and, where applicable, legal action.

13.4. The Company shall maintain records of compliance activities, audit findings, and corrective actions taken to address identified gaps or risks.

14. POLICY REVIEW

14.1. This Policy shall be reviewed periodically to ensure it remains effective, relevant, and compliant with applicable laws, regulations, licensing requirements, and technological or organizational changes.

14.2. Updates to the Policy shall be approved by the Board of Directors or equivalent governing body.

14.3. All relevant stakeholders, including employees, contractors, and third parties, shall be informed of any changes or updates to the Policy.

14.4. The Company shall ensure that historical versions of the Policy are archived for reference, compliance verification, and regulatory purposes.