

INFORMATION SECURITY POLICY

I. INTRODUCTORY PROVISIONS AND APPLICABILITY.

1. This Information Security Policy (hereinafter - **"Policy"**) is provided and adopted by **1Win N.V.**, a limited liability company duly incorporated under the laws of Curacao, with company number 147039 and its registered business address at Dr. H. Fergusonweg 1, Curacao (hereinafter - **"Company"**).
2. Information constitutes one of the Company's most significant and valuable assets. In the course of providing online gaming services, ensuring compliance with applicable regulatory requirements, and conducting internal business operations, the Company relies upon both physical resources and information technology systems for the storage, management, processing, and dissemination of information. The protection of these assets is essential to maintain stakeholder trust, ensure the continuity of operations, and safeguard the integrity and reputation of the Company.
3. By adopting this Policy, the Company adheres to its obligations arising under the requirements of the Curaçao Gaming Authority (CGA), the internationally accepted standards, including ISO/IEC 27001, as well as the guidelines issued by the Central Bank of Curacao and Sint Maarten.
4. This Policy is adopted in order to maintain the confidentiality, integrity, and availability of the Company's information systems and data, thereby ensuring the lawful, secure, and responsible conduct of its operations, as well as to reaffirm the commitment to protecting all information assets from unauthorized access, disclosure, modification, or destruction.
5. The scope of this Policy encompasses all forms and formats of information, including, but not limited to, electronic data, paper-based records, verbal communications, images, audio and video materials, and any other medium utilized for the creation, storage, processing, or transmission of information. This Policy applies to all Company assets, including hardware, software, networks, databases, cloud environments, mobile devices, and physical infrastructure used for processing, storing, or transmitting information.
6. The Policy governs all business functions and operational activities of the Company, including, without limitation, online gaming services, payment and transaction processing, customer support, marketing and promotional initiatives, financial management, human resources administration, and regulatory or statutory reporting. The Policy shall apply in all environments where Company information is accessed, processed, or transmitted, including remote work settings, third-party hosted platforms, and cross-border data exchanges.
7. This Policy is applicable to all Company personnel, including employees, contractors, consultants, temporary and agency staff, interns, volunteers, third-party service providers, and any other individuals or entities granted access to the Company's information assets, systems, or facilities (hereinafter also referred as "third parties granted access").

8. Adherence to this Policy is mandatory for all covered parties and constitutes a binding contractual obligation. Compliance shall be enforced through continuous monitoring, periodic audits, and the application of disciplinary or contractual measures as deemed appropriate.

II. GENERAL INFORMATION SECURITY PRINCIPLES

1. The Company is dedicated to ensuring the comprehensive protection of all critical information and technology assets from cybersecurity, physical, and operational risks. This commitment extends to maintaining, at all times, the confidentiality, integrity, and availability of such assets.
2. All employees, contractors, and third parties with access to Company systems or sensitive data shall be required to complete mandatory information security awareness training, maintain an appropriate and up-to-date understanding of security practices, and apply that knowledge diligently in the course of their professional activities to safeguard Company's resources.
3. The Company shall adopt and enforce a comprehensive set of technical, organizational, and procedural safeguards, established through systematic risk assessment processes. These safeguards shall be proportionate to the nature and severity of identified risks, ensuring an effective balance between operational efficiency and information security.
4. The Company shall develop, maintain, and continuously enhance its capabilities for preventing, detecting, responding to, analyzing, mitigating, and investigating security incidents, ensuring timely and effective resolution of any events that may compromise information assets.
5. The Company shall engage in an ongoing process of review and refinement of its information security management framework, taking into account technological evolution, emerging threat landscapes, and changing legal or regulatory obligations.
6. The Company shall fully comply with all applicable legislation, regulatory directives, licensing conditions, and contractual requirements relating to information security and data protection.
7. Each employee, contractor, and third party granted access is expected to share responsibility for the protection of Company's information assets and to act in full alignment with the principles, objectives, and obligations set forth in this Policy.

III. GENERAL ROLES AND RESPONSIBILITIES OF THE COMPANY

1. The key persons of the Company, as well as the Company's departments and other personnel granted access to the information specified in this Policy, have specific responsibilities in order to maintain compliance with this Policy and development of information security processes.
2. Non-compliance with the provisions of this Policy shall constitute a breach of contractual and/or employment obligations and may result in disciplinary action,

termination of employment or contractual relationship, and, where applicable, civil or criminal proceedings in accordance with governing laws.

3. These responsibilities are included, but not limited:

- to exercise strategic oversight of the Company's information security posture, ensuring that this Policy remains aligned with the Company's overall objectives and approving any subsequent amendments or revisions (Board of Directors or equivalent governing authority);
- To manage the protection of the Company's information assets and to ensure that adequate financial, technological, and human resources are allocated to enable the effective implementation of this Policy (Chief Executive Officer);
- To establish, implement, and supervise the Company's information security framework (Chief Technology Officer).
- To ensure that all identified risks and incidents are appropriately reported to the chief management and that the Company's security practices remain in full compliance with applicable regulatory and licensing requirements (Chief Technology Officer).
- To implement, maintain, and conduct the monitoring of all technical and physical security controls, including mechanisms for threat detection, incident response, and regular vulnerability assessments, as well as to ensure the resilience of the Company's information systems (IT and Security Department);
- To oversee the integration of information security principles into the Company's governance structure, conduct periodic compliance audits, and ensure that all operations adhere to relevant statutory, regulatory, and licensing obligations (Compliance Department);
- To ensure the effective implementation of this Policy within business departments of the company;
- To enforce compliance among employees and contractors, promoting awareness of security responsibilities, and reporting any actual or suspected breaches or irregularities to the Compliance Officer or other designated authority overseeing information security governance.

4. All employees, contractors, and third parties granted access to Company systems, data, or facilities are required to comply fully with this Policy, should participate in all mandatory information security training programs, and promptly report any suspected or confirmed security incidents. They are expected to actively support the Company's ongoing efforts to safeguard its information assets.

IV. INFORMATION MANAGEMENT AND CONTROL

1. The Company shall develop, implement, and maintain formal standards governing the classification and handling of all information assets. Each asset shall be assigned an appropriate classification level reflecting its sensitivity, confidentiality, and any applicable legal or regulatory obligations.

2. All employees, contractors, and third-party partners shall manage and process information strictly in accordance with its designated classification level. Appropriate safeguards must be applied during storage, transmission, sharing, and disposal.

3. Designated information asset owners shall ensure that all assets under their control are accurately classified, properly documented, adequately protected, and periodically reviewed to confirm ongoing compliance with Company's internal policies, as well as with applicable regulations.

4. The Company shall establish and maintain a comprehensive Records Retention Schedule defining the minimum and maximum retention periods applicable to each category of information. This schedule shall prescribe secure methods for the archiving, permanent preservation, or irreversible destruction of records, as appropriate. All employees and contractors are required to adhere strictly to the Records Retention Schedule. The unauthorized retention, deletion, or destruction of information outside the prescribed parameters is expressly prohibited.

5. All employees, contractors, and third parties acknowledge that any unauthorized alteration, destruction, or disclosure of information assets constitutes a serious violation of this Policy. Such actions may result in disciplinary measures, termination of employment or contractual engagement, and, where applicable, legal action.

V. ACCESS MANAGEMENT AND CONTROL REQUIREMENTS

1. Access to the Company's systems, applications, networks, and information assets shall be strictly controlled and granted solely on the principles of **"need-to-know"** and **"least privilege."** Authorization shall be provided only to individuals with a verified and legitimate business requirement, in accordance with their designated roles and responsibilities.

2. Each user shall be assigned a unique account that is traceable to a single identifiable individual. All accounts shall be protected through the use of strong authentication mechanisms, and multi-factor authentication (MFA) shall be mandatory for administrative, privileged, or otherwise sensitive access. The sharing or reuse of credentials, passwords, or authentication tokens is strictly prohibited under all circumstances.

3. Access rights shall be reviewed at regular intervals to ensure continued appropriateness and consistency with current job functions. All access privileges shall be immediately revoked upon employment termination, resignation, reassignment, or any change in role that renders such access unnecessary. Temporary or exceptional access shall be time-bound, limited in scope, and formally documented for accountability and audit purposes.

4. All employees, contractors, and third parties granted access must promptly report any suspected or confirmed unauthorized access or misuse of credentials to the Information Security Department of the Company. The Company shall maintain comprehensive audit logs of access to critical systems and sensitive information, and such logs shall be periodically reviewed to detect anomalies and support incident response and investigations.

5. Any breach or attempted circumvention of access control requirements shall constitute a serious security violation. Violations may result in disciplinary action, termination of employment or contractual relationship, and, where applicable, legal or

regulatory action in accordance with governing laws.

VI. RISK MANAGEMENT

1. The Company shall establish and maintain an information security risk management framework designed to identify, evaluate, and manage risks that may impact the confidentiality, integrity, and availability of its information assets and supporting systems.
2. Comprehensive risk assessments shall be conducted on an annual basis, and additionally whenever significant modifications occur to the Company's infrastructure, operational processes, technological environment, or regulatory landscape. Such assessments shall ensure that emerging threats and changes in business context are promptly identified and addressed.
3. The Company shall implement a range of preventive, detective, and corrective controls to manage information security risks effectively. These controls shall include, but not be limited to, measures designed to address:
 - **Cybersecurity threats**, such as malware, phishing, denial-of-service (DoS), and ransomware attacks;
 - **Technological risks**, including system incompatibility, software obsolescence, and lack of critical updates;
 - **Innovation-related risks** arising from the deployment of new technologies, system integrations, or data migrations;
 - **Data integrity risks**, including poor data quality, inaccuracies, and decision-making errors;
 - **Access and physical security risks**, including unauthorized access, insufficient authentication, and misuse of facilities or equipment.
4. Identified risks shall be classified into digital, operational, and physical categories. The Company shall ensure that each class of risk is addressed through tailored mitigation strategies proportionate to its likelihood and potential business impact.
5. The Chief Technology Officer, in coordination with the Compliance Officer, shall be responsible for maintaining and reviewing the Company's Risk Register, assessing the effectiveness of mitigation measures, and submitting regular reports and recommendations to the Chief Executive Officer and the Board of Directors as appropriate.
6. The Company acknowledges that certain residual risks may persist despite the implementation of comprehensive security controls. The Company shall ensure that such residual risks are continuously evaluated, monitored, and maintained at a level deemed acceptable by the Company.
7. All employees, contractors, and third parties granted access are required to immediately report any identified or suspected risks, vulnerabilities, or weaknesses to the Information Security Department for investigation and remediation.

VII. DATA PROTECTION AND SYSTEM SECURITY MEASURES

1. All personal, confidential, and sensitive data shall be collected, processed, stored, and transmitted strictly in accordance with applicable data protection legislation, regulatory frameworks, and licensing requirements. The Company shall ensure that data processing activities adhere to the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, and accountability.
2. Sensitive and personal information shall be secured through the implementation of robust encryption mechanisms. Data in transit shall be protected using protocols such as TLS/SSL, and data at rest shall be encrypted using AES-256 or an equivalent industry-standard encryption algorithm. Additional security measures shall be employed to prevent unauthorized access, alteration, or disclosure.
3. Data retention shall be managed in strict alignment with the Company's Records Retention Schedule. Information exceeding its designated retention period shall be securely deleted, irreversibly anonymized, or archived in accordance with established procedures and applicable legal requirements.
4. Any transfer, sharing, or processing of data by third parties shall be subject to formal contractual arrangements incorporating data protection clauses and technical safeguards that ensure full compliance with this Policy and all applicable legal standards. Third parties granted access shall be required to demonstrate equivalent levels of protection and accountability.
5. All employees, contractors, and third parties granted access are obligated to immediately report any suspected or confirmed data breaches, privacy violations, or non-compliance incidents to the Information Security Department. Such incidents shall be promptly investigated, documented, and remediated in accordance with the Company's inner policies and incident report procedures.
6. The Company shall deploy and maintain a comprehensive set of technical security controls designed to protect its network infrastructure, information systems, and related assets from internal and external threats. Such measures shall include, but not be limited to, firewalls, intrusion detection and prevention systems (IDS/IPS), anti-malware and endpoint protection solutions, as well as network segmentation and secure configuration management practices.
7. All systems, applications, and connected devices shall be maintained in a secure and up-to-date state. Security patches, firmware updates, and vendor-issued fixes shall be applied promptly following their release to minimize exposure to known vulnerabilities.
8. The Company shall conduct periodic penetration testing, vulnerability assessments, and other proactive security evaluations to identify potential weaknesses across its technological environment. Identified vulnerabilities shall be prioritized, documented, and remediated in a timely manner based on their assessed severity and business impact.
9. Continuous logging and real-time monitoring of critical systems and network activities shall be implemented to detect, investigate, and respond to suspicious or anomalous

events. Audit logs shall be retained and regularly reviewed to support incident analysis, forensic investigation, and compliance with applicable security and regulatory requirements.

VIII. INCIDENT REPORT MANAGEMENT. BUSINESS CONTINUITY AND DISASTER RECOVERY

1. All employees, contractors, and third parties with access to the Company's systems or information assets are required to immediately report any suspected or confirmed security incident to the Information Security Department of the Company. Such incidents include, but are not limited to, unauthorized access, data breaches, malware infections, system failures, or any operational disruptions that may compromise the confidentiality, integrity, or availability of information or services.

2. The Company shall establish and maintain a formally documented Incident Response Plan (IRP) defining clear roles, responsibilities, escalation paths, and procedures for the effective management of security incidents. The IRP shall ensure the timely detection, investigation, containment, eradication, recovery, and root cause analysis of all identified incidents.

3. Any incident deemed significant, particularly those impacting customer data, financial systems, or regulatory compliance, shall be immediately escalated to senior management. Such incidents shall also be reported to the Curacao Gaming Authority (CGA) or other competent authorities within the prescribed regulatory timeframes and in accordance with applicable laws and licensing requirements.

4. Following the resolution of each incident, the Company shall conduct a post-incident review to document lessons learned, identify root causes, and recommend appropriate corrective and preventive measures. These findings shall be integrated into updated policies, controls, and training programs to reduce the likelihood of recurrence and enhance the Company's overall security resilience.

5. The Company shall perform periodic reviews and trend analyses of security incidents to identify recurring patterns, emerging threats, and systemic weaknesses. Based on these analyses, security measures, technical controls, and awareness programs shall be refined and strengthened to ensure a proactive and adaptive approach to risk management.

6. The Company shall develop, implement, and maintain a comprehensive Business Continuity Plan ("BCP") and Disaster Recovery Plan ("DRP") designed to ensure the continued availability and resilience of critical business operations, systems, and services in the event of a disruption, emergency, or catastrophic incident. These plans shall define the procedures, responsibilities, and resources required to maintain essential functions and restore normal operations within acceptable timeframes.

7. The Company shall ensure that all critical systems, applications, and data are subject to regular, secure, and verifiable backup processes. Recovery procedures shall be periodically tested and validated to confirm their effectiveness, accuracy, and alignment

with operational and business continuity objectives. Backup data shall be protected with appropriate encryption and stored in secure, access-controlled environments.

8. The BCP and DRP shall be reviewed, tested, and updated at least annually, or whenever significant organizational, operational, regulatory or technological changes occur.

IX. PERSONNEL TRAINING AND AWARENESS

1. All employees, contractors, and third parties with access to the Company's systems, networks, or information assets shall be required to complete mandatory training programs covering information security, data protection, and records management upon commencement of their engagement with the Company and at least once every two years thereafter.

2. The Company shall implement and maintain continuous awareness programs to promote secure behavior, enhance understanding of information security principles, and educate personnel about emerging threats, best practices, and procedural updates. These initiatives shall ensure that security controls are effectively understood and applied in daily business operations.

3. Employees, contractors, and third parties with granted access and privileged, sensitive, or high-risk roles shall receive targeted and role-specific training aligned with the level of access and responsibility entrusted to them. Such training shall emphasize secure system administration, privileged account management, and regulatory compliance obligations.

4. All personnel shall formally acknowledge their understanding of this Policy and their commitment to comply with established information security requirements. Each individual shall accept personal responsibility for adhering to all applicable procedures, maintaining the confidentiality and integrity of information, and promptly reporting any suspected or actual security incidents in accordance with Company's inner policies and procedures.

X. COMPLIANCE AND AUDIT

1. The Company shall conduct regular internal audits and compliance reviews to verify adherence to this Policy, as well as to all applicable laws, regulations, standards, and licensing obligations. These reviews shall evaluate the adequacy and effectiveness of implemented security controls and identify areas requiring improvement.

2. The Company may engage independent external auditors to perform periodic evaluations of its information security management framework. Such assessments shall provide objective verification of the framework's effectiveness and demonstrate ongoing regulatory and contractual compliance to relevant authorities, partners, and stakeholders.

3. Any instance of non-compliance with this Policy by employees, contractors, or third parties granted access shall be regarded as a serious violation of this Policy. Depending on the severity of the breach, appropriate measures may include disciplinary action, termination of employment or contractual engagement, and, where applicable, civil or criminal proceedings in accordance with governing laws and contractual obligations.

4. The Company shall maintain comprehensive and verifiable records of compliance activities, including audit results, review findings, and corrective actions implemented to remediate identified weaknesses or control deficiencies. Such records shall serve as evidence of due diligence and accountability in maintaining the integrity of the Company's information security procedures.

XI. POLICY REVIEW AND MAINTENANCE

1. This Policy shall be periodically reviewed and evaluated to ensure its ongoing effectiveness, applicability, and alignment with current legal, regulatory, and licensing requirements, as well as with technological advancements and organizational developments. The review process shall confirm that the Policy continues to adequately support the Company's strategic objectives and risk management framework.

2. Any amendments, updates, or substantial revisions to this Policy shall be formally reviewed and approved by the Board of Directors or an equivalent governing authority responsible for corporate oversight and information security governance.

3. All relevant stakeholders, including employees, contractors, and third parties granted access, shall be promptly informed of any approved modifications to this Policy. The Company shall ensure that updated versions are readily accessible and that affected personnel acknowledge their understanding and compliance with the revised provisions.

4. The Company shall maintain archived copies of all previous versions of this Policy for purposes of auditability, compliance verification, and regulatory reference. Version control procedures shall be applied to track the history of amendments, ensuring transparency and accountability in the policy management process.

THIS INFORMATION SECURITY POLICY IS REVIEWED AND APPROVED BY:



Vivian Ersilia, o.b.o SMES Solutions for Management and Employment Support N.V.
Managing Director

Date: September 15, 2025