



INFORMATION SECURITY POLICY

Version: 2.1

XZ Solutions B.V.
Effective Date: 10.10.2024



1. PURPOSE

The purpose of this Information Security Policy is to establish a structured and comprehensive framework to ensure that all information and data assets under the control of XZ Solutions B.V., a duly licensed online gambling operator pursuant to the laws of Curaçao, are safeguarded against unauthorized access, misuse, loss, or destruction. This Policy delineates the Operator's commitment to maintaining the confidentiality, integrity, and availability of all data assets, and to preserving regulatory compliance in all operational aspects.

2. SCOPE

This Policy applies without limitation to all directors, officers, employees, consultants, contractors, and any third parties who have access to XZ Solutions B.V.'s data or information systems. It encompasses all data, information technology assets, hardware, software, communications networks, and cloud-based services owned, leased, or otherwise controlled by the Company.

3. LEGAL AND REGULATORY COMPLIANCE

XZ Solutions B.V. recognizes and adheres to its legal and regulatory obligations, including compliance with the provisions of the National Ordinance on Data Protection (Landsverordening bescherming persoonsgegevens), the requirements established by the relevant Licensing Authority of Curaçao, and where applicable, the General Data Protection Regulation (EU 2016/679) (GDPR). The Company further complies with obligations under anti-money laundering legislation and any other laws governing the responsible operation of remote gaming services.

4. INFORMATION SECURITY OBJECTIVES

The objectives of this Policy are: (a) to protect information systems and data assets from security threats; (b) to ensure the availability, reliability, and integrity of all IT operations; (c) to foster a culture of security awareness and proactive risk management; (d) to comply with all applicable legal, regulatory, and contractual requirements; and (e) to assure stakeholders of the Company's robust and responsible data governance practices.

5. GOVERNANCE AND ACCOUNTABILITY

The Board of Directors shall have ultimate accountability for the effectiveness of this Policy. CTO shall be responsible for its day-to-day implementation, enforcement, and revision. All staff members are individually and collectively responsible for complying with the provisions of this Policy, and for reporting any actual or suspected breaches.

6. CLASSIFICATION OF INFORMATION

Information assets shall be identified, documented, and classified in accordance with their sensitivity and criticality to business operations. The following classification levels shall apply: (a) Public; (b) Internal; (c) Confidential; (d) Restricted/Sensitive – including, without limitation, customer personal data, KYC documentation, and financial transaction records.



7. ACCESS MANAGEMENT

Access to Company systems and information shall be granted on a strict need-to-know and least-privilege basis, commensurate with the individual's role and responsibilities. All access rights must be reviewed at regular intervals and revoked immediately upon termination of employment or contract.

8. DATA SECURITY AND ENCRYPTION

All sensitive and confidential data shall be encrypted in transit and at rest, using encryption protocols conforming to industry standards. Passwords shall be securely hashed, and no plaintext passwords shall be stored. Secure key management procedures must be implemented and maintained.

9. NETWORK SECURITY AND SYSTEM HARDENING

The Company shall deploy robust security infrastructure including firewalls, intrusion detection systems (IDS), and anti-malware solutions. Regular vulnerability assessments and penetration testing must be conducted, and system patches must be applied promptly. Administrative access shall be segregated from general access functions.

10. THIRD-PARTY AND VENDOR SECURITY

All third-party vendors or service providers who process or have access to Company data must sign binding data protection agreements and undergo due diligence prior to engagement. Subcontracting of data processing functions is prohibited without the Company's prior written authorization and regulatory notification where required.

11. SECURITY INCIDENT MANAGEMENT

All actual or suspected information security incidents shall be immediately reported to the CTO. The Company shall implement and maintain an Incident Response Plan to ensure timely and effective handling, documentation, and remediation of all such incidents, including notification to the regulator and affected data subjects within the legally prescribed timeframes.

12. BUSINESS CONTINUITY AND DISASTER RECOVERY

A Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) shall be implemented, reviewed annually, and tested periodically. These plans must ensure that critical business functions and services can be restored within acceptable timeframes in the event of a significant disruption or disaster.

13. TRAINING AND SECURITY AWARENESS

All personnel shall receive mandatory information security training upon commencement of employment and at least annually thereafter. Specialized training shall be provided to staff members with access to critical systems or sensitive data.



14. AUDIT, MONITORING AND CONTINUOUS IMPROVEMENT

Information systems shall be continuously monitored to detect unauthorized access or misuse. Regular audits shall be carried out by internal and/or external auditors to verify compliance with this Policy and applicable laws. Identified gaps shall be remediated without undue delay.

15. REVIEW AND AMENDMENT

This Policy shall be reviewed annually or upon significant operational, legal, or technological changes. Amendments shall require formal approval by the Board of Directors and shall be communicated to all affected parties.

16. ENFORCEMENT AND SANCTIONS

Non-compliance with this Policy shall result in disciplinary action, up to and including termination of employment or contract, and may expose the offending party to civil or criminal liability. The Company reserves the right to pursue legal remedies against any individual or entity that compromises its information security framework.