

**Information Security Policy**  
**WILLX NV**  
**Effective Date - 01.01.2025**  
**Version 1.0**

### **Purpose**

The purpose of this policy is to establish a framework for managing and protecting the confidentiality, integrity, and availability of information assets at **WILLX NV**, in compliance with ISO 27001 standards. This policy ensures secure operations, protection of sensitive data, customer data protection, and compliance with regulatory requirements, including Curaçao Gaming Control Board (GCB) License Requirements and GDPR, and other jurisdictional data protection laws.

### **Scope**

This policy applies to all employees, contractors, third-party vendors, stakeholders and any other individuals or entities who access, process, or manage information assets related to **WILLX NV**'s operations. It includes physical, digital, and cloud-based systems, gaming platforms, payment processing, and customer information, whether stored digitally, transmitted over networks, or maintained in physical format.

## **1. Information Security Objectives**

- Ensure the confidentiality, integrity and availability of customer and company business data.
- Protect information systems from unauthorized access, disclosure, modification of sensitive information, breaches and fraud.
- Guarantee the integrity and reliability of data and systems.
- Maintain continuous availability of gaming operations and associated services.
- Comply with ISO 27001 requirements, eGaming regulations, and relevant data protection laws.

## **2. Key Principles**

- **Confidentiality:** Protect sensitive data from unauthorized access or disclosure.
- **Integrity:** Prevent unauthorized modifications to data and ensure accuracy.

- **Availability:** Ensure systems and information are available to authorized personnel when required.

### 3. Roles and Responsibilities

- **Information Security Officer (ISO):** Responsible for implementing and monitoring the Information Security Management System (ISMS), and continuous improvement of security controls.
- **Department Heads:** Accountable for enforcing security practices within their teams.
- **IT Department:** Ensures technical controls like firewalls, encryption, and monitoring systems are implemented and maintained.
- **All Employees and Contractors:** Responsible for adhering to the security policies and reporting potential incidents.

### 4. Risk Management

- Conduct regular risk assessments to identify and address vulnerabilities in systems, networks, and processes.
- Apply a risk treatment plan to mitigate identified risks, following ISO 27001 guidelines.
- Document and review risks annually or after any significant changes in operations or threats.

### 5. Security Controls

#### 5.1. Access Control

- Use role-based access control (RBAC) to restrict access to systems and data.
- Implement multi-factor authentication (MFA) for all sensitive systems.
- Enforce password policies that include complexity requirements and expiration intervals.

#### 5.2. Data Protection

- Encrypt sensitive data at rest (AES-256) and in transit (TLS).
- Regularly back up critical systems and store backups securely offsite.
- Anonymize or pseudonymize customer data where possible.

#### 5.3. Network Security

- Deploy firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).
- Conduct regular penetration testing and vulnerability assessments.
- Protect against Distributed Denial of Service (DDoS) attacks using dedicated mitigation solutions.

#### **5.4. Third-Party Management**

- Require all third-party vendors to comply with regulatory standards.
- Conduct due diligence and security audits of third-party providers, including gaming software vendors and payment processors.
- Maintain contracts with clear terms regarding security, confidentiality, and data protection.

#### **5.5. Incident Management**

- Maintain an Incident Response Plan (IRP) to address security breaches, fraud, or cyberattacks.
- Ensure incidents are logged, analyzed, and resolved promptly.
- Notify relevant stakeholders and regulatory authorities in compliance with legal requirements (e.g., GDPR breach notification).

#### **5.6. Physical Security**

- Secure server rooms and offices with access controls such as key cards.
- Ensure physical data storage (e.g., backups) is stored in secure, climate-controlled locations.
- Use CCTV surveillance for monitoring critical infrastructure.

### **6. Business Continuity and Disaster Recovery**

- Maintain a documented Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).
- Test BCP and DRP annually to ensure preparedness for disruptions.
- Ensure backups are regularly tested for data integrity and restoration accuracy.

### **7. Compliance and Audits**

- Comply with ISO 27001 requirements and regulatory obligations such as Gaming Control Board (GCB) License Requirements and GDPR.

- Conduct internal and external audits annually to assess ISMS performance.
- Maintain all audit documentation and evidence for regulatory review.

## **8. Employee Training and Awareness**

- Provide regular security awareness training to employees and contractors.
- Include topics such as phishing, password management, and social engineering in training programs.
- Ensure employees are familiar with reporting protocols for security incidents.

## **9. Policy Review and Updates**

This Information Security Policy will be reviewed annually or as needed due to changes in regulations, operations, or identified risks. Updates will be approved by the Information Security Officer and executive management.

## **10. Enforcement**

Non-compliance with this policy may result in disciplinary action, including termination of employment or contracts, and potential legal consequences.

Employees and contractors are required to acknowledge and comply with this policy as a condition of their role within the company.