

Evelnex B.V.

Information Security Policy

Version 2.0

1. Purpose

This Information Security Policy establishes the framework for protecting Evelnex B.V.'s information and IT systems. Its purpose is to safeguard the **confidentiality, integrity, and availability** of our data and infrastructure.

This document outlines the security rules and expected behaviors for all personnel. It also details how the company protects against **external threats** (like phishing, hacking, and fraud) and **internal threats** (like data mismanagement, theft, or accidental leaks).

2. Scope

This policy applies to:

- **All Personnel:** All employees, contractors, vendors, and third-party partners who interact with the company's IT systems.
- **All Systems & Data:** All data, systems, applications, and network resources owned, managed, or operated by Evelnex B.V. or its affiliated companies.
- **All External Stakeholders:** Any external party, including customers, interacting with Evelnex B.V.'s platform or digital infrastructure.

3. Internal Information Security Guidelines

3.1 Acceptable Use

- All company computing resources must be used for company-approved, business-related tasks.
- Minimal personal use of company devices is permitted only if it does not interfere with work or compromise security.

3.2 Password Management

- You must use **strong, unique passwords** for all company systems.
- **Multi-Factor Authentication (MFA)** is mandatory for accessing all designated sensitive systems.

3.3 Access Control

- Access to systems and data is granted based on the **principle of least privilege** (meaning, you only get access to what you absolutely need for your job).
- Employee access rights are reviewed regularly and immediately revoked upon termination or a change in role.

3.4 Data Classification and Handling

- Data must be classified into one of three categories: **Confidential, Internal, or Public**.
- All data must be handled according to its classification.
- All Confidential customer and operational data must be **encrypted at rest and in transit**.

3.5 Device and Endpoint Security

- All company-managed devices must have approved antivirus and anti-malware tools installed and kept up-to-date.
- Devices must be **locked when unattended** and receive regular security updates.

3.6 Security Awareness and Training

- All staff must complete **mandatory security awareness training** upon hiring and at least annually thereafter.
- The company will conduct periodic phishing simulations and awareness campaigns to reinforce this training.

3.7 Software Installation

- Installing any new software or applications on company devices is **prohibited** without explicit approval from an Administrator.
- All software downloads require administrator approval.

4. External Threat Protection

4.1 Phishing and Social Engineering

- All email and communication platforms are monitored for suspicious activity.
- Customers are educated on identifying phishing attempts through public awareness on our platform and support channels.

4.2 Scams and Fraud Detection

- We utilize **AI-based fraud detection systems** to monitor gaming behavior for anomalies.
- Financial transactions are actively screened for irregularities using anti-fraud tools.

4.3 Protection Against Hacking

- Our web applications and systems undergo regular **penetration testing** to find vulnerabilities.
- The network is protected by firewalls, intrusion detection/prevention systems (IDS/IPS), and DDoS mitigation tools.

4.4 Secure Software Development

- All code is reviewed, tested, and scanned for vulnerabilities before being deployed.
- An **internal bug bounty initiative** is encouraged to find and fix any potential coding gaps.
- All third-party libraries and dependencies are vetted for security compliance.

5. Incident Response and Reporting

- Any suspected security incident must be **reported immediately** to a Senior Information Security Officer.

- The incident response team will follow established procedures to assess, contain, and remediate the breach.
- Breaches affecting external users (e.g., customers) will be disclosed transparently and in accordance with all regulatory obligations.

6. Regulatory and Legal Compliance

- Evelnex B.V. is committed to full compliance with the **Curaçao Gaming Authority's** requirements and all applicable data protection laws, such as the **GDPR**.
- Regular audits are conducted to ensure we meet all internal and external security standards.

7. Roles and Responsibilities

- **Management:** Responsible for policy enforcement, providing necessary resources, and appointing Senior Officers.
- **Senior Officers:** Responsible for managing the IT Security Team, implementing technical safeguards, monitoring the IT Team, and handling incident reports.
- **IT Security Team:** Responsible for monitoring policy compliance across all staff and ensuring security best practices are applied.
- **All Staff:** Responsible for understanding and complying with this policy, attending mandatory annual training, and reporting all suspicious activity.
- **Vendors & Third Parties:** Must adhere to the security standards defined in their contractual agreements.

8. Policy Review

This policy will be reviewed at least **annually**, or upon any significant changes to the threat landscape, regulatory requirements, or organizational structure.

9. Version Control

The Company is committed to the continuous improvement of its policies. All revisions to this policy are tracked, and the Director must approve all changes.

Version	Date	Approved By
2.0	November 5, 2025	

For Approval