

SDC Studio

Information Security Policy

Table of Contents

SDC STUDIO ERROR! BOOKMARK NOT DEFINED.

INFORMATION SECURITY POLICY 1

1. PURPOSE 3

2. SCOPE 3

3. INTERNAL INFORMATION SECURITY GUIDELINES 3

 3.1 *Acceptable Use*..... 3

 3.2 *Password Management* 3

 3.3 *Access Control* 3

 3.4 *Data Classification and Handling* 4

 3.5 *Device and Endpoint Security*..... 4

 3.6 *Security Awareness and Training* 4

4. EXTERNAL THREAT PROTECTION 4

 4.1 *Phishing and Social Engineering* 4

 4.2 *Scams and Fraud Detection* 4

 4.3 *Protection Against Hacking*..... 4

 4.4 *Secure Software Development*..... 5

 4.5 *Protection Against new Programs* 5

5. INCIDENT RESPONSE AND REPORTING..... 5

6. REGULATORY AND LEGAL COMPLIANCE 5

7. ROLES AND RESPONSIBILITIES..... 5

8. POLICY REVIEW 6

1. Purpose

The purpose of this Information Security Policy is to establish a framework that safeguards the confidentiality, integrity and availability of SDC Studio's IT System. This policy outlines rules and behaviors expected of employees and explains how the company protects both against external threats such as phishing, scams, hacking and other malicious activities and Internal threats such as miss-managing Customers' sensitive data, exploiting, stealing and or leaking Sensitive information

2. Scope

This policy applies to:

All employees, contractors, vendors and third-party partners who will interact directly or indirectly with the company's IT System.

All data, systems, applications and network resources owned, managed, or operated by SDC Studio or any of its Sister-, Mother- or Daughter- companies that has either Direct or Indirect access to company's IT System.

All external stakeholders interacting with SDC Studio's platform or digital infrastructure

3. Internal Information Security Guidelines

3.1 Acceptable Use

All computing resources must be used in compliance with company-approved tasks.

Personal use of company devices must be minimal and must not compromise security.

3.2 Password Management

Strong, unique passwords must be used for all company systems.

Multi-Factor Authentication (MFA) is mandatory for accessing sensitive systems.

3.3 Access Control

Access is granted based on the principle of least privilege.

Employee access is regularly reviewed and revoked upon termination or role change.

3.4 Data Classification and Handling

Data must be classified (Confidential, Internal, Public) and handled accordingly.

Confidential customer and operational data must be encrypted at rest and in transit.

3.5 Device and Endpoint Security

Company-managed antivirus and anti-malware tools must be installed on all devices.

Devices must be locked when unattended and updated regularly.

3.6 Security Awareness and Training

Mandatory security training for all staff upon hiring and annually thereafter.

Phishing simulations and awareness campaigns conducted periodically.

4. External Threat Protection

4.1 Phishing and Social Engineering

All email and communication platforms are monitored for suspicious activity.

External users (customers) are educated on identifying phishing attempts through public awareness efforts on the platform and support channels.

4.2 Scams and Fraud Detection

AI-based fraud detection systems monitor gaming behavior for anomalies.

Financial transactions are screened for irregularities using anti-fraud tools.

4.3 Protection Against Hacking

Web applications and systems undergo regular penetration testing.

Firewalls, intrusion detection/prevention systems (IDS/IPS), and DDoS mitigation tools are employed.

4.4 Secure Software Development

Code is reviewed, tested and scanned for vulnerabilities before deployment.

Internal Bounty Initiative is encouraged to assure any possible Gap in Coding is discovered internally and fixed accordingly.

Third-party libraries and dependencies are vetted for security compliance.

4.5 Protection Against new Programs

Downloads are Blocked and will require Administrator approval before possible.

New Programs cannot be installed without Administrator's approval

5. Incident Response and Reporting

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

The incident response team will assess, contain and remediate the breach following predefined playbooks and best practices

External breaches (e.g., affecting customers) are disclosed according to regulatory obligations and with transparency to impacted users.

6. Regulatory and Legal Compliance

The company complies with the Curaçao Gaming Authority's requirements and applicable data protection laws such as GDPR where applicable.

Regular audits are conducted to ensure compliance with internal and external security standards.

7. Roles and Responsibilities

Management is responsible for Policy enforcement and resourcing – appointing Senior Officers.

Senior Officers are responsible to manage IT Security Team, create Technical safeguards, monitoring IT Team and handling incident reports accordingly

IT Security Team is responsible for overlooking All staff and ensure best practices are applied and policies are complied with.

Staff must fulfill their obligations and attend mandatory training at least once per annum, Compliance with policy and reporting suspicious activity |

Vendors and third parties must Adhere to security standards defined in contractual terms

8. Policy Review

This policy is reviewed annually, or upon significant changes to threat landscape, regulatory requirements, or organizational structure.

Version	Date	Drafted By
1.1	May 21, 2025	Compliance Officer