



SGD TECH N.V.

CompanyRegistrationNo.:169025

Information Security Policy

Company: SGD TECH N.V.

Registered Address: Trias Building, Hanchi Snoa 19, Willemstad, Curaçao

Platform: <https://kickwin.io>

Version	Description	Effective Date	Approved By	Review Date
1	Initial Information Security Policy	02/02/2026	Board of Directors	02/02/2026

This Policy is established in accordance with, and shall be interpreted in line with:
National Ordinance for Games of Chance (LOK, PB 2024 no. 157);
Requirements and guidance issued by the Curaçao Gaming Authority (CGA);

Approved by (Board of Directors):

Name:

Title: Director

Signature: _____

Date: 25-02-2026

Reviewed by (Compliance Officer):

Name: Ms. Eliane Solis Vazquez

Title: Compliance Officer

Signature: _____

Date: _____



Trias Building, Hanchi Snoa 19, Willemstad Curaçao



compliance@kickwin.io



1. Policy Statement

SGD TECH N.V. is committed to protecting the confidentiality, integrity, and availability of information and information systems used in connection with its gaming operations. The Company recognizes that effective information security is essential to protect player data, maintain operational resilience, safeguard regulatory compliance, and preserve trust in its platform. This Information Security Policy sets out the principles and controls adopted by the Company to manage information security risks in a proportionate and risk-based manner.

2. Purpose

The purpose of this Policy is to:

- Protect sensitive, confidential, and personal information from unauthorized access, disclosure, alteration, or destruction;
- Safeguard the integrity and availability of systems supporting gaming operations;
- Reduce the risk of data breaches, cyber incidents, and operational disruptions;
- Support compliance with applicable legal, regulatory, and contractual requirements;
- Establish clear responsibilities for information security governance and oversight.

3. Legal and Regulatory Framework

This Policy is established in accordance with, and shall be interpreted in line with:

- National Ordinance for Games of Chance (LOK, PB 2024 no. 157);
- Applicable requirements and guidance issued by the Curaçao Gaming Authority (CGA);
- Applicable data protection, cybersecurity, and confidentiality obligations;
- Relevant international information security best practices.

4. Scope and Applicability

This Policy applies to:

- All information assets owned, processed, or managed by SGD TECH N.V.;
- All systems, networks, applications, databases, and infrastructure supporting the platform <https://kickwin.io>;
- All employees, directors, contractors, and third parties with access to Company information or systems;
- All information, regardless of format (electronic, paper, or verbal).



5. Information Security Principles

The Company's information security framework is based on the following core principles:

- Confidentiality: Information is accessible only to authorized individuals and systems;
- Integrity: Information is accurate, complete, and protected from unauthorized modification;
- Availability: Information and systems are available when required to support business operations.

Security controls are implemented using a risk-based approach, proportionate to the sensitivity of the information and the associated risks.

6. Governance and Responsibilities

6.1 Board of Directors

The Board of Directors retains ultimate responsibility for information security and shall:

- Approve this Information Security Policy and any material amendments;
- Oversee the Company's information security risk posture;
- Ensure that appropriate resources are allocated to information security controls.

6.2 Senior Management

Senior Management is responsible for:

- Implementing this Policy across the Company's operations;
- Ensuring that information security risks are identified, assessed, and managed;
- Supporting incident response, remediation, and continuous improvement.

6.3 Employees and Third Parties

All employees and relevant third parties are responsible for:

- Complying with this Policy and related security requirements;
- Protecting credentials and access rights;
- Promptly reporting suspected or actual security incidents.

7. Access Control and Authentication

The Company implements access control measures to ensure that:

- Access to systems and information is granted on a need-to-know and least-privilege basis;
- User access rights are reviewed periodically;
- Authentication mechanisms are used to prevent unauthorized access.

8. Data Protection and Confidentiality

The Company applies appropriate safeguards to protect sensitive and personal data, including:

- Logical and physical security controls;
- Secure handling, storage, and transmission of data;
- Restrictions on unauthorized disclosure of confidential information.

Information shall be used solely for legitimate business purposes and in accordance with applicable data protection requirements.

9. System and Network Security

The Company implements measures to protect systems and networks, which may include:

- Secure system configuration and maintenance;
- Monitoring of system activity for potential security threats;
- Protection against malware, unauthorized access, and cyber attacks.

10. Incident Management and Reporting

The Company maintains procedures to identify, respond to, and manage information security incidents, including data breaches and system compromises.

Security incidents shall be:

- Escalated without delay to Senior Management and the Compliance Officer / MLRO where relevant;
- Assessed for potential regulatory, operational, or customer impact;
- Reported to competent authorities, including the Curaçao Gaming Authority (CGA), where required under applicable laws or regulations.

11. Business Continuity and System Availability

The Company takes reasonable measures to ensure the availability and resilience of its systems, including:

- Backup and recovery arrangements;
- Measures to minimize service disruption;
- Periodic review of system resilience and recovery capabilities.

12. Third-Party and Outsourcing Security

Where third parties provide services involving access to Company systems or data, the Company shall:

- Assess information security risks associated with such arrangements;
- Require appropriate security and confidentiality safeguards;
- Maintain oversight of third-party compliance with agreed security requirements.

Ultimate responsibility for information security remains with SGD TECH N.V.

13. Training and Awareness

Employees and relevant contractors receive appropriate information security awareness and training, proportionate to their roles and access rights.

14. Record Keeping

Records relating to information security incidents, assessments, and corrective actions shall be maintained in accordance with applicable record-keeping requirements.

15. Review and Update of the Policy

This Policy shall be reviewed at least annually, or sooner where required by changes in law, regulation, technology, or the Company's business operations.



SGD TECH N.V.

CompanyRegistrationNo.:169025

16. Contact Information

For questions or concerns relating to information security, please contact:

Compliance Officer

SDG TECH N.V.

Trias Building, Hanchi Snoa 19

Willemstad, Curaçao

Attention: Ms. Eliane Solis Vazquez

Title: Compliance Officer

Email: compliance@ecorpp.com



Trias Building, Hanchi Snoa 19, Willemstad Curaçao



compliance@kickwin.io



SGD TECH N.V.

CompanyRegistrationNo.:169025

BOARD RESOLUTION

Approval of Information Security Policy

SDG TECH N.V.

(Incorporated in Curaçao)

Registered Address: Trias Building, Hanchi Snoa 19, Willemstad, Curaçao

RESOLUTION OF THE BOARD OF DIRECTORS

The undersigned, being the members of the Board of Directors of SGD TECH N.V. (the "Company"), hereby adopt the following resolutions:

1. Approval of Information Security Policy

RESOLVED THAT the Board of Directors has formally reviewed and approved the Company's Information Security Policy, which establishes the principles, governance, and controls adopted by the Company to protect the confidentiality, integrity, and availability of information and information systems used in its gaming operations.

The Information Security Policy is adopted in accordance with applicable Curaçao laws and regulatory requirements, including:

- National Ordinance for Games of Chance (LOK, PB 2024 no. 157);
- Applicable requirements and guidance issued by the Curaçao Gaming Authority (CGA).

2. Implementation and Oversight

RESOLVED THAT Senior Management is hereby instructed to ensure the effective implementation of the Information Security Policy across all business operations, systems, and third-party arrangements.

RESOLVED FURTHER THAT appropriate technical, organizational, and administrative controls shall be maintained to support compliance with the Information Security Policy and to mitigate information security risks.



Trias Building, Hanchi Snoa 19, Willemstad Curaçao



compliance@kickwin.io



SGD TECH N.V.

CompanyRegistrationNo.:169025

3. Ultimate Responsibility

RESOLVED THAT the Board of Directors retains ultimate responsibility for information security governance and oversight and shall review the Information Security Policy at least annually or upon material changes to applicable laws, regulatory requirements, technology, or the Company's business operations.

4. Effective Date

RESOLVED THAT this Resolution shall take effect as of [DD / MM / YYYY]. 25-02-2026

By order of the Board of Directors

Name: _____

Title: Director

For and on behalf of SGD TECH N.V.



Trias Building, Hanchi Snoa 19, Willemstad Curaçao



compliance@kickwin.io