

INFORMATION SECURITY POLICY

Table of Contents

1. Purpose.....	3
2. Scope.....	3
3. Definitions.....	3
4. Regulatory Framework.....	4
5. Governance and Responsibilities.....	4
6. Information Security Risk Management.....	5
7. Data Classification.....	5
8. Access Control.....	6
9. Data Protection, Systems, and Network Security.....	6
10. Physical Security.....	7
11. Secure Software Development Lifecycle (SDLC).....	7
12. Change Management.....	7
13. Incident Response.....	8
14. Third-Party and Supplier Security.....	8
15. Human Resources Security.....	9
16. Monitoring and Logging.....	9
17. Acceptable Use.....	10
18. Regulatory Compliance and Reporting.....	10
19. Policy Review and Maintenance.....	10
20. Information Security Controls Matrix.....	11

1. Purpose

This Information Security Policy (the “Policy”) establishes the principles, roles, requirements, and minimum controls for protecting information, information systems, technology infrastructure, and related processes of Dreamtek Solutions B.V. (the “Company”) within the scope of its activities as a reseller and/or aggregator in the iGaming industry.

The objectives of this Policy are to ensure:

- confidentiality of information, including player data, transaction data, and commercially sensitive information;
- integrity of data, systems, and game-related processes;
- availability of critical services and platforms;
- appropriate management of information security risks;
- timely detection of, response to, and recovery from security incidents;
- adequate controls over internal and external access, third-party providers, and integrations;
- compliance with applicable regulatory requirements, including those set forth by the competent Curaçao gaming regulator (the “Regulator”).

2. Scope

This Policy applies to:

- all employees, directors, officers, consultants, contractors, and temporary staff of the Company;
- all information assets, systems, services, networks, environments, accounts, integrations, and data owned by, used by, or processed on behalf of the Company;
- third-party providers to the extent they provide critical or security-relevant services, including but not limited to hosting, cloud infrastructure, platform services, payment processing, identity and compliance-related verification services, customer support, software development, and game provision;
- all locations from which the Company systems or data are accessed, including offices, data centers, remote work environments, and mobile devices.

3. Definitions

Term	Definition
Information Asset	Any data, system, application, network component, or service that has value to the Company.
Critical System	A system, service, or infrastructure component whose unavailability or compromise would materially affect the Company’s operations, regulatory compliance, financial position, or player experience.
Privileged Access	Elevated access rights that allow administrative, configuration, or unrestricted actions on systems, databases, infrastructure, or security controls.
Incident	An event or series of events that constitutes a breach or imminent threat of breach of information security policies, controls, or the confidentiality, integrity, or availability of information assets.
Third-Party Provider	Any external entity that provides services, software, infrastructure, or processes that interact with or support the Company’s information assets or operations.
Game Integrity Data	Data related to the fairness and correctness of games, including RTP calculations, game round logs, and provider audit trails.
MFA	Multi-Factor Authentication — an authentication mechanism requiring two or more independent verification factors.

RTO	Recovery Time Objective — the maximum acceptable duration of system downtime following a disruption.
RPO	Recovery Point Objective — the maximum acceptable amount of data loss measured in time.

4. Regulatory Framework

The Company operates within the regulatory framework applicable to remote gaming in or from Curaçao, including the National Ordinance on Games of Chance (Landsverordening op de kansspelen, P.B. 2024, no. 157) (“LOK”), and the licensing, supervisory, and reporting requirements issued or administered by the competent Curaçao gaming regulator.

This Policy is intended to support the Company’s compliance with applicable information security and governance requirements arising from:

- the LOK and related Curaçao licensing conditions, policies, portal requirements, and supervisory measures issued from time to time by the competent Curaçao gaming regulator;
- applicable data protection and privacy laws relevant to the Company’s operations and the categories of data processed by the Company;
- applicable anti-money laundering and counter-terrorist financing (AML/CFT) legislation and regulation, including, where relevant, the National Ordinance on Identification when Rendering Services (Landsverordening identificatie bij dienstverlening, P.B. 2017, no. 92, as amended) and the National Ordinance on the Reporting of Unusual Transactions (Landsverordening melding ongebruikelijke transacties, P.B. 2017, no. 99, as amended), together with related implementing regulations and supervisory requirements applicable to the gaming sector;
- relevant contractual, operational, and risk-based information security obligations adopted by the Company, taking into account recognized industry standards and practices where appropriate.

The Company shall cooperate with the Regulator and provide such information, records, notifications, and access as may be required under applicable law, license conditions, and supervisory procedures.

5. Governance and Responsibilities

5.1 Management

The Managing Director and senior management bear overall responsibility for maintaining an adequate level of information security and for approving this Policy.

5.2 Document Owner

The Legal and Compliance Function is responsible for coordinating the review and update of this Policy, ensuring its alignment with internal processes and applicable regulatory requirements.

5.3 Chief Technology Officer (CTO)

The CTO is responsible for the implementation and maintenance of technical and organizational information security measures, including oversight of the IT, DevOps, Security, and QA functions.

5.4 Function Heads

Function heads are responsible for ensuring compliance with this Policy within their respective areas, including approving access requests, reporting risks and incidents, and enforcing control procedures.

5.5 All Personnel

All employees, contractors, and other users of Company systems are required to:

- use systems and data only within the scope of their authorized role and responsibilities;

- comply with security and confidentiality requirements;
- report incidents, suspicious events, or credential compromise immediately through designated channels;
- complete mandatory security awareness training.

6. Information Security Risk Management

The Company adopts a risk-based approach to information security.

Information security risks are identified, assessed, and reviewed at least annually, as well as in response to:

- significant changes to systems, integrations, or infrastructure;
- changes to the business model or outsourcing arrangements;
- security incidents;
- changes in applicable regulatory requirements;
- introduction of new third-party providers or technologies.

Risk assessments consider, among other things:

- cyberattacks, including targeted and advanced persistent threats;
- phishing and social engineering;
- unauthorized access to systems and data;
- data breach, leakage, or loss;
- insider threats and personnel misconduct;
- ransomware and other malware;
- unavailability of critical services and platforms;
- disruption or failure of third-party providers;
- vulnerabilities in integrations, APIs, and critical operational systems;
- threats specific to iGaming operations, including game manipulation, abnormal player behavior, and RTP deviations.

Risk assessment results are documented in a risk register. Corrective actions are tracked to closure or formal acceptance by an authorized individual. The risk register is made available to the Regulator upon request.

7. Data Classification

The Company classifies information assets according to the following scheme:

Level	Description	Examples
Confidential	Highly sensitive information whose unauthorized disclosure would cause significant harm to the Company, its partners, or players.	customer and business verification and anti-money laundering compliance records, encryption keys, API secrets, security configurations, access credentials.
Internal	Information intended for internal use that is not suitable for public disclosure.	Internal procedures, architecture documentation, employee data, contracts, operational metrics, incident reports.
Public	Information approved for unrestricted disclosure.	Marketing materials, public website content, published API documentation.

All information is classified as Internal by default unless explicitly classified otherwise. Data handling, storage, transmission, and disposal procedures are applied in accordance with the classification level.

8. Access Control

8.1 General Principles

Access to Company systems, data, and services is granted exclusively on the basis of business need, user role, and the principle of least privilege. No user is granted access beyond what is required for their function.

8.2 Access Lifecycle

Provisioning, modification, and revocation of access follow a formalized procedure with documented approval. Access is revoked without undue delay upon termination, end of contract, or role change.

8.3 Multi-Factor Authentication

MFA is mandatory for:

- all production environment access;
- cloud management consoles (AWS, GCP, or equivalent);
- administrative and privileged accounts;
- VPN and remote access;
- code repositories and CI/CD pipelines.

Exceptions to MFA requirements require a documented risk exception approved by the CTO.

8.4 Password and Authentication Policy

Where passwords are used, the following minimum requirements apply:

- minimum length of 12 characters with complexity requirements (uppercase, lowercase, digits, special characters);
- prohibition of password reuse across systems;
- use of a password manager for non-SSO credentials;
- prohibition of sharing credentials under any circumstances.

The Company prioritizes SSO and passwordless authentication mechanisms where technically feasible.

8.5 Session Management

Interactive sessions to critical systems are subject to automatic timeout after a defined period of inactivity. Concurrent session limits may be applied based on risk assessment.

8.6 Privileged Access

Privileged access is granted to a restricted set of individuals and is subject to enhanced controls, including separate administrative accounts, logging of all privileged actions, and periodic review.

8.7 Access Reviews

Access rights are reviewed on a periodic basis (at minimum quarterly for privileged access and semi-annually for standard access) and adjusted or revoked as necessary.

9. Data Protection, Systems, and Network Security

9.1 Technical and Organizational Measures

The Company implements appropriate technical and organizational measures to protect personal, operational, financial, commercially sensitive, player, and game integrity data. These measures include but are not limited to:

- role-based access control (RBAC);
- encryption of data in transit using TLS 1.2 or higher;
- network segmentation (separation of production, staging, development, and corporate environments);
- firewall and intrusion detection/prevention systems;
- endpoint detection and response (EDR);
- anti-malware controls;
- hardened and documented system configurations;
- timely patching and updates based on vulnerability severity;
- secure remote access (VPN with MFA);
- centralized logging and monitoring;
- DDoS mitigation for public-facing services.

9.2 Data Retention and Disposal

Data is retained only for the period necessary to fulfill its legitimate purpose and to comply with internal, contractual, and applicable regulatory requirements. Retention periods for key data categories are defined in a data retention schedule. Archiving and secure deletion are performed in a controlled manner with appropriate records.

10. Physical Security

Although the Company's infrastructure is primarily cloud-based, the following physical security controls are maintained:

- office premises are protected by access controls (electronic locks, access cards, or equivalent);
- visitors to Company premises are registered and escorted in areas where sensitive information may be visible or accessible;
- a clean desk policy is enforced: sensitive documents and removable media are not left unattended;
- physical media and hardware containing Company data are securely wiped or destroyed prior to disposal or reassignment;
- for cloud infrastructure providers, the Company seeks appropriate evidence of information security controls, which may include recognized certifications, independent audit reports, or other equivalent assurance documentation, where available and proportionate to the level of risk.

11. Secure Software Development Lifecycle (SDLC)

As a technology platform, the Company integrates security into all stages of software development:

- secure coding guidelines are established and communicated to all developers;
- code review is mandatory before merging to protected branches;
- third-party libraries and dependencies are monitored for known vulnerabilities;
- production credentials and secrets are not used in development or testing environments;
- security requirements are considered during the design phase of new features and integrations.

12. Change Management

Significant changes to systems, integrations, configurations, or critical processes are initiated, approved, tested, and deployed in a controlled manner with due regard for security requirements prior to implementation.

A change is classified as significant if it:

- affects production systems or infrastructure;

- modifies security controls, access policies, or network configurations;
- introduces new third-party integrations or dependencies;
- alters data flows involving player data, financial transactions, or game integrity data.

Changes are accompanied by a rollback plan where applicable. Emergency changes are permitted only to address critical risks, restore service availability, or respond to incidents, and must be documented and retrospectively reviewed within five business days.

13. Incident Response

13.1 Incident Categories

Information security incidents include but are not limited to:

- unauthorized access to systems or data;
- credential compromise;
- data breach, leakage, or loss;
- malware infection;
- denial-of-service attacks;
- critical system failure or unavailability;
- fraudulent or suspicious activity;
- security breach at a third-party provider affecting the Company;
- game integrity compromise (RTP manipulation, abnormal patterns);
- incidents are escalated to the CTO, Compliance, and Management depending on severity;
- containment and recovery actions are coordinated by the relevant technical and management functions;
- material incidents are documented and reviewed for lessons learned and remediation. Incident records are treated as confidential and are retained and disclosed only to authorized persons, or where required under applicable law, license conditions, or lawful regulatory process.

13.2 Response Process

The Company seeks to maintain procedures for detection, reporting, assessment, containment, investigation, remediation, and documentation of information security incidents.

All employees and contractors must report potential incidents without delay through designated channels (security incident reporting procedure).

14. Third-Party and Supplier Security

The Company manages risks associated with third-party providers that supply hosting, cloud infrastructure, platform services, payment processing, identity and compliance-related verification services, game content, customer support, development, or other critical services.

14.1 Due Diligence

Prior to engaging providers that will have access to data, systems, or critical processes, the Company conducts a risk-based due diligence review. For critical providers, and where appropriate to the level of risk, the Company obtains and evaluates documentation demonstrating that appropriate information security measures are in place. Such documentation may include, where available and appropriate, recognized certifications, independent audit reports, security questionnaires, or other equivalent evidence of information security controls.

14.2 Contractual Requirements

Contracts with relevant providers include, where applicable, provisions regarding:

- confidentiality and non-disclosure;
- data protection and data processing agreements;
- information security requirements and minimum controls;
- access control and privilege management;
- incident notification obligations and timelines;
- right to audit or request evidence of compliance;
- termination of access and secure data return or destruction upon end of engagement.

14.3 Game Provider Security

Game providers are subject to additional requirements, including:

- game integrity controls and audit trails for game rounds;
- secure API integration in accordance with Company technical standards;
- compliance with applicable regulatory requirements for the jurisdictions served.

14.4 Ongoing Monitoring

Critical third-party providers are reviewed periodically based on their risk classification. The Company monitors provider performance, security posture, and compliance with contractual obligations.

15. Human Resources Security

15.1 Pre-Employment

Background verification checks are performed for candidates being considered for positions that involve access to critical systems, sensitive data, or financial operations, to the extent permitted by applicable law.

15.2 Onboarding

New employees and contractors sign confidentiality and non-disclosure agreements. Access is provisioned in accordance with the access control procedures described in Section 8. Security awareness training is completed before or within the first week of access being granted.

15.3 During Employment

Employees are subject to ongoing obligations regarding confidentiality, acceptable use of systems, and compliance with this Policy. Violations are addressed through the disciplinary process.

15.4 Offboarding

Upon termination or end of engagement, all access is revoked promptly (within 24 hours), Company equipment and data are returned, and the individual is reminded of continuing confidentiality obligations.

16. Monitoring and Logging

The Company performs logging and monitoring of critical system, security, administrative, and other relevant events commensurate with risk and technical architecture.

Logging covers, at minimum:

- authentication events (successful and failed);
- privileged operations and administrative actions;
- access to sensitive data and critical systems;
- changes to security configurations;

- network events and firewall activity;
- application-level events relevant to security and game integrity.

Access to logs is restricted to authorized personnel. Logs are protected against unauthorized modification or deletion. Log retention periods are defined by the Company taking into account legal, regulatory, security, and operational requirements.

17. Acceptable Use

All users of Company systems and information assets are expected to:

- use systems, applications, and data only for authorized business purposes;
- protect credentials and not share passwords, tokens, or access keys;
- lock workstations when unattended;
- not install unauthorized software on Company-managed devices;
- not store Company data on personal devices or unauthorized cloud services without approval;
- not attempt to circumvent security controls;
- report security incidents, suspicious emails, and policy violations promptly.

Violations of acceptable use requirements may result in disciplinary action, up to and including termination.

18. Regulatory Compliance and Reporting

The Company maintains compliance with information security-related requirements of the Regulator and applicable legislation. This includes:

- making the risk register, incident logs, and audit records available to the Regulator upon request;
- cooperating with regulatory audits and inspections;
- ensuring that data processed for customer and business verification and for anti-money laundering, counter-terrorist financing, and counter-proliferation financing purposes is protected in accordance with this Policy and the Company's AML/CFT/CPF Policy;
- maintaining records sufficient to demonstrate compliance with this Policy and regulatory requirements.

19. Policy Review and Maintenance

This Policy is reviewed at least annually, as well as in response to:

- significant changes to systems, infrastructure, or integrations;
- material changes to the outsourcing model or third-party arrangements;
- information security incidents;
- changes to the business model;
- changes in applicable regulatory requirements;

Updates to this Policy are reviewed by relevant functions and approved by the Managing Director. The version history is maintained in the Document Control section.

20. Information Security Controls Matrix

Control Area	Owner	Frequency	Evidence / Records
Risk Management	Management / Compliance / IT	Annually + after significant changes or incidents	Risk register, review records, action tracker
Data Classification	IT / Compliance	Annually + at introduction of new data types	Data classification register, handling guidelines
Access Control	IT	Onboarding, role change, offboarding + quarterly (privileged) / semi-annual (standard) reviews	Access approval records, review records, access logs
Privileged Access	IT / CTO	As needed + quarterly review	Privileged access register, admin logs, MFA configuration records
Data Protection	IT / Legal / Compliance	Ongoing + periodic review	Data inventory, retention schedule, encryption configuration records, deletion records
Cryptography & Key Management	IT / DevOps	Ongoing + key rotation per schedule	Key inventory, rotation records, certificate management logs
Network & System Security	IT / DevOps	Ongoing + regular technical reviews	System configurations, patch records, monitoring logs, security tool records
Vulnerability Management	IT / DevOps	Regularly per risk level	Vulnerability scan reports, remediation tracker
Physical Security	Office Management / IT	Ongoing + annual review	Access logs, visitor logs, asset disposal records
Secure SDLC	CTO / Dev Leads	Every release + periodic security testing	Code review records, SAST/DAST reports, dependency scan results
Change Management	IT / CTO / DevOps	Every significant change	Change requests, approvals, deployment records, rollback records
Incident Response	IT / CTO / Management / Compliance	As needed + post-incident review	Incident log, investigation records, lessons learned, the Regulator notifications
Backup & Restore	IT / DevOps	Daily or per system criticality	Backup logs, restore test results, backup configuration records
Third-Party Security	Legal / Compliance / CTO	Onboarding + periodically per risk	Due diligence records, contracts, vendor review records
HR Security	HR / IT	Onboarding, offboarding, role changes	NDA records, background check records, offboarding checklists
Monitoring & Logging	IT / DevOps	Ongoing + periodic review	System logs, SIEM records, log retention configuration
Regulatory Compliance	Compliance / Legal / CTO	Ongoing + per the Regulator requirements	Regulatory correspondence, incident notifications, audit evidence
Policy Review	Document Owner / Management	Annually + after significant changes	Policy review record, version history, approval record