

Information Security Procedure

DG Innovations B.V.

Document Control

Version	Date	Description of Changes	Author
1.0	04.02.2026	Initial draft	IGA Trust B.V.

1. Purpose

The purpose of this policy is to ensure that all information handled by DG Innovations B.V., in any form—written, spoken, electronically recorded, or printed—is protected from accidental or intentional unauthorized access, modification, destruction, or disclosure throughout its lifecycle. This includes maintaining appropriate security over the equipment and software used to process, store, and transmit information. The policy also establishes standards for the storage of player-critical data and transaction records on local Curaçao servers.

2. Scope

This policy applies to all employees, contractors, affiliates, and departments within DG Innovations B.V. and covers:

All forms of information, including player data, financial transactions, and operational records.

All systems and infrastructure used to process, store, or transmit information.

Compliance with regulatory obligations, including local Curaçao data storage requirements.

3. Policy Statements

3.1 Information Protection

All information must be safeguarded from unauthorized access, modification, destruction, or disclosure.

Security measures must be implemented at every stage of the information lifecycle.

3.2 Documentation of Policies and Procedures

All policies, procedures, and activities related to information security must be fully documented.

Documentation must be made available to individuals responsible for implementation and compliance.

Documentation must be retained for at least five (5) years from creation or from the date of changes to policies/procedures.

Documentation must be periodically reviewed for appropriateness and currency, with review cycles determined by each entity or department.

3.3 Departmental and Entity-Level Policies

Each department or entity must develop additional policies, standards, and procedures to implement this policy and address specific system functionality.

Departmental policies must be consistent with this overarching policy.

All systems implemented after the effective date must comply with this policy; existing systems must be brought into compliance as soon as practical.

3.4 Data Storage Requirements

All player-critical data (including personally identifiable information, account balances, and gaming activity) and transaction records must be stored on a local server physically located in Curaçao.

Servers must ensure secure daily backups of all player-critical data and transactions.

Data storage systems must comply with security standards to prevent unauthorized access, modification, or loss of data.

Backup and archival processes must be verified regularly to ensure integrity and recoverability of data.

3.5 Systems Security

All hardware and software used to process, store, or transmit information must be protected with appropriate security controls, including access controls, encryption, and logging.

Security incidents must be reported and addressed promptly.

4. Compliance and Responsibilities

All employees and contractors are responsible for following this policy and associated procedures.

Department heads must ensure that their teams comply with these requirements.

IT teams must maintain secure systems and ensure that all data storage, especially player-critical data, adheres to the Curaçao local server requirement.

Internal audits will be conducted periodically to verify compliance with this policy.

5. Enforcement

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contracts. Regulatory authorities may also be notified if breaches involve sensitive player or transaction data.

6. Review and Updates

This policy will be reviewed periodically by DG Innovations B.V. management to ensure it remains up-to-date with legal, regulatory, and operational requirements. All updates must be documented and communicated to relevant personnel.