

INFORMATION SECURITY POLICY

Version:	V. 1
Date:	August 05, 2025

Purpose.....	3
Policy basis.....	3
Responsibilities.....	4
Policy objectives.....	4
Pointissimo B.V. IT Security Governance and Management.....	5
Enforcement.....	5
Revision and changes.....	5
Security policy.....	6
Classification of Information Storage for Security Purposes.....	7
Information Storage.....	7
Automated Information Management System.....	7
Access to Information.....	7
Communications & Operations Management.....	8
Information Systems Acquisition, Development & Maintenance.....	9
Data protection policy.....	11
Clear Desk/Screen Policy.....	13
Privacy and security of player information.....	14
Players' Password Management.....	17
Credit Card Information Management.....	19
Business Continuity Management.....	20
Compliance.....	21

Purpose

Pointissimo B.V. (hereinafter the “Company” or “Pointissimo”) is committed to protecting the confidentiality, integrity, and availability of all business information in order to safeguard the **Company’s** assets, stakeholders, and reputation, irrespective of its form (electronic, paper-based, verbal, etc.). Information must be available only to those authorized to access it, and there must never be any doubt as to its completeness and accuracy.

This policy forms part of **Pointissimo’s** Corporate Governance framework and is developed in alignment with the regulatory and licensing requirements of the **Curacao Gaming Authority**.

Policy basis

This information security policy has been developed with reference to a number of legal and regulatory sources, the main of which are:

- National Ordinance on the Supervision of Gaming (LOK), Curaçao;
- Curacao National Ordinance on the Protection of Personal Data, enacted on 1 October 2010;
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, GDPR);
- Payment Card Industry Data Security Standard (PCI DSS) v4.0 (March 2022);
- Such other legislation and regulations as may be applicable from time to time by virtue of the Company’s services to residents of relevant jurisdictions.

This policy also aspires to implement recognized industry best practices, including:

- ISO/IEC 27002:2022 – Information security, cybersecurity, and privacy protection – Information security controls;
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 5;
- Cybersecurity Maturity Model Certification (CMMC) 2.0;
- ITIL (Information Technology Infrastructure Library) v4.

Additional standards or frameworks may be referenced where applicable to the **Company’s** operations, markets, or technical environment.

Responsibilities

The teams/person responsible for the implementation and effectiveness of this policy are:

- *General supervision/key functions*
 - **CTO (Chief Technology Officer)**

- *Implementation and control*
 - **ISO (Information Security Officer)**
- *Adherence to the policy requirements*
 - **All staff and assignees**

Policy objectives

The objectives of this Information Security Policy are:

- To protect **Pointissimo's** business and customer information from unauthorized disclosure, modification, or loss.
- To implement safeguards that protect the Company's information resources, equipment, networks, and applications from theft, abuse, misuse, or damage, including protection against intrusive software (such as computer viruses and malware).
- To establish clear responsibility and accountability for Information Security across all levels of the organization.
- To ensure the Company's ability to continue operations in the event of significant Information Security incidents.
- To ensure compliance with applicable laws, regulations, and industry best practices, including the licensing requirements of the **Curacao Gaming Authority**.
- To promote an appropriate level of awareness, knowledge, and skills among management and employees in order to minimize the occurrence and severity of Information Security incidents.
- To protect the confidentiality, integrity, and availability of the **Company's** business information, thereby safeguarding its assets, stakeholders, and reputation, irrespective of the information's form (electronic, paper-based, verbal, etc.).

Pointissimo B.V. IT Security Governance and Management

The **Pointissimo** Executive Board is responsible for the Information Security Policy. The Board has delegated the day-to-day operation of Information Security to the Information Security Officer ("ISO").

Information Security Officer (ISO)

The ISO is responsible for ensuring that the Information Security Policy is implemented in **Pointissimo's** business operations. The ISO is also responsible for all day-to-day Information Security issues and is the first point of contact for all security-related issues within the organization. The ISO may delegate some or all of the policy sections, but is ultimately responsible for its implementation.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Companies contracted by **Pointissimo** that are found to be in violation of this policy will be deemed in breach of contract.

Revision and changes

In accordance with **Curacao Gaming Authority** regulatory requirements, **Pointissimo's** information security policies and procedures must be documented, communicated, and reviewed annually, and more frequently in the event of material changes.

Significant changes to any policy or procedures are to be approved by the **Company's** Key Official and formally documented. Security policies require yearly documentation, communication, and review. Both internal and external security audits must be performed annually. In addition, risk-based IT security reviews are conducted regularly on data transmissions that carry sensitive player information and gaming data, as deemed appropriate by management.

Security policy

- The function of an Information Security Officer (ISO) shall be fulfilled by a person within the organization or its subsidiaries and shall be appointed by the Executive Board. This function must be fulfilled at all times. The position of the ISO shall be independent of other organizational functions and shall be part of the department responsible for Corporate Governance.
- An Information Security Management Committee, composed of senior managers, should meet quarterly to review the current status of **Pointissimo's** information security, approve new or modified security policies, and oversee other high-level security management activities.
- The ISO must compile and maintain a list of contacts in relevant authorities, such as law enforcement, the CGA, the Financial Intelligence Unit Curaçao (FIU), emergency services, health & safety bodies, and relevant service providers.
- The ISO must maintain contact with special interest groups, security forums, and professional associations dealing with information security.
- A periodic independent review of **Pointissimo's** approach to managing information security and its implementation shall be commissioned by the ISO in accordance with the **Curacao Gaming Authority** requirements and industry best practices.
- The ISO must strive to make the information security policy easily accessible to all staff.
- The ISO must ensure that all contracts and agreements with third parties comply with **Pointissimo's** security policies and include appropriate Non-Disclosure Agreements (NDAs).
- A comprehensive set of Information Security Policies, of which this document is one, shall be written, agreed upon, and communicated to all employees and relevant third parties so that security requirements and obligations are well understood by all concerned.

Classification of Information Storage for Security Purposes

The classification of data and the determination of its sensitivity, and the level of protection required are governed by internal documents.

Information Storage

All information is stored electronically, ensuring a streamlined and secure approach to data management.

Any information that is required to be kept in physical form (such as statutory documents, certificates, financial reports, deeds) is stored by the **Company's** officers in the designated place of business. This ensures compliance with legal requirements while maintaining a secure and organized system for handling critical documents.

Automated Information Management System

The management of information assets within the organization is automated. The Information Security Officer (ISO) is responsible for ensuring that information is captured, processed, and stored in accordance with internal data protection and security requirements. All sensitive information is stored in a centralized location and is strictly encrypted.

Access to Information

The Gaming System operates under a strict role-based model founded on a need-to-know basis. This model ensures a precise segmentation into groups, roles, and permissions assigned to specific roles. The system is highly flexible, allowing any specific set of individuals to be granted any specific set of permissions. However, no permissions are granted unless they are required for the employee to perform their direct duties. The ISO is responsible for maintaining and updating these access rights.

Information transferred outside of controlled systems in hard copy format should be classified as follows:

- **Confidential:** Access is role-based on a need-to-know basis.
- **Internal:** Access is available to all employees.
- **Public:** Information that is available to the general public.

Communications & Operations Management

Objective

To ensure the correct and secure operation of information processing facilities.

Scope

Applies to all **Pointissimo** information processing facilities.

Policy

- Printed sensitive information communicated across the organization must be placed in a sealed envelope and clearly marked “**CONFIDENTIAL**”.
- Operating procedures must be documented, maintained, and made available to all authorized users who require them.
- Where feasible, duties and areas of responsibility must be segregated to reduce opportunities for unauthorized or accidental modification, misuse, or loss of the **Company**’s assets.
- All third-party service definitions and delivery levels (Service Level Agreements, SLAs) must be included in binding contracts and agreements, and monitored for compliance.
- Production application resource usage must be monitored and optimized, with projections made for future capacity requirements.
- Acceptance criteria for all systems must be defined, and appropriate testing carried out during development prior to implementation.
- A culture of continuous improvement must be established to enhance both service delivery and security.
- An incident management process must be formally established, documented, and maintained.
- Threat intelligence should be leveraged to proactively identify, assess, and mitigate potential security threats.
- The backup and data recovery process must strictly adhere to the **Company**’s official *Backup and Data Recovery Policy*.

Information Systems Acquisition, Development & Maintenance

Objective

To ensure that security is an integral part of information systems.

Scope

This policy applies to all information and systems within the **Pointissimo** infrastructure.

Policy

General

- Business requirements for new information systems or enhancements to existing systems must include clearly defined security control requirements.
- Data and databases used in test or staging environments must be sanitized and must not contain sensitive or confidential information.
- The ISO must remain aware of newly discovered security vulnerabilities and assess their impact on the **Company's** production and office environments.
- The production environment must be audited for compliance with this security policy both prior to go-live and on a recurring basis.
- Independent third-party security reviews and penetration tests must be performed at least annually, and always prior to go-live or following any material change.

Production Environment

- All production environments must be designed and operated in a redundant configuration to eliminate single points of failure.
- All production systems must undergo operating system hardening and must not run unnecessary services.
- All production systems must have an effective patch management program in place to identify and apply software patches in a timely manner.
- No production environment component may contain known vulnerabilities unless a formal risk assessment has been conducted and approved by the ISO.

Application Design

- Application software must be robust, self-checking, and resistant to invalid input or intentional/unintentional data corruption.
- All production applications must protect the confidentiality, integrity, and availability of the data they process or store.
- Applications must include safeguards against denial-of-service (DoS/DDoS) attacks and similar threats.

- Secure audit logs must be generated for all critical activities and entities within the system.
Customer-requested data changes must follow a formal verification and authorization process. Direct alteration of data fields without validation is prohibited. Technical support staff must authenticate and validate customer identity prior to approving any data changes.
- All applications must comply with applicable data protection laws and regulations, including GDPR where relevant.

Source Code

- Access to application source code must be restricted to authorized personnel only, and source code must be encrypted when stored outside of the **Company's** secure environment.
- Source code must not contain embedded authentication credentials.
- Source code must never reside in the production environment.
- All production or source code changes must be tracked via a formal change management system, reviewed, and approved by peers prior to release into test or staging environments.
- Production environment changes must include an approved rollback plan to mitigate unforeseen consequences.
- Release of code from staging to the live production environment must require multiple levels of sign-off and documented approval.

Data protection policy

Objective

To ensure the protection of personal and sensitive data from unauthorized access, use, disclosure, alteration, or destruction, in compliance with the Curacao National Ordinance on the Protection of Personal Data (2010), the General Data Protection Regulation (GDPR), where applicable, and other relevant laws and regulations.

Scope

This policy applies to all employees, contractors, and third-party service providers who collect, process, store, or transmit personal and sensitive data within the **Pointissimo** systems.

Policy

Data Privacy

Company electronic information resources must conform to **Company** policies and regulations related to the privacy of data or information records associated with them.

Transferring Data

- Prior to transferring restricted data, the information resource proprietor must ensure appropriate safeguards are implemented.
- Wherever appropriate, restricted data must be encrypted during transmission using strong cryptographic standards.
- Encryption keys must be exchanged through secure methods, such as public key infrastructure or verified separate communication.

Encryption

- Encryption must be employed to protect the confidentiality of sensitive or business-critical information whenever physical or logical security cannot be guaranteed.
- All sensitive information transmitted over communication systems must be encrypted (e.g., TLS/SSL for player activity).
- Sensitive data stored on devices or media must be encrypted to prevent unauthorized access.
- Encryption algorithms and protocols must comply with industry best practices (e.g., AES-256, TLS 1.2+).
- Encryption complements but does not replace other logical security measures.

Storage

- Records subject to disclosure must be accessible to authorized **Company** officials at all times.
- Business-critical information must be securely stored in known, controlled locations. If

encrypted, decryption means must be available to more than one authorized custodian.

Firewalls and External Connectivity

- Communications access controls, such as firewalls, must be implemented to limit unauthorized access to restricted or essential resources across the **Company's** networks.
- Firewall protections must be deployed at the appropriate subnet and perimeter levels.

Intrusive Computer Software

- The **Company** must regularly assess exposure to malicious software (viruses, malware, ransomware).
- Based on risk assessments, the **Company** must implement preventive measures such as antivirus software, firewalls, and patch management.
- The ISO must coordinate prevention, detection, response, and user notification in the event of malware propagation.

Internet Use Browsing Guidelines

- Employees must comply with the **Company's** Acceptable Use Policy.
- Use of **Company** IT resources for non-business-related purposes is strictly prohibited, including access to inappropriate websites or unauthorized instant messaging applications.
- All internet usage may be subject to monitoring and audit to ensure compliance with the **Company's** policies.

Clear Desk/Screen Policy

Objective

To ensure that all confidential and sensitive information belonging to **Pointissimo** is protected from unauthorized access, use, disclosure, alteration, or destruction by maintaining a secure clear desk and screen environment, in compliance with **Curacao Gaming Authority** requirements and recognized industry best practices.

Scope

This policy applies to all employees, contractors, and temporary staff who handle, process, or manage confidential and sensitive information within the **Company's** systems or premises.

Policy

Clear Screen Policy

- Desktop and laptop computers must not be left logged in when unattended and must always be password-protected.
- A security lock (screensaver with password protection) must automatically activate after a short, predetermined period of inactivity.
- Computer screens must be positioned so that they are not visible to unauthorized persons.

Session Time-Out

- All user sessions must automatically terminate after 30 minutes of inactivity.
- Users reconnecting remotely must re-authenticate with their login credentials and VPN.

Privacy and security of player information

Objective

To ensure that player information is protected from unauthorized access, use, disclosure, alteration, or destruction, in compliance with the Curacao National Ordinance on the Protection of Personal Data (2010), applicable anti-money laundering (AML) and counter-terrorism financing (CTF) requirements, and the General Data Protection Regulation (GDPR) where applicable.

Scope

This policy applies to all player information collected, processed, stored, and transmitted within and outside **Pointissimo** systems.

Policy

General

- Player names and other identifying particulars must be treated as confidential and protected against unauthorized access.
- Sensitive information, including KYC documentation, responsible gambling information, and masked payment card data, must be safeguarded with the highest level of confidentiality and security.
- Policies and procedures for handling player information must be documented, communicated to all relevant personnel, and strictly enforced.
- Annual reviews of security policies must be conducted to ensure continued compliance and effectiveness.

Data Collection and Use

- Only player information strictly necessary for business operations, AML/KYC compliance, or legal obligations may be collected and used.
- Players must be informed of the categories of data collected and the purposes of processing.
- Explicit consent must be obtained before collecting sensitive personal data.
- All financial transactions (deposits, withdrawals, adjustments) must be protected by strict security controls and logged in secure audit systems.

Data Storage and Protection

- Player information must be stored in secure databases with strong access controls.
- Encryption must be applied to player data both in transit and at rest.
- All systems must be regularly patched and updated.

Access Control

- Access to player information must be strictly on a need-to-know basis.

- A role-based access model must be implemented, with restricted features and functions per role.
- Strong authentication, including two-factor authentication (2FA), must be implemented for system access and for all critical actions.
- Logs of access to player information must be generated, retained, and regularly reviewed.

Incident Response

- An incident response plan must be developed and maintained to address potential data breaches.
- Affected players and the CGA must be notified without undue delay in the event of a data breach; FIU Curaçao must also be informed where applicable.
- All incidents must be thoroughly investigated, documented, and mitigated.

Compliance and Audits

- The **Company** must comply with all relevant data protection laws and licensing requirements.
- Internal and external audits must be conducted regularly to verify compliance with this policy.
- Records of audits and compliance reviews must be maintained.

Training and Awareness

- Employees must receive regular training on data protection and privacy obligations.
- Awareness programs must emphasize the importance of protecting player information and the consequences of non-compliance.

Data Retention and Disposal

- Player information must only be retained as long as necessary to meet business and legal requirements.
- Data no longer required must be securely disposed of in a manner that prevents recovery.

Encryption and Secure Communication

- TLS/SSL encryption must be used for all communications involving player information.
- Encryption keys must be securely generated, stored, and rotated.

Vendor Management

- Third-party vendors must undergo due diligence to ensure adequate data protection practices.
- Vendor contracts must include binding data protection obligations.

- Ongoing monitoring of vendor compliance must be performed.

Monitoring and Review

- Automated monitoring tools must be in place to detect unauthorized access or suspicious activity.
- Security policies must be regularly reviewed and updated in response to emerging threats and regulatory changes.

Players' Password Management

Objective

To ensure the security and confidentiality of players' login credentials in compliance with **Curacao Gaming Authority** requirements and industry best practices.

Scope

This policy applies to all players creating an account with **Pointissimo** and to all **Company** employees involved in the management and security of player accounts.

Policy

Account Creation

- When creating an account, players must provide a unique account identifier (email) and set a password ("login credentials").
- Each email address must be unique to ensure that each account is distinctly identifiable.
- Account creation and identity verification must comply with AML/KYC obligations applicable to the **Company**.

Access Control

- Access to player accounts must be secured using a unique identifier and password.
- Access to account data by employees must be strictly role-based, on a need-to-know basis. Unauthorized personnel must not access sensitive player data or system functions.

Password Requirements

Passwords must be strong and secure, adhering to the following requirements:

- At least 8 characters in length;
- Must include uppercase, lowercase, numbers, and special characters;
- Must not be based on easily guessable information (e.g., names, dates of birth);
- Must be unique to the **Company's** systems and not reused from other services.

Players are encouraged to update their passwords periodically and must reset them if compromise is suspected.

Password Storage and Management

- Players' passwords must never be stored in plaintext and must be protected using strong one-way hashing algorithms with salt.
- Passwords must not be accessible to the **Company's** employees under any circumstances.

- A formal password reset process must be in place for players who experience login issues.

Players Responsibility

Players are solely responsible for keeping their login details safe and secure and should refrain from disclosing them to other individuals, including family members and friends.

Audit and Monitoring

- The **Company** must maintain detailed, tamper-proof logs of access to player information.
- Logs must be regularly reviewed to detect unauthorized access attempts.
- All financial transactions (deposits, withdrawals, adjustments) must be logged and subject to strict security controls.

Compliance and Training

- The **Company** ensures compliance with Curaçao data protection requirements and relevant international standards.
- Employees must receive regular training on secure password management and account security.
- Players must authenticate with at least their account identifier and password, and for critical actions (e.g., profile changes, withdrawals), multi-factor authentication (MFA) must be implemented.

Credit Card Information Management

Objective

To ensure the secure handling, storage, and processing of credit card information, and to protect sensitive cardholder data from unauthorized access, breaches, and misuse, thereby safeguarding the privacy and financial security of players. This policy is designed in compliance with the Payment Card Industry Data Security Standard (PCI DSS), the Curacao National Ordinance on the Protection of Personal Data (2010), and applicable international regulations.

Scope

This policy applies to all employees and contractors who have access to or manage credit card information within **Pointissimo**. It covers all systems, networks, and processes involved in the collection, transmission, storage, and disposal of credit card data.

Policy

- The **Company** does not store sensitive credit card data for player deposit transactions. Such data is only transmitted in encrypted form (TLS 1.2 or higher) directly to the payment provider.
- For user verification purposes only, the **Company** may collect images of credit cards, in which sensitive details are masked or blurred. These images remain encrypted at all times and cannot be used in their primary form.
- The **Company** applies strict data minimization principles, collecting and retaining only the minimum information required for processing and verification.
- All credit card data transmitted across the **Company's** systems is encrypted using industry-standard protocols to ensure confidentiality and integrity.
- Strict access control measures are implemented so that only authorized personnel with a legitimate business need can access credit card data. Access rights are logged, regularly reviewed, and updated.
- All employees who handle credit card information receive periodic training on information security, PCI DSS compliance, and data privacy to ensure they are aware of their responsibilities.
- Credit card data is retained only for as long as necessary for the stated business purpose and is securely disposed of in accordance with GDPR and PCI DSS requirements, ensuring it cannot be reconstructed or retrieved.
- The **Company** conducts regular security assessments, including vulnerability scans and penetration tests, to identify and remediate potential weaknesses, and maintains evidence of PCI DSS compliance.

Business Continuity Management

Objective

To counteract interruptions to business activities, protect critical business processes from the effects of major failures of information systems or disasters, and ensure their timely resumption in compliance with **Curacao Gaming Authority** requirements and international best practices.

Scope

The production infrastructure for **Pointissimo**.

Policy

- A managed process must be developed and maintained for business continuity that addresses both business and information security requirements necessary for the **Company's** operational resilience.
- Events that may cause interruptions to business processes must be identified, along with their likelihood, potential impact, and consequences.
- Plans must be developed and implemented to maintain or restore operations and ensure the availability of critical information and services at the required level and within the required timeframes following a disruption or failure.
- A unified framework of business continuity plans must be maintained to ensure consistency and to establish priorities for testing and maintenance.
- Business continuity plans must be regularly tested, reviewed, and updated to ensure their effectiveness and continued alignment with the **Company's** operational and regulatory obligations.

Compliance

Objective

To prevent breaches of any legal, statutory, regulatory, or contractual obligations by ensuring that **Pointissimo** operates in full compliance with applicable requirements.

Scope

This policy applies to all **Pointissimo** core operational processes.

Policy

- Statutory, regulatory, and contractual requirements must be explicitly defined, documented, and kept up to date.
- All licensing terms for the use of proprietary software products must be respected and enforced within **Pointissimo** and by all contractors and 3rd parties.
- Critical data must be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
- Data protection and privacy must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
- Managers must ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
- Managers must ensure that all regulatory data within their area of responsibility is securely maintained and available for the relevant analysis and reporting.
- Regulated information and content (i.e., Company policies, website Terms and Conditions, rules, privacy notices, etc.) are approved by the Compliance function; no changes can be deployed to production environments before such approval is obtained.