

Information Security Procedure

Cura Casino B.V

Version 1.0

Date: 1st August 2025

1. Policy Overview

It is the policy of Cura Casino B.V. that all information, in any form—written, spoken, electronically recorded, or printed—will be protected from unauthorized modification, destruction, or disclosure throughout its lifecycle. This protection includes securing the equipment and software used to process, store, and transmit that information.

All policies and procedures must be documented and accessible to the individuals responsible for their implementation and compliance. All activities governed by these policies and procedures must also be documented.

- All documentation, which may be in electronic form, must be retained for at least five years from its creation date or, for policies and procedures, from the date of the last change.
- All documentation must be periodically reviewed for relevance and accuracy. The review frequency will be determined by each entity within Cura Casino B.V.

Each entity or department may develop additional policies, standards, and procedures to detail the implementation of this policy. All departmental policies must be consistent with this overarching policy. New systems implemented after the effective date of this policy are expected to comply with its provisions where possible. Existing systems should be brought into compliance as soon as is practical.

2. Scope

The scope of this information security policy includes the protection of the **confidentiality, integrity, and availability** of information.

The framework for managing information security applies to all Cura Casino B.V. entities, workers, and other involved persons, as well as all involved systems throughout Cura Casino B.V. as defined in Section 4.

This policy and all its standards apply to all protected information in any form, as defined in Section 6, "Information Classification."

3. Risk Management

A thorough analysis of all Cura Casino B.V. information networks and systems will be conducted periodically to document threats and vulnerabilities. The analysis will examine both internal and external, electronic and non-electronic threats (e.g., natural disasters, man-made incidents) that could affect our ability to manage information resources.

- The analysis will document existing vulnerabilities that could expose information resources to threats.
- It will also include an evaluation of information assets and the technology used for their collection, storage, dissemination, and protection.

Based on the combination of threats, vulnerabilities, and asset values, an estimate of the risks to the confidentiality, integrity, and availability of information will be determined. The frequency of this risk analysis will be set at the entity level.

Based on the periodic assessment, we will implement measures to reduce the impact of threats by mitigating vulnerabilities.

Cura Casino B.V. uses various protection mechanisms to prevent unauthorized access to data and applications.

- **Firewall controls** are implemented to detect common network attacks such as DDoS, SYN floods, and eavesdropping.
- **DDoS attacks** are handled with the help of our Internet Service Provider (ISP), which assists in blocking attacking botnet IP addresses.
- **Stateful inspection** on the firewall checks higher-level protocols to protect applications from hacking through known code vulnerabilities.
- **Checksums** of application code on servers are compared daily against a reference database. Any changes are reported to the system administrator for review.
- **Anti-virus software** scans all files in system memory and on disks. Daily definition updates and disk scans are scheduled during off-peak hours to prevent virus infiltration.

4. Information Security Definitions

- **Affiliated Covered Entities:** Legally separate, but affiliated, entities that choose to be treated as a single entity for HIPAA purposes.
- **Availability:** Data or information is accessible and usable by an authorized person upon demand.
- **Confidentiality:** Data or information is not disclosed to unauthorized persons or processes.
- **Integrity:** Data or information has not been altered or destroyed in an unauthorized manner.
- **Involved Persons:** Every person working for Cura Casino B.V., including employees, contractors, consultants, and temporary staff.
- **Involved Systems:** All computer equipment and network systems within the Cura Casino B.V. environment. This includes all platforms, devices (PDAs, desktops, mainframes), applications, and data.
- **Risk:** The probability of a loss of confidentiality, integrity, or availability of information resources.

5. Information Security Responsibilities

5.1. Information Security Officer (ISO)

The ISO for each entity is responsible for working with management, owners, custodians, and users to develop and implement security policies, procedures, and controls, subject to the approval of Cura Casino B.V.

Specific responsibilities include:

- Ensuring security policies and standards are in place and followed.
- Providing basic security support for all systems and users.
- Advising owners on the identification and classification of computer resources.
- Guiding system development teams on implementing security controls from the design phase through production.

- Educating custodians and user management on security controls.
- Providing ongoing employee security training.
- Performing security audits.

5.2. Information Owner

The owner is typically the manager responsible for creating the information or the primary user. This role can be shared and may be delegated.

The Information Owner is responsible for:

- Knowing the information, they are responsible for.
- Determining data retention periods.
- Ensuring procedures are in place to protect the integrity, confidentiality, and availability of the information.
- Authorizing access and assigning custodianship.
- Specifying controls and communicating them to custodians and users.
- Promptly reporting any loss or misuse of information to the ISO.
- Initiating corrective actions when problems are identified.
- Promoting security education and awareness.
- Following all approval processes for the selection, purchase, and implementation of new systems.

5.3. Custodian

The custodian is generally responsible for processing and storing the information. They are responsible for administering the controls specified by the owner.

Responsibilities may include:

- Providing and/or recommending physical and procedural safeguards.
- Administering access to information.
- Releasing information as authorized by the owner or ISO, using privacy-protecting procedures.
- Evaluating the cost-effectiveness of controls.
- Maintaining security policies, procedures, and standards in consultation with the ISO.
- Promoting employee education and awareness.

- Promptly reporting any loss or misuse of information to the ISO.
- Identifying and responding to security incidents and initiating appropriate actions.

5.4. User Management

User management is responsible for overseeing their employees' use of information.

Responsibilities include:

- Reviewing and approving all access requests for their employees.
- Initiating security change requests to keep employee access current with their job functions.
- Promptly informing relevant parties of employee terminations or transfers.
- Revoking physical access for terminated employees (e.g., confiscating keys).
- Providing employees with necessary training for system use.
- Promptly reporting any loss or misuse of information to the ISO.
- Initiating corrective actions when problems are identified.
- Following all approval processes for the selection, purchase, and implementation of new systems.

5.5. User

A user is any person authorized to read, enter, or update information.

Users are expected to:

- Access information only in support of their authorized job responsibilities.
- Comply with all security policies, standards, and controls.
- Keep personal authentication credentials (passwords, PINs, etc.) confidential.
- Promptly report any loss or misuse of Cura Casino B.V. information to the ISO.
- Initiate corrective actions when problems are identified.

6. Information Classification

6.1. General Principles

Information is classified to ensure proper controls are in place to safeguard its confidentiality. Regardless of classification, the integrity and accuracy of all information must be protected. The classification is based on the most sensitive detail it contains, and the same classification must apply to all formats (e.g., electronic, print).

6.2. Confidential Information

This is highly sensitive material that must be restricted to individuals with a legitimate business need.

- **Examples:** Personnel information, key financial data, proprietary commercial research, system access passwords, and encryption keys.
- **Security:** Unauthorized disclosure may violate laws and regulations or cause significant problems. Access must be approved by the information owner.

6.3. Internal Information

This information is intended for unrestricted use within Cura Casino B.V. and, in some cases, with affiliated business partners.

- **Examples:** Personnel directories, internal policies and procedures, most internal emails.
- **Default Classification:** Any information not explicitly classified as Confidential or Public is, by default, Internal Information.
- **Security:** Unauthorized disclosure to outsiders may be inappropriate due to legal or contractual provisions.

6.4. Public Information

This information has been specifically approved for public release by a designated authority.

- **Examples:** Marketing brochures, public website content.
- **Disclosure:** This information may be disclosed outside of Cura Casino B.V.

7. Computer and Information Control

All involved systems and information are assets of Cura Casino B.V. and must be protected from misuse, unauthorized manipulation, and destruction through physical and/or software-based measures.

7.1. Ownership and Licensing

- **Software Ownership:** All software developed by or for Cura Casino B.V. is its property and must not be copied for use elsewhere unless the license agreement specifies otherwise.
- **Installed Software:** All software must comply with applicable licensing agreements and Cura Casino B.V. acquisition policies.

7.2. Virus Protection

- Approved virus-checking systems must be deployed using a multi-layered approach (desktops, servers, gateways).
- Users are not authorized to disable virus-checking systems.

7.3. Access Controls

Physical and electronic access to Confidential and Internal information and computing resources is controlled.

- **Authorization:** Access is granted on a "need to know" basis and must be authorized by the immediate supervisor and application owner with the ISO's assistance. This can be based on context, role, or user identity.
- **Identification/Authentication:** Unique user IDs and authentication are required for all systems containing Confidential and/or Internal information. At least one of the following methods must be implemented:
 - Strictly controlled passwords (see Section 9).
 - Biometric identification.

- Tokens in conjunction with a PIN.
- **Session Management:** An automatic timeout re-authentication is required after a maximum of 15 minutes of inactivity. Users must log off or secure the system when leaving it.

7.4. Data Integrity and Transmission

- **Data Integrity:** Mechanisms like transaction audits, disk redundancy (RAID), checksums, and encryption are used to ensure that information has not been altered or destroyed.
- **Transmission Security:** Technical security mechanisms, including integrity controls and encryption, are used to protect data transmitted over networks.

7.5. Remote and Physical Access

- **Remote Access:** Access from outside the Cura Casino B.V. network is granted on an individual basis using approved devices and pathways. Remote access to Confidential and Internal information must maintain the same level of protection as information accessed within the network.
- **Physical Access:** Access to areas where information processing occurs must be restricted to authorized individuals.
 - **Mainframe systems** must be in an access-controlled area protected from environmental hazards.
 - **File servers** must be in a secure area.
 - **Workstations and PCs** must be secured against unauthorized use with local procedures for physical safeguards, password-protected screensavers, and controlled access areas.
- **Facility Access:** Facility access controls must be in place to limit physical access while ensuring authorized entry. Policies and procedures must cover contingency operations, a security plan, access validation, and maintenance records.

7.6. Emergency Access

Each entity must have a documented mechanism to provide emergency access to systems and applications if the assigned custodian or owner is unavailable. Procedures must cover authorization, implementation, and revocation.

7.7. Equipment and Media Controls

The disposal of information must ensure the continued protection of Confidential and Internal information. Policies and procedures must govern the movement of hardware and electronic media.

- **Disposal:** Hard copies, magnetic media (hard drives), and optical media (CDs, DVDs) must be properly disposed of. Electronic drives are degaussed or overwritten. Non-functioning memory or storage is physically destroyed.
- **Accountability:** A record of the movement of hardware and electronic media and the person responsible must be maintained.
- **Backup:** A retrievable, exact copy of electronic data must be created before equipment is moved.

7.8. Other Media Controls

- **External Media:** Confidential information on external media (diskettes, memory sticks) must be protected from theft, labeled as confidential, and never left unattended in unsecured areas.
- **Mobile Devices:** Confidential information must not be stored on mobile devices (laptops, smartphones) unless they have power-on passwords, auto-logoff, and encrypted storage.
- **Personal Accountability:** The owner of any medium or device that results in a breach of confidentiality will be held personally accountable.

7.9. Data Transfer and Printing

- **Mass Data Transfers:** Downloading or uploading of Confidential and Internal information must be strictly controlled. Mass downloads for research must be approved by the Internal Review Board (IRB). All other mass downloads require application owner approval and must contain only the minimum necessary information.
- **General Transfers/Printing:** Confidential and Internal information should not be indiscriminately downloaded, copied, or printed, or left unattended.

7.10. Oral Communications

Staff should be mindful of their surroundings when discussing Confidential information, particularly when using cellular phones or speaking in public areas like waiting rooms, corridors, or restaurants.

7.11. Audit Controls

Hardware, software, and procedural mechanisms must be implemented to record and examine activity in information systems. Regular reviews of audit logs and access reports are required.

7.12. Contingency Plan

Controls must ensure that Cura Casino B.V. can recover from any damage to computer equipment or files within a reasonable timeframe. Each entity must have a plan for responding to system emergencies, including:

- **Data Backup Plan:** Documented and routinely updated plan to create and store retrievable copies of information. Backups must be stored off-site and protected.
- **Disaster Recovery Plan:** A plan to restore any lost data.
- **Emergency Mode Operation Plan:** A plan to ensure continued operation in the event of a disaster.
- **Testing and Revision:** Procedures for periodic testing of contingency plans.
- **Applications and Data Criticality Analysis:** An assessment of the criticality of specific applications and data to support the contingency plan.

8. Compliance

This policy applies to all users of Cura Casino B.V. information. Failure to comply may result in disciplinary action, up to and including dismissal, or termination of affiliation for external parties. Penalties associated with relevant legislation may also apply.

Disciplinary action may be instituted for, but is not limited to:

- Unauthorized disclosure of Confidential Information.
- Unauthorized use or sharing of passwords.
- Attempting to obtain another person's password.

- Unauthorized destruction of information.
- Installing or using unlicensed software.
- Attempting to gain fraudulent access to information.

9. Password Control Standards

The Cura Casino B.V. Information Security Policy requires the use of strictly controlled passwords for accessing Confidential and Internal information.

9.1. Standards for Accessing Protected Information

Users are responsible for complying with the following password standards:

- Passwords must never be shared, except with a designated security manager.
- Passwords must be changed regularly (every 45 to 90 days, depending on sensitivity).
- Passwords must have a minimum length of six characters.
- Passwords must not be saved when prompted by applications, except for ISO-approved central single sign-on (SSO) systems.
- Passwords must not be recorded where others can find them.

9.2. Password Creation

When creating a password, avoid using dictionary words or easily guessed personal information. Combinations of letters and numbers are more secure.

Where possible, system software must enforce the following:

- Passwords transmitted over a network must be encrypted.
- Passwords must not be displayed when entered.
- The system must enforce password changes and minimum length.

- The system must disable a user ID after more than three consecutive invalid passwords within a 15-minute timeframe, with a lockout of at least 30 minutes.
- The system must maintain a history of previous passwords and prevent their reuse.