

Cartwheel B.V

Information security Policy

Doc. Ref.	CMP-0.1	Version	1.0
Maintained by	Compliance		
Reviewed by	Compliance Manager & Information Security Manager		
Approved by	Compliance Manager & Information Security Manager		
Effective Date	30.10.2025	Classification	Internal

Document Control

Version	Date Approved / Issued	Author / Editor	Summary of Changes
1.0	30.10.2025	Compliance	Policy Creation

Table of Contents

Introduction and Context	3
Executive Summary	3
Scope and Applicability	3
Objectives	3
Roles and Responsibilities	4
Information Classification.....	4
Data Protection Measures	5
Virus Protection and Software Installation	5
Access Control	6
Physical Security	6
Non-Disclosure Agreements (NDAs)	6
Compliance	6
Password Control.....	6
Risk Management	7
Threat and Vulnerability Analysis.....	7
Risk Assessment.....	7
Implementation of Protective Measures	7
Safeguarding and Protection Mechanisms	8
DDoS Protection	8
Regular Security Evaluations	8
Secure Connections.....	8
Incident Response	8
Backup and Recovery	8
Oral Communications	8
Policy Review and Maintenance	9
Monitoring and Review	9
Continual Improvement.....	9
Conclusion	9

Introduction and Context

Executive Summary

This Information Security Policy (herein referred to as the “Policy”) outlines Cartwheel B.V’s (herein referred to as the “Company”) the framework for managing and securing information assets in compliance with the Curaçao Gaming Authority (CGA) under the National Ordinance on Games of Chance (LOK) and any associated regulations.

The Policy establishes the Company’s commitment to maintaining safe, responsible, transparent, and reliable gaming operations as required by the CGA and ensures the protection of all information assets from internal and external threats. It is designed to protect the Company’s information assets from all threats, whether internal or external, deliberate, or accidental.

This Policy is reviewed and approved by the Compliance Manager as well as the Information Security Manager who emphasizes the importance of information security in safeguarding the confidentiality, integrity, and availability of the Company’s data.

Scope and Applicability

This Policy applies to all employees, contractors, and third-party service providers of the Company, who have access to information systems and data. The scope of information security includes the protection of the confidentiality, integrity, and availability of information.

Objectives

The primary objectives of this Information Security Policy are to:

- Ensure all players financial and operational data are protected from unauthorized access, loss or misuse.
- Ensure the protection of player data protection and information security standards.
- Ensure players are able to play in a safe environment / safe manner without interruption of service.
- Maintain the confidentiality, integrity, and availability of all physical and electronic information assets.
- Define roles and responsibilities for maintaining secure information management.
- Promote staff awareness by providing information security training to all employees and contractors.
- Comply with legal and regulatory obligations concerning information security

Roles and Responsibilities

Information Security Manager

The full-time information Security Manager will be responsible for overseeing the implementation and maintenance of the information security program.

Responsibilities include (but are not limited to):

- Incident management and reporting
- Risk assessment
- System hardening (a collection of tools and techniques to reduce vulnerability in applications, systems, infrastructure, firmware, etc.)
- Penetration testing
- Security Audits
- Information Security awareness training

Employees and Contractors

All employees and contractors must adhere to this Policy, participate in security awareness training, and handle Company data responsibly. They are required to keep personal authentication devices (e.g. passwords, SecureCards, PINs, etc.) confidential; as well as, report promptly to the Security Operations Engineer the loss or misuse of the Company's information, and initiate corrective actions when problems are identified.

Information Classification

Classification is used to promote proper controls for safeguarding the confidentiality of information. Regardless of classification the integrity and accuracy of all classifications of information must be protected. The classification assigned and the related controls applied are dependent on the sensitivity of the information. Information must be classified according to the most sensitive detail it includes. Information recorded in several formats (e.g., source document, electronic record, report) must have the same classification regardless of format.

Information is classified into three levels:

- **Level 0 (Confidential):** Confidential Information is very important and highly sensitive material. This information is private or otherwise sensitive and must be restricted to those with a legitimate business need for access.
It includes customer accounts, names, emails, credit card information, contracts, and private employee information.

Unauthorized disclosure of this information to people without a business need for access may violate laws and regulations or may cause significant problems for the Company, its customers, or its business partners. Decisions about the provision of access to this information must always be cleared through the Information Security Manager

- **Level 1 (Internal Use):** Internal Use information is intended for unrestricted use within the Company and in some cases within affiliated organizations such as business partners. This type of information is already widely distributed within the Company, or it could be so distributed within the Company without advance permission. It encompasses application code, internal policies and procedures, and other internal-use-only data.

Any information not explicitly classified as Confidential or Public will, by default, be classified as Internal Use. Unauthorized disclosure of this information to outsiders may not be appropriate due to legal or contractual provisions.

- **Level 2 (Public):** Public information has been specifically approved for public release by a designated authority within each entity of the Company. Examples of Public information may include marketing brochures and material posted to the Company's internet web pages. This information may be disclosed outside of the Company.

Data Protection Measures

Virus Protection and Software Installation

All Company-owned and remote provider computers will be equipped with virus protection and necessary security software to mitigate the risk of viruses and intrusion.

To prevent virus infiltration, anti-virus software scans all files in system memory as well as those written to disks. Daily AV definition updates followed by disk scans are invoked at the time of least system load.

Virus-checking systems must be deployed using a multi-layered approach (desktops, servers, gateways, etc.) that ensures all electronic files are appropriately scanned for viruses. Users are not authorized to turn off or disable virus-checking systems.

The company's technical system setup has been tested in a controlled test environment by an independent qualified entity

Access Control

Access to information will be controlled and restricted based on role based access controls (RBAC) for all employees and vendors, using the following methods:

- Multi-factor authentication (MFA), for privileged accounts
- Access logs are retained for at least a minimum of one year.
- Remote service providers will be provided with a remote workstation to ensure secure access to company data.

Physical Security

Physical access to the Company's offices will be controlled through identification documents, keycards or biometric identification. All visitors are to be logged and escorted. Entry logs are recorded for all access points

Non-Disclosure Agreements (NDAs)

All employees and contractors must sign an NDA to ensure the confidentiality of sensitive information

Compliance

Compliance with this Policy is mandatory for all employees, contractors, affiliates, and third-party service providers.

Violations of this Policy will be met with disciplinary action, up to and including termination of employment or contracts

Password Control

This Policy requires the use of strictly controlled passwords for accessing Confidential Information and Internal Information.

Listed below are the minimum standards that must be implemented to ensure the effectiveness of password controls.

Users are responsible for complying with the following password standards:

1. Passwords must never be shared with another person.
2. Every password must, where possible, be changed regularly – (between 45 and 90 days depending on the sensitivity of the information being accessed).
3. Passwords must, where possible, have a minimum length of eight (8) characters and are composed of at least alphanumeric characters and/or symbols, or of a mix of lowercase and uppercase characters.

4. Passwords must never be saved when prompted by any application except for a central single sign-on (SSO) system as approved by the Security Operations Engineer. This feature should be disabled in all applicable systems.
5. Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
6. When creating a password, it is important not to use words are identical to their usernames and that can be found in dictionaries or words that are easily guessed due to their association with the user (i.e. children's names, pets' names, birthdays, etc.). Combinations of alpha and numeric characters are more difficult to guess.

Risk Management

The Company is committed to a comprehensive and proactive approach to risk management to ensure the confidentiality, integrity, and availability of its information assets. This involves a periodic and thorough analysis of all information networks and systems to identify and document potential threats and vulnerabilities.

Threat and Vulnerability Analysis

The analysis will cover a wide range of potential threats, both internal and external, natural and man-made, as well as electronic and non-electronic, that could impact the management of information resources. It will also identify existing vulnerabilities within the system that may expose information assets to these threats. This comprehensive evaluation will include the examination of information assets and the technology used for their collection, storage, dissemination, and protection.

Threat modelling is conducted regularly to identify risks from both internal and external sources. Vulnerability assessments and penetration tests are carried out periodically to ensure the continued security and resilience of systems.

Risk Assessment

By assessing the combination of identified threats, vulnerabilities, and the value of the information assets, The Company will evaluate the risks to the confidentiality, integrity, and availability of its information. The frequency of this risk analysis will be determined at the entity level, ensuring a timely and relevant assessment of potential risks. Controls and residual risks, resulting from any risk assessment, will be reviewed by the Senior Management team.

Implementation of Protective Measures

Based on the findings from the periodic risk assessments, the Company will implement measures aimed at mitigating the impact of identified threats. This will involve reducing the vulnerabilities within the system to minimize the scope and amount of potential exposure.

Safeguarding and Protection Mechanisms

The Company employs various protection mechanisms to prevent unauthorized access to data, application software, equipment, and networks. These include:

DDoS Protection

The network will be equipped with DDoS (Distributed Denial of Service) protection measures to safeguard against attacks aimed at disrupting service availability. This protection will help ensure that the Company's services always remain accessible to legitimate users.

Regular Security Evaluations

Regular evaluations will be conducted to detect any instances where malicious actors may have gained unauthorized control over computers previously deemed safe. These evaluations are critical in identifying and mitigating threats that could compromise our information systems.

Secure Connections

All connections to production and development environments will be secured using VPN (Virtual Private Network) software. This ensures that all data transmitted between users and our systems is encrypted and protected from interception or tampering.

Incident Response

All incidents affecting player data or platform integrity must be logged, investigated and reported to the Curaçao Gaming Authority (CGA) within the required time frame, with a Root Cause analysis (RCA) to be provided after the incident resolution

Backup and Recovery

Encrypted daily backups are maintained in multiple secure locations. Disaster recovery procedures are tested quarterly

Oral Communications

The Company's staff should be aware of their surroundings when discussing Confidential Information. This includes the use of cellular telephones in public areas. All staff should not discuss Confidential Information in public areas if the information can be overheard.

Caution should be used when conducting conversations in semi-private rooms, waiting rooms, corridors, elevators, stairwells, cafeterias, restaurants, or on public transportation. Moreover, the Company shall have in place secure communication protocol during player's activity.

Policy Review and Maintenance

Monitoring and Review

This Information Security Policy will be reviewed and updated annually, or as necessary, to reflect changes in legal, regulatory, or business requirements.

Continual Improvement

Any non-conformities, changes in business context, or changes in risk **shall** be reviewed and **may** trigger an update to this document to ensure its continued suitability and effectiveness.

Conclusion

By adopting these risk management strategies, the Company demonstrates its commitment to safeguarding its information assets against a wide array of threats. This proactive approach to security ensures the ongoing confidentiality, integrity, and availability of our information systems, thereby protecting the Company's business operations and the trust of its customers.