

Information Security Policy

Zerone B.V.

(License Holder – Curaçao Gaming Authority)

1. Purpose and Objective

This Information Security Policy defines the framework for protecting the integrity, confidentiality, and availability of all systems and data managed by Zerone B.V. It establishes responsibilities and technical guidelines to ensure compliance with Curaçao Gaming Authority (CGA) directives, as well as applicable data protection and cybersecurity standards.

The purpose of this policy is to ensure that Zerone B.V. and all third-party providers implement and maintain adequate safeguards for information assets related to gaming operations, customer data, and company communications.

2. Scope

This policy applies to:

- All contractors, service providers, and business partners working with Zerone B.V.;
- All systems and platforms used to operate the ClubR10 brand and related services;
- All information and communication channels through which customer, financial, or operational data is transmitted or stored.

Zerone B.V. operates exclusively through licensed third-party platforms, and does not develop or host proprietary systems. Therefore, this policy governs the secure use and oversight of these external systems and their integration into Zerone B.V.'s operations.

3. Responsibility

- Chief Operating Officer (COO): Responsible for approving and overseeing this policy and its implementation.
- Compliance Team: Monitors adherence to this policy, coordinates incident response, and communicates with regulatory authorities when required.
- Department Managers: Ensure that team members follow established security practices.
- All Employees: Must comply with this policy and immediately report any security incidents or suspicious activities.
- Third-Party Providers: Are contractually required to comply with internationally recognized information security standards.

4. Systems and Platforms

Zerone B.V. does not develop or host proprietary systems. All business operations are conducted through licensed and third-party platforms that meet security and compliance standards.

The following systems and providers are used:

a) Core Gaming Platforms

- Front-End and Back Office: Innovaplay

b) Customer Service

- Platform: HubSpot

c) Payments

- Processor: D24

d) CRM, Business Intelligence and Marketing Tools

- Tools: Google Cloud, Google Analytics, Google Sheets, N8N, HotJar, Mautic, Listmonk, MuDigital

Each system operates under its respective provider's infrastructure and security framework. Zerone B.V. oversees their compliance, monitors access permissions, and ensures data is only used for legitimate operational purposes.

5. Data Protection and Confidentiality

- All customer, transactional, and operational data must be protected against unauthorized access, loss, or alteration.
- Data may only be accessed by authorized personnel or service providers who require it for legitimate business functions.
- All data transfers must be conducted through encrypted channels.
- Zerone B.V. prohibits the use of personal emails or unsecured messaging platforms to share customer or business data.
- All contractors must sign a Confidentiality and Acknowledgment Agreement, confirming that they understand and agree to abide by this policy.

6. Access Control and Remote Access

- Access to systems must follow the principle of least privilege (only the minimum necessary permissions).

- All systems must require secure passwords and, when available, multi-factor authentication (MFA).
 - All remote connections to company systems must be made through secure and encrypted channels (VPN or equivalent zero-trust access solution).
 - Contractors using personal devices must ensure:
 - Updated operating systems and antivirus software;
 - Active firewall protection;
 - Password-protected user accounts.
 - The use of unauthorized or pirated software is strictly prohibited.
-

7. Network and Communication Security

- All data exchanged between Zerone B.V. and its partners must occur over encrypted HTTPS or equivalent secure protocols.
 - Sharing login credentials via unsecured channels (e.g., chat, email) is forbidden.
 - Contractors must immediately report any suspicious communication or phishing attempt to the COO.
 - Public Wi-Fi should not be used to access company systems unless a VPN or equivalent protection is active.
-

8. Physical and Environmental Security

Although Zerone B.V. operates remotely and does not maintain local servers or offices, all contractors must ensure the following minimum standards:

- Devices used for company operations must be physically protected from unauthorized access;
 - Screens should be locked when unattended;
 - Storage devices (USB, external drives) containing company data must be encrypted or securely erased after use.
-

9. Backup and Data Retention

All critical operational and customer data are stored within third-party systems that maintain automated backups (e.g., Google Cloud, HubSpot, Innovaplay). Zerone B.V. ensures that these providers comply with data retention and recovery standards.

Contractors must not create or store independent backups of company or customer data without authorization.

10. Incident Management

Any suspected or confirmed data breach, unauthorized access, or security vulnerability must be reported immediately to the COO. The COO is responsible for documenting and investigating all incidents and, when necessary, notifying the CGA in compliance with regulatory procedures.

Incidents must be recorded with:

- Date and time of detection;
 - Description of the issue;
 - Systems or data affected;
 - Corrective and preventive actions taken.
-

11. Third-Party Security Management

All service providers engaged by Zerone B.V. must demonstrate compliance with recognized security and privacy frameworks.

Periodic assessments are performed to ensure that:

- Access controls remain appropriate;
- Data processing agreements are up to date;
- Providers maintain data protection mechanisms equivalent to CGA expectations.

If a third-party provider fails to meet required standards, Zerone B.V. reserves the right to suspend access or terminate the relationship.

12. Employee Communication and Acknowledgment

Zerone B.V. operates exclusively through independent contractors, not direct employees. Each collaborator is required to:

- Review this Information Security Policy;
- Sign the Confidentiality and Acknowledgment Agreement confirming understanding and compliance;
- Follow all security practices outlined herein.

This acknowledgment serves as confirmation of individual awareness and replaces the need for formal in-person training.

13. Policy Review and Approval

This policy is reviewed annually or when significant operational changes occur. The COO maintains responsibility for version control and submission to the CGA as part of ongoing license compliance.

Approved by: XX - Chief Operating Officer (COO)

Operational Implementation: Compliance Team

Zerone B.V.

Date: _____
