

Information Security Policy

Version: 1.0

Effective Date: September 29, 2025

Prepared by: Compliance Officer

Approved by: Management Board

Classification: Confidential

1. Purpose and Scope

The purpose of this Information Security Policy is to define the governance framework for ensuring the confidentiality, integrity, and availability of information assets owned or managed by Famagousta B.V. This Policy applies to all employees, contractors, consultants, and third parties with access to company information systems or data. It covers all information assets, communication systems, networks, and physical premises utilized for company operations, including gaming and player data, financial records, and intellectual property.

2. Information Security Principles

Famagousta B.V. is committed to the following principles of information security:

- Confidentiality – Information shall be accessible only to authorized individuals.
- Integrity – Information shall remain accurate and complete, protected from unauthorized alteration.
- Availability – Information and systems shall be accessible to authorized users when required for legitimate business purposes.

3. Roles and Responsibilities

The Management Board shall ensure that this Policy is implemented, maintained, and reviewed annually. The Compliance Officer shall oversee all aspects of the information security framework, monitor compliance with regulatory obligations, and serve as the central authority for reporting and resolving security incidents. The IT Administrator shall implement and maintain appropriate technical and operational controls.

All employees and contractors are required to comply with this Policy and immediately report any suspected or confirmed information security incident.

4. Information Classification and Handling

All information assets shall be classified according to their sensitivity and handled in accordance with the following levels:

- Public – Information approved for public disclosure.
- Internal – Information restricted to internal use within Famagousta B.V.
- Confidential – Sensitive information including customer data, credentials, and financial records. Confidential data must be encrypted during transmission and storage.

4A. Data Protection and Privacy

Famagousta B.V. recognizes its responsibility as a data controller and is committed to protecting personal data in accordance with applicable privacy principles. All personal data shall be processed lawfully, fairly, and transparently, collected for legitimate business purposes, and retained only as long as necessary. Employees handling personal data must maintain strict confidentiality and ensure adequate safeguards against unauthorized disclosure, alteration, or destruction. Data subjects shall be informed of their rights and, where applicable, may exercise access or rectification requests through the Compliance Officer. Any personal data breach must be reported immediately to the Compliance Officer, who shall assess whether regulatory notification is required.

5. Access Control and Authentication

Access to information and systems shall be restricted based on the principle of least privilege. Each user shall be assigned a unique identifier; shared credentials are prohibited. Passwords shall contain a minimum of eight characters, include alphanumeric combinations, and be changed at least every ninety (90) days.

Multi-factor authentication shall be implemented where technically feasible. User access rights shall be reviewed annually or upon any employment change.

6. System and Network Security

All systems shall be protected by updated anti-malware software, firewalls, and intrusion detection mechanisms. Security patches must be applied promptly following validation. Remote connections shall utilize encrypted channels such as VPN. Only company-authorized devices may connect to the corporate network. The IT Administrator shall maintain system activity logs and review them for anomalies.

7. Incident Management

All personnel shall report any suspected or actual security incident to the Compliance Officer without delay. The Compliance Officer shall record the incident, coordinate investigation, and initiate corrective actions. Incidents involving data breaches or regulatory exposure must be escalated immediately to senior management. Post-incident reviews shall be conducted to prevent recurrence.

8. Physical and Environmental Security

Physical access to Famagousta B.V. premises shall be restricted to authorized personnel. Visitors must be signed in and accompanied at all times. IT equipment, laptops, and removable media shall be secured when unattended. Printed confidential materials shall be locked when not in use and disposed of securely via shredding.

9. Backup and Business Continuity

Critical data shall be backed up daily and stored in secure off-site or cloud repositories. Backup restorations shall be tested semi-annually. A Business Continuity Plan (BCP) shall be maintained to ensure resilience and recovery in the event of operational disruption or disaster.

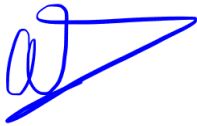
10. Training and Enforcement

All employees shall undergo information security awareness training during onboarding and periodically thereafter. Failure to adhere to this Policy may result in disciplinary measures up to and including termination of employment. Third-party service providers must comply with equivalent information security standards contractually enforced by Famagousta B.V.

11. Review and Approval

This Policy shall be reviewed at least annually or following significant operational or regulatory changes. The Compliance Officer shall ensure that revisions are approved by the Management Board and communicated to all relevant stakeholders.

Approved by: eMagnus Curacao B.V.



Director of Famagousta B.V.

Date: 10/27/2025