

Information Security Policy

IN-COM-040-01

Signed by:

eMagnus Curacao B.V., Managing Director



Date: 9/2/2025



1. Purpose of the Policy

The purpose of this Policy is to ensure a secure and responsible use of the Internet, corporate IT infrastructure, and other digital assets by all employees of Epicstar B.V., its affiliates, contractors and service providers (hereinafter collectively the “User”, “Users”). As Epicstar B.V. (the “Company”) operates within the online gambling sector, which is highly sensitive to data breaches, cyberattacks, and privacy violations, stringent controls are required to manage cybersecurity risks.

This Policy governs the use of internet access, mobile internet and telecommunications, internal IT systems, devices, Company-owned platforms, and servers. All users are expected to comply strictly with this Policy, under penalty of disciplinary, civil, administrative, or criminal liability.

2. Acceptable and Restricted Use

2.1 Authorized Use

Corporate networks and IT resources are provided for business purposes only. Any unauthorized use (including for personal purposes) is discouraged and may be restricted or revoked.

2.2 Prohibited Activities

Users must refrain from:

- Unauthorized access or use of any systems/accounts;
- Distribution of malware or other harmful software;
- Cyberbullying, harassment, or unethical behavior;
- Infringement of copyrights or licensing terms;
- Sharing confidential Company data or personal data without proper authorization;
- Using IT systems for phishing or fraudulent activities;
- Initiating or participating in cyberattacks (e.g., DDoS).

2.3 Handling of Personal and Confidential Data

Personal data shall only be processed based on legal grounds under the applicable laws, including but not limited to the General Data Protection Regulation (GDPR) and National Ordinance on the Protection of Personal Data of Curacao.

3. Access and Monitoring

3.1 Internet Use

3.1.1. All Internet traffic from Company-issued devices must pass through Company-controlled secure communication channels, such as corporate firewalls, secure proxies, or VPNs approved by the Information Security department.

3.1.2. Accessing the Internet using unsecured personal hotspots, USB modems, public Wi-Fi, or any other non-Company network is strictly prohibited.

3.1.3. Where public or external networks must be used (e.g., during business travel), users are required to initiate a secure VPN connection before accessing any Company resources.

3.1.4. Internet use must be consistent with the user's work responsibilities.

3.1.5. Downloading illegal software, torrents, or pirated content, visiting darkweb or hidden network resources is strictly prohibited.

3.2 Monitoring.

The Company reserves the right to monitor all user activity on corporate systems, including web access, email communications, data transfers, and device usage, to ensure compliance with this Policy and regulatory obligations under CGA rules.

4. Data Protection and Physical Security

4.1 Password, general rules

All users must adhere to the following password security requirements:

4.1.1 . Passwords must be at least 8 characters in length.

4.1.2. Passwords must include:

- At least one uppercase letter (e.g., B, W, T);
- At least one lowercase letter (e.g., b, w, t);
- At least one numeral (e.g., 3, 5, 7);
- At least one special character (e.g., &, \$, <, >).

4.1.3. Passwords must not include easily guessable information, such as names, birthdays, or simple sequences (e.g., "123456", "password").

4.1.4. Passwords must not be reused across multiple systems.

4.1.5. Examples of strong password combinations include: C@r!b3aN, H4mp\$hirE, M4!@y\$IA.

4.1.6. Passwords must be changed at least once every 90 days.

4.1.7. Users are encouraged to change passwords immediately if they suspect compromise.

4.1.8 Password sharing between users or with external parties is strictly prohibited under all circumstances.

4.1.9. In the event of a forgotten password, users must follow the Company's official password recovery procedure through the IT support.

4.1.10. If a password compromise is suspected, the user must immediately reset the password and notify the Information Security Department.

4.2 Printed Information

4.2.1. Physical copies of sensitive or confidential documents must only be printed when absolutely necessary and in the minimum number of copies required.

4.2.2. Printed materials must not be left unattended on desks, printers, or in meeting rooms.

4.2.3. When no longer needed, printed confidential materials must be disposed of securely using approved shredding facilities.

4.2.4 Users must prioritize the use of **secure digital document management systems** over printing, in accordance with the Company's environmental and information security initiatives

4.3 Device Handling

4.3.1 All Company-issued devices (laptops, mobile phones, external storage media) must be physically secured at all times.

4.3.2. When traveling, devices must never be left unattended in public or unsecured spaces (cafes, airports, hotel lobbies).

4.3.3. Any loss, theft, or suspected tampering of devices must be reported immediately to the System Administrator.

4.3.4. All critical business data must be stored on Company-approved cloud services (e.g., Google Workspace).

5. Incident Reporting

5.1. All users must immediately report the following incidents to the Information Security Department:

- Detection of malware;
- Abnormal device behavior;
- Missing or altered files;
- Suspected social engineering or phishing;
- Lost or stolen equipment;
- Unauthorized access or password issues;
- Any interactions with government authorities involving Company hardware.

6. Regulatory Compliance

6.1 Compliance with CGA Minimum Control Standards

This Policy is designed in alignment with the Minimum Control Standards (MCS) issued by the Curacao Gaming Authority, specifically Section C on "IT Security and Data Management". All procedures herein are subject to internal audit and external assessment, where required.

6.2 Alignment with International Standards

The Company aims to align with the principles and controls of ISO/IEC 27001:2022, ensuring continual improvement of the information security management system (ISMS).

6.3 Internal and External Audits

An internal review of IT security practices shall be conducted at least once annually. Where applicable, an external IT audit by an independent security provider will be arranged to meet the expectations of the CGA and stakeholders.

7. Remote Access

7.1 Secure Remote Work Practices

Users accessing Company systems remotely must:

- Use Company-approved VPN with mandatory two-factor authentication (2FA);
- Only connect from devices that meet Company security standards (antivirus, encryption, OS updates);
- Avoid the use of public or unsecured Wi-Fi unless access is routed through encrypted Company channels.

7.2 Device Control and Confidentiality Outside Office

All users working remotely must:

- Avoid saving files locally when cloud access is available;
- Lock or encrypt devices when traveling;
- Refrain from sharing Company devices or logins with any third parties, including family members.

8. Roles and Responsibilities

8.1 Designated Security Officer

The Information Security Officer is responsible for IT security governance and implementation oversight. Responsibilities include:

- Responding to security incidents;
- Identify violations and investigate cases;
- Block necessary accesses;
- Initiate disciplinary actions process;
- Monitoring compliance with this Policy;
- Coordinating audits and training.