

INFORMATION SECURITY POLICY

Please read this information carefully for your own benefit.

www.coinhero.io is operated by Gatepost N.V. having its office at Landhuis Zuikertuintje, Zuikertuintje z/n, Willemstad, Curacao. Company Registration number 163081.

Document Version

Revision	Date	Security Class	Responsible Person	Purpose
V1.0	01.02.2024	Confidential	CO	Creation & Approval
V1.1	11.12.2025	Confidential	CO	Updated Policy with LOK Requirements

1. INTRODUCTION

Storage of any data on computers and transfer across the network eases use and expands our functionality. Commensurate with that expansion is the need for the appropriate security measures.

The Information Security Policy recognizes that not all business functions within the Company are the same and that data are used differently by various units.

The Policy is written to incorporate current technological advances. Instances of non-compliance must be reviewed and followed up by the Chief Technology Officer.

This Information Security Policy should be disseminated to all users including vendors, contractors, and business partners. This information security policy should be reviewed and updated on an annual basis. All employees must sign an agreement verifying they have read and understood this document.

2. PREAMBLE

Should positions within the Company, referred to within policies and procedures, be vacant, the Chief Technology Officer is vested with all the applicable responsibilities. The Chief Technology Officer is authorised to engage consultants and experts in meeting his responsibilities relating to technical, legal and similar issues.

2.1. PURPOSE, OBJECTIVE & SCOPE

By information security we mean protection of the Company's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose and objective of this Information Security Policy is to protect the Company's information assets, including data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation, from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage.

The purpose of the information security policy is:

- a. To establish an operation-wide approach to information security.
- b. To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of data, applications, networks and computer systems.
- c. To define mechanisms that protect the reputation of the Company and allow the same to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- d. To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

2.2. RESPONSIBILITY

The Chief Technology Officer is responsible for the regular updating, review, approval, publishing and implementation of the Information Security policy, management of information security and to provide advice and guidance on information security.

The Chief Technology Officer must ascertain that appropriate training is provided to data owners, data custodians, network and system administrators, and users.

Managers / Directors are directly responsible for implementing the Information Security Policy within their business areas.

3. GENERAL POLICY

The Company adopts a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the operation's data, network and system resources.

Vulnerability and risk assessment tests of external network connections are conducted on a regular basis.

Information must be protected from a loss of confidentiality, integrity and availability.

Regulatory and legislative requirements must be met.

Business continuity plans must be produced, maintained and regularly tested.

Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

Education and training must be provided to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This must be tailored to the role of the individual network administrator, system administrator, data custodian, and users.

All breaches of information security, actual or suspected, must be reported to, and investigated by, the Chief Technology Officer. The appropriate Incident Reporting procedures must be followed.

Other guidance and procedures (such as system access control and backup procedures) within the company procedures manual support this policy.

It is the responsibility of each employee to adhere to the Information Security Policy.

All employees have a responsibility to conduct themselves in an ethical manner.

Non-compliance with this Policy will be subject to Management review and action in conformance with the Company's disciplinary procedures.

4. DATA CLASSIFICATION POLICY

It is essential that all data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. Three classes of data have been identified:

- a. **High Risk** - Information assets over which there are legal requirements for preventing disclosure. Data covered by local and international legislation, are in this class. Payroll, personnel, gaming, player and financial information are also in this class because of privacy requirements. This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the Company if disclosed or modified. The data owner should make this determination. Access to High Risk data must be controlled from creation to destruction, and will be granted only to those persons who require such access in order to perform their job ("need-to-know"). Access to High Risk data must be individually requested and then authorized by the Data Owner who is responsible for the data. In addition, the dissemination of such information with third parties is prohibited from doing so without the express confirmation in writing by a member of the Executive Team and preferably the right of the third party to receive such information should be prescribed in a contract.
- b. **Confidential** - Data that would not expose the Company to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. Access to such data shall be by default given solely to employees who maintain a managerial role within the company. Access to other employees may be given on a 'need to know' basis. The dissemination of such information requires the express confirmation by a member of the Executive Team.
- c. **Public** - Information that may be freely disseminated. Access to such information need not be controlled although specific guidelines may be issued by the Executive Team if they perceive the dissemination such information to be harmful to the business.

No system or network subnet can have a connection to the Internet without the means to protect the information on those systems reflecting its confidentiality classification.

Data custodians are responsible for creating data repositories and data transfers which protect data in the manner appropriate to its classification.

High risk data and confidential data must be encrypted during transmission over insecure channels.

All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

5. ACCESS CONTROL / PASSWORD POLICY

Data must have sufficient granularity to allow the appropriate authorized access. There needs to be a balance between protecting the data and permitting access to those who need to use the data for authorized purposes.

Access to the network and servers and systems should be achieved by individual and unique logins and should require authentication. Authentication includes the use of passwords, or other recognized forms of authentication, such as 2FA.

All systems which store user passwords must do so using non-reversible encryption.

All systems which store sensitive player information such as player passwords and player payment information must do so using non-reversible encryption.

Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. Exceptions may be allowed under specific scenarios and under specific authorisation by the Chief Technology Officer. All users must secure their username or account, password, and system access from unauthorized use.

Users are accountable for the security and use of their user accounts and passwords.

System user accounts should regularly be reviewed and audited for malicious, obsolete, and unneeded accounts. Inactive accounts should be disabled.

Passwords associated with Logon IDs must comply with the Password policy of the Company. All users must have a strong password. Basics for creating a strong password include minimum length being of eight characters which should include a mix of uppercase, lowercase, and numerical characters. Empowered accounts, such as administrator, must be at least eight characters long, contain at least one numerical and one special character, and be regularly changed.

Should a user of any system forget his or her password, the password will be reset by the systems administrator. The system must prompt the users to enter a new password immediately upon the first login attempt.

All system passwords must be changed every 42 days for security purposes.

Encrypted passwords should be enabled on any devices where it is not on by default.

Back-end systems should have an automatic inactivity log-off period of 1 hour.

Users who leave their workstations must lock their workstation or log off to prevent unauthorized access. Users which fail to comply with this policy will be held liable for the use of their account and disciplinary action may be taken.

Default passwords on all systems must be changed after installation.

Terminated employees should have their accounts disabled.

Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

Accounts should be locked automatically after multiple password failures in any system which supports such functionality. If a system does not support such a feature, the Chief Technology

Officer should regularly review the access logs of that system, to ensure that user accounts are not being mismanaged.

Activities performed as administrator or super user must be logged by the system and where the system does not allow such logging, compensating controls put in place.

Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks.

System logs should be reviewed regularly.

6. NETWORK SECURITY POLICY

The company hardware and media is co-located on the premises of a Tier-IV certified data centre registered in Curacao.

All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk and/or confidential.

All systems connected to the Internet should have a vendor supported version of the operating system installed.

All systems connected to the Internet must be current with security patches.

System integrity checks of host and server systems housing high risk data should be performed.

All player activity shall be communicated over a secure communication protocol.

6.1. FIREWALLS

Firewalls should be configured to "Deny" all traffic that is not explicitly "Allowed".

Firewalls should filter both inbound and outbound (ingress and egress) connections, limiting them to that which is required to conduct business.

6.2. SERVERS AND WORKSTATIONS

Databases will only store entire credit card details if the company acquires a PCI compliance certificate. The company currently encrypts all credit card details stored in the database.

Publicly accessible web servers should be located on a network which is both logically separated and secured from the internal systems network.

Mobile computers that connect to the internet must have a personal firewall and up-to-date anti-virus software installed.

Antivirus scanners should be installed on all servers and workstations and should be updated with the latest virus definitions.

All development, testing, and production systems should be updated with the latest vendor security patches.

6.3. ASSET DEPLOYMENT AND MAINTENANCE

All changes to firewalls must be reviewed and authorized by the Chief Technology Officer and logged for future reference.

Changes to the production environment should be authorized and logged before being implemented.

When an employee leaves the company, that employee's company user accounts and passwords should be immediately revoked.

Remote maintenance accounts should be enabled when needed and disabled when the maintenance process is completed.

Access to sensitive data should be logged where practically possible.

Successful and unsuccessful login attempts and the accessing of the audit logs should be logged.

System clocks should be synchronized, and log files should contain date and time stamps.

The firewall, router, and wireless access point logs should be regularly reviewed for unauthorized traffic.

Audit logs should be regularly backed up, secured, and retained for at least three months online and one year offline for all critical systems.

Wireless analyzers should be periodically run to identify all wireless devices.

Vulnerability scans or penetration tests should be performed on all applications and systems before they are put into a production environment. Before going into production, all devices must undergo a lockdown procedure where unnecessary or default services, protocols, settings, accounts, and passwords are changed or disabled.

Only secure, encrypted communications should be used for remote administration of production devices.

6.4. PHYSICAL SECURITY AND ACCESS CONTROL

Equipment and media containing sensitive information should be physically protected from unauthorized access.

The distribution and disposal of backups and other media containing sensitive information should be in accordance with a procedure approved by the Chief Technology Officer.

Media that contains sensitive information should be inventoried and securely stored.

Media that contains sensitive information should be deleted, shredded, or degaussed before disposal.

6.5. WIRELESS COMMUNICATIONS

All wireless access points must be configured with encryption, MAC filters, or technology that limits access to those devices that are explicitly authorized.

Networks with wireless access should be separated by a firewall from networks that handle sensitive information.

Wireless access points that support WPA2 should be configured to use it.
Wireless communications should be encrypted with WPA2, or 128-bit SSL.

6.6. VIRUS PREVENTION POLICY

The introduction of computer viruses into the Company's environment is prohibited, and violators may be subject to prosecution.

All desktop systems, servers and workstations that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept/automatically updated.

Headers of all incoming data including electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned.

System or network administrators should inform users when a virus has been detected.

Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Users must not tamper with or disable anti-virus software installed on their workstations.

Users must do their best to contain any spread of malicious software within the company's environment.

6.7. INTRUSION DETECTION

Intrusion detection and security monitoring is very important to protect resources and data. This section is the policy and guideline over intrusion detection implementation of the organizational networks and hosts along with associated roles and responsibilities. Every host on the organizational network and the entire data network are covered. The ISO should ensure:

- An increased level of security via active searching for signs of unauthorized intrusion.
- Prevention or detection of any threats to the confidentiality of organizational data on the network.
- Preservation of the integrity of organizational data on the network.
- Prevention of unauthorized use of organizational systems.
- Hosts and network resources are continuously available to authorized users.
- Increased security by detecting weaknesses in systems and network design early.

All systems accessible from the internet or by the public must operate ISO approved active intrusion detection software during anytime the public may be able to access the system.

All host based and network-based intrusion detection systems must be checked on a daily basis and their logs reviewed.

All intrusion detection logs must be kept for a minimum of 30 days.

Any suspected intrusions, suspicious activity, or system unexplained erratic behaviour discovered by administrators, users, or computer security personnel must be reported to the ISO which may report incidents in line with the respective policy.

7. SECURITY AWARENESS POLICIES

7.1. EMAIL POLICY

Email equipment and messages are property of the Company.

Messages that are created, sent or received using the Company's email system are the property of the Company.

The Company reserves the right to access and disclose to relevant entities the contents of all messages created, sent or received using its email system.

Users must be very careful when opening email attachments.

All email communication must be handled in the same manner as a letter, fax, memo or other business communication.

Sensitive data in the email or any attachments must not be transmitted in clear text over the Internet.

No copyrighted or proprietary information is to be distributed via the Company's email system.

Any urgent Virus warnings should be channelled to the Chief Technology Officer for verification of authenticity.

Email messages should not have any content that may be considered offensive or disruptive. Offensive content includes but is not limited to obscene or harassing language or images, racial, ethnic and sexual or gender specific comments or images or other comments or images that would offend someone on the basis of their religious or political beliefs, sexual orientation, national origin or age.

Employees may not retrieve or read email that was not sent to them unless specifically authorised by the Chief Technology Officer or by the email recipient.

Employees may not execute attachments to emails received when these are executable files.

Company email may not be used for personal reasons.

7.2. PORTABLE COMPUTERS AND MEDIA POLICY

Personnel computers, laptops and workstations issued by the organization are viewed as the company's assets and must be adequately protected.

Laptops, and their peripherals are popular targets for thieves. Since these assets are highly vulnerable to unauthorized access or theft, they present unique risks in the areas of disclosure, modification or destruction of proprietary information.

During the normal workday, whether working in an office or at an off-site location, employees are strongly encouraged to use a security cable to fasten the laptop to a desk, chair or other fixed object.

Employees should never leave a laptop on the desk, in the work area or in any other visible location overnight. Portable media should be locked in a secured area at the end of the workday.

When transporting a laptop or peripheral, employees should never leave it unattended in a visible location or in an unlocked vehicle.

When travelling with a laptop never check it with other baggage.

In the event a laptop is stolen (regardless of where the theft occurs), employees should immediately file a police report and notify the Chief Technology Officer immediately. A copy of the police report should be submitted to the Chief Technology Officer/ Management Team.

All assigned laptops, peripherals, related equipment and media remain the property of the company and are to be returned upon request, or when a staff member leaves.

All of the organisations' owned or leased facilities, equipment, related components and resources should be protected from unauthorized physical access, damage, loss from theft or other risks.

All media that becomes obsolete such as PCs, hard-drives, USB memories, CDs must be handed in to the Information Technology & Technical/ Management Team for proper disposal in accordance with the media disposal policy.

Adequate building security should be provided, and all facilities should be well-maintained, clean and free from safety or fire hazards.

Users must ensure that their portable PC is securely stored when not in use.

When outside of the office, employees should avoid leaving their PC unattended in their car. If it is inevitable to leave a PC in a car, it should be stored out of sight, e.g. in the boot.

PCs must never be left unattended while travelling on public transport.

7.3. ACCEPTABLE USE & ETHICS

Any computer resources must be used in a manner that complies with the Company's policies.

The company will monitor the use of office systems.

All control system events are logged.

Unauthorised access to office systems is an offence.

It is against our policy to install or run software requiring a license on any computer without a valid license.

Use of the Company's computing and networking infrastructure by employees unrelated to their positions must be limited.

Use of the Company's computer resources for personal profit is not permitted.

Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations.

All data contained on, or passing through corporate assets is subject to monitoring and remains the property of the corporation.

Under no circumstances is an employee authorized to engage in any activity that is illegal under local or international law while utilizing company-owned resources.

Employees must not use company accounts to post publicly accessible messages or posts without permission.

Users are expressly forbidden to install any software on their workstations without prior approval from their supervisor.

Portable personal media should not be connected to company equipment and should not contain company documents.

Users may not perform vulnerability scans, monitor network traffic, or perform any action that is designed to escalate privileges or gain access to information that was not expressly intended for them.

Users must not reveal any information about company clients, employees, business practices, technology, schedules, or any other information not already publicly available to any outside resource or person without expressed permission from their supervisor.

Users must not use their company email accounts for purposes other than the conduct of company business. Forbidden actions include any and all forms of harassment, phishing, solicitation, spamming, forwarding chain letters and pyramid schemes, conducting personal business, and general personal correspondence.

7.4. CLEAN DESK AND CLEAR SCREEN POLICY

Clear desk and clear screen policy used to reduce the risks of unauthorized access to, or loss of, or damage to, information.

Ensure that appropriate facilities are available in the office in which, depending on their security classification, computer media (disks, tapes, CDs) and paper and paper files can be stored and locked away, including in lockable pedestals, filing cabinets and cupboards.

Personal computers should be switched off when not in use and should be password protected.

Everyone should be required to use a password protected screen saver that automatically fires up after only a few minutes of inactivity.

Incoming and outgoing mail collection points should be protected or supervised so that letters cannot be stolen or lost, and faxes and telexes should be protected when not in use.

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

8. Security in Supplier Relationships Policy

Purpose

The purpose of this policy is to ensure proper protection of the Company's assets that are accessed by suppliers.

Scope

This Security in Supplier Relations Policy applies to all business processes and data, information systems and components, personnel, and physical areas of the Company.

Policy

Information Security in Supplier Relationships:

- Procedures surrounding risk mitigation of a supplier's access to [the Company's assets must be documented, reviewed, and agreed upon by the Company and the specific supplier.
- All suppliers that access, process, store, or provide various IT components must be in agreement with the Company's security requirements around suppliers' relationship with the assets.
- Types of information access should be defined that different types of suppliers will be allowed, as well as monitoring and controlling the access.
- Types of obligations applicable to suppliers should be defined to protect the organization's information.
- Security requirements agreements for suppliers must also include details on addressing risks surrounding the handling, processing, and communicating of assets or services.
- processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
- Legal and regulatory requirements, including data protection, intellectual property rights, and copyright, etc. should be clear identified and addressed.

Supplier Service Delivery Management:

- A process must be developed to monitor and assess the service delivery of a supplier to ensure it is meeting appropriate business and security requirements, as well as meeting any contract or SLA requirements.
- A change management process must be in place to address any alterations to an existing policy, including documentation of said change and ensuring it is in alignment with business processes and follows appropriate re-assessment of risk involved, if necessary.

9. THIRD PARTY ACCESS POLICY

Third parties occasionally conduct business/provide services to the Company and thus require network communication. Access is only given to third parties after request is received from one of the company Executives who must also specify the level of access required by such person which must be assigned by the Chief Technology Officer.

The following guidelines apply in giving access to third parties:

- The third party must be covered by a contractual undertaking which binds the third party to security measures which are equivalent to the measures specified within the security policies of the company. Where no such contractual undertaking is present, the third party must sign a declaration confirming acceptance of the security policies of the company.
- Access to third parties must respect data protection laws. The third party shall only be given access to the databases of the company where it is absolutely necessary for the third party to have access to them given the nature of the work and service the third party must provide to the company.
- Where a third party requires a remote connection to the company's network the remote access policy shall be read in conjunction with this policy. The third party's access shall be closely monitored and removed immediately when the purpose for which it was given has been exhausted.
- All third party network connections will be reviewed on a yearly basis and information regarding specific third party network connection will be updated as necessary. Obsolete third party network connections will be terminated immediately.
- Third party access to contracted service providers must be terminated as and when software contracts are terminated/expired.

DOCUMENT, EQUIPMENT AND MEDIA DISPOSAL

This document explains the company's procedure to make sure that information is not made available to unauthorized personnel in case any equipment / media is to be removed from the premises mentioned above or in case that a piece of equipment is to be made entirely redundant.

Equipment / Media containing confidential data must be marked "Confidential" to indicate this without requiring it to be read.

Faulty Equipment / media located at the ISP; If any equipment / media is faulty it will have to be replaced by the ISP providing such equipment. Changes will be carried out by authorized personnel at the ISP and if need arises by an appointed third party authorized personnel. Personnel authorization forms will be provided and kept up to date with the ISP to ensure that only authorized persons can enter the data centre and work on the company's servers. In case of faulty hardware / media and emergency action required, the Chief Technology Officer and the appointed third party authorized personnel shall have 24 hour access to the data centre. The CGA may be informed about the particular incident through the submission of an incident report within 24 hours after the incident. If any equipment needs to be removed from the data centre then the approval of the Chief Technology Officer must be sought and if needed included within the Incident Report submitted to the CGA within 24 hours of decommissioning. Any equipment /media that is to be removed from the data centre falls under the Chief Technology Officer's care and custody.

Hardware / media that has been cleared for removal from the data centre and for its subsequent disposal/recycling is to first be checked to ensure that it contains no data or information. The Chief Technology Officer will then be responsible for the full disposal/recycling. Hardware / media will be demagnetized / degaussed prior to manual disposal / recycling. Any failing hard drives will be immediately exchanged for new hard drives. Failing hardware / media that does not contain any data will be destroyed and disposed of / recycled. If any equipment is to be installed to replace the faulty equipment the installation will be completed to allow the operation to continue, notifying the CGA of the new equipment where applicable.

Faulty Equipment / media located at the Office; Hardware / media that is to be disposed of will be safely stored in locked cabinets under supervision of the Chief Technology Officer. The Chief Technology Officer will be responsible for the hardware being demagnetized prior to manual destruction and will then be disposed of.

Redundant Equipment / media located at the ISP; In case of any equipment at the data centre that is to be made redundant the CGA will be notified through the submission of an incident report or the relevant notification form where required. The hardware will be demagnetized / degaussed and the Chief Technology Officer will then be responsible for disposal / recycling.

Redundant Equipment/ Media located in the office; The hardware / media will be safely stored in a locked cabinet under the supervision of the Chief Technology Officer. If it is to be disposed of it will be demagnetized / degaussed prior to disposal / recycling.

Company documents should be shredded prior disposal.

An incident report with the full explanation and action taken will be submitted to the CGA within 24 hours of the occurrence of any of the following issues:

- a) any gaming security breaches that (may) have compromised personal information of gamblers or game details, along with measures taken in response;
- b) failure or loss of, or damage to, all or part of the equipment or software that (may have) resulted in the loss of all or part of the Remote Games of Chance offered, along with measures taken in response;
- c) gaming-related (attempted) fraud or other forms of criminal behavior of players, along with measures taken in response;
- d) any other behaviors or events that may pose a serious threat to the responsible, reliable, and verifiable organization of the Games of Chance offered, or that may undermine the public trust in the responsible, reliable, and verifiable organization of the licensed Games of Chance.

If the incident is a planned incident, then the CGA will be given prior notice and authorization requested when necessary.