

Overseas Gaming Management N.V.

Information Security Policy

Version: 2.0

Date: 13th November 2025

CONFIDENTIALITY STATEMENT

This document is strictly confidential and has been prepared solely for the purpose of regulatory review by the Curacao Gaming Authority (CGA). It contains proprietary, commercially sensitive, and operationally confidential information belonging to the Company. No part of this document may be disclosed, reproduced, distributed, or used for any purpose other than its intended regulatory submission, without the express prior written consent of Overseas Gaming Management N.V. Unauthorized use or disclosure of the contents herein is strictly prohibited and may result in legal or regulatory action.

Version Control

Version	Date	Description	Status	Next Review Date
1.0	11.08.2025	Creation of Policy	Approved	
2.0	13.11.2025	Updated in line with feedback	Approved	13.11.2026

Change and Review History

Version	Date	Description of Changes	Reviewed/Approved By
1.0	11.08.2025	Policy Creation and Approval	Head of Compliance
2.0	13.11.2025	Updated on feedback received	Head of Compliance

Table of Contents

1	Introduction	5
1.1	Policy	5
1.2	Responsibilities.....	5
1.3	Compliance.....	6
1.4	Training.....	7
1.5	Risk Management.....	7
2	Acceptable Use	7
2.1	Purpose.....	8
2.2	General Use	8
2.3	Commercial Security Information	9
2.4	Protection of Players	9
2.5	Unacceptable Actions.....	9
2.6	Third-Party Controls	10
3	Email Policy.....	11
3.1	Usage	11
4	Internet Security and Usage	12
4.1	Usage	12
5	Network Firewalls.....	13
5.1	Firewall Rules Configuration	13
5.2	Documented Firewall Rules	13
5.3	Network Security and Protection.....	13
6	Cryptography Control	14
7	Monitoring of System	14
8	User Management	15
8.1	Policy Control and Authorisation	15
8.2	User Access Termination	16
8.3	Automatic Log-off.....	17
8.4	Login Attempts	17
8.5	Adherence	17
9	Anti-Virus	18

10	Laptops and Portable Devices Security.....	18
11	Removable Media	19
12	Equipment and Media Disposal	20
13	Data Classification.....	20
13.1	Asset Inventory.....	21
14	Incident Response Plan	22
14.1	Triage and Identification	23
14.2	Escalation	23
14.3	Containment and Mitigation	23
14.4	Investigation and Analysis	23
14.5	Review and Lessons Learned.....	24
14.6	Recordkeeping.....	24
15	Conclusion.....	24
16	References	25

1 Introduction

Information is regarded as a key asset for Overseas Gaming Management N.V. (“Overseas” or “the Company”), and as such, it is essential to implement appropriate measures to protect it against unauthorized access, alteration, disclosure, or destruction. This policy applies to all information owned, processed, or maintained by the Company, regardless of whether it is stored electronically, physically, or in any other format.

The policy is applicable to all employees, officers, contractors, and any other personnel associated with the Company, irrespective of their role, location, or relationship with the Company. Additionally, as the Company may outsource certain functions or activities to external service providers, this policy also covers any Company information accessed, processed, or stored by such service providers and their personnel.

To ensure operational resilience, the Company develops and maintains a comprehensive Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). These plans define recovery objectives, including Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), and establish procedures for maintaining critical business functions during disruptive events. Both the BCP and DRP are regularly tested through simulations and drills to validate their effectiveness, identify gaps, and ensure that staff and service providers can respond effectively to incidents affecting systems, data, or operations. All findings from tests are documented and used to continuously improve continuity and recovery procedures.

1.1 Policy

The Company is committed to the effective protection and management of its information assets. This includes preventing unauthorized access, ensuring the confidentiality and integrity of information, and maintaining its availability for authorized use. All measures are designed to comply with applicable regulatory and legislative requirements.

Business continuity plans are established, regularly tested, and maintained to ensure operational resilience. Information security awareness is actively promoted among all employees, and any actual or suspected information security incidents are promptly reported, investigated, and remediated.

1.2 Responsibilities

The Director & CEO of the Company assumes direct responsibility for overseeing the maintenance of this policy and providing strategic guidance on information security, ensuring its effective implementation across all business areas. To strengthen governance, the Company shall appoint a Chief Information Security Officer (CISO), who will report directly to the Board of Directors and be responsible for the overall management, monitoring, and continuous improvement of the Company’s information security

framework. Management is tasked with enforcing this policy within their respective areas, ensuring that all employees understand their obligations to safeguard the Company's assets and adhere to established security standards and procedures.

All employees are required to conduct themselves ethically, refrain from misusing data or information obtained inappropriately, and avoid exploiting system weaknesses. Each user is accountable for diligently performing their responsibilities and will be subject to disciplinary action for any misuse of the Company's computer systems. In cases where the confidentiality or classification of information is uncertain, it must be clarified before use. Any known violations, system weaknesses, or security incidents including intrusions must be promptly reported to the relevant security personnel, line manager, or the CISO. Failure to comply with this Policy will result in Management conducting a thorough review and taking appropriate corrective or disciplinary action in accordance with the Company's procedures.

1.3 Compliance

All non-public information handled or processed by the Company must be treated as confidential and retained strictly within the organization. Any unauthorized disclosure, use, or modification of such information is strictly prohibited and constitutes a violation of Company policy.

The use of electronic communications, IT systems, and other technology resources must comply with applicable laws, including the provisions on computer misuse under the Criminal Code (Articles 337B–337F), as well as the requirements of the Curaçao Gaming Authority (CGA). Personal data is processed and safeguarded in accordance with the General Data Protection Regulation (GDPR) and other relevant privacy legislation.

The Company maintains a data retention schedule that defines how long different categories of information, including player data, financial records, and operational logs, are retained. Data is securely archived or disposed of once it reaches the end of its retention period, in compliance with regulatory, contractual, and operational requirements.

In addition, the Company has implemented a data subject rights process to enable individuals to exercise their rights under applicable privacy laws. This includes rights to access, rectify, delete, or restrict the processing of their personal data, as well as the right to object to processing or request data portability. Requests from data subjects are handled promptly and documented in accordance with regulatory timelines and standards.

This policy provides guidance to all employees, contractors, and relevant personnel to ensure compliance with Curacao regulatory obligations, including the proper handling, protection, and security of information assets. Any breaches or suspected breaches of information security must be reported immediately and managed in line with regulatory expectations.

1.4 Training

The Company maintains a comprehensive Security Awareness Program to ensure all employees, contractors (3rd party providers), and relevant personnel are knowledgeable about information security risks and best practices. The program includes mandatory annual training covering key topics such as data protection, secure system usage, and regulatory compliance. Additionally, the Company conducts simulated phishing exercises to test awareness, reinforce secure behaviours, and identify areas requiring additional training. Participation and completion of the program are monitored and documented to ensure ongoing compliance and to strengthen the Company's overall security posture.

1.5 Risk Management

The Company is committed to a structured and proactive approach to information security risk management, ensuring that all digital assets, systems, and data are adequately protected. A formal risk management methodology is implemented to identify, assess, evaluate, and mitigate risks associated with information security. This methodology includes:

- Risk Identification: Systematic identification of potential threats and vulnerabilities affecting systems, networks, and data.
- Risk Assessment: Evaluation of the likelihood and potential impact of identified risks, considering both operational and regulatory factors.
- Risk Mitigation: Implementation of appropriate controls, safeguards, and corrective actions to reduce risks to acceptable levels.
- Risk Monitoring: Continuous oversight of emerging threats, system changes, and effectiveness of applied controls.

Risk assessments are conducted at regular intervals, with formal reviews at least annually or more frequently in response to significant operational or technological changes. All identified risks are linked to corresponding security controls and mitigation measures, ensuring traceability from risk assessment to practical safeguards. Findings and recommendations are reported to management and the CISO, who ensures alignment with the Company's overall information security strategy and reports significant risks directly to the Board of Directors.

2 Acceptable Use

This policy is to ensure the responsible and secure use of the Company's IT and network resources while supporting the Company's principles of openness, trust, and integrity. Management is committed to protecting employees, partners, and the Company from unlawful, inappropriate, or harmful actions, whether intentional or unintentional.

All network-related systems, including computer equipment, software, operating systems, storage media, network accounts, email, web browsing, FTP, and related documentation,

remain the property of the Company. These resources are to be used exclusively for legitimate business purposes, in support of the Company's operations and in service of its clients and customers, in line with normal operational requirements and in compliance with Curaçao Gaming Authority (CGA) regulatory obligations.

Employees and associated personnel are expected to use these systems responsibly, adhere to all applicable laws and regulatory requirements, and report any actual or suspected misuse, security breaches, or violations immediately.

2.1 Purpose

Aims to present the permissible use of computer equipment and documentation within our Company. These guidelines are established to safeguard the well-being of employees, players with an account, and the Company as a whole. Improper utilization may subject the Company to risks including virus infiltration, compromise of network systems and services, and potential legal ramifications. Additional policies about specific areas of concern, such as email and internet usage, have been formulated and should be referenced for further information.

This applies to all staff members, contractors, consultants, part-time workers, and any other individuals associated with the Company, including those connected with third-party entities. It encompasses all equipment owned or leased by the Company, as well as the services it supports, along with any documentation related to the equipment, products, services, clients, partnerships, and business entities.

2.2 General Use

The Company's IT Support aims to uphold a reasonable level of privacy for users, yet it's crucial for users to recognize that data generated on Company systems remains the Company's property. Given the imperative to safeguard the Company's network, management cannot guarantee the confidentiality of employees' information stored on any network device owned by the Company.

Employees bear responsibility for exercising firm judgment regarding personal use, with further guidance available in policies such as internet and email usage. In cases of uncertainty, employees should seek guidance from their direct supervisor.

Management strongly advises encrypting sensitive or vulnerable information or, at the very least, password-protecting it. Authorized individuals within the Company may monitor equipment, systems, and network traffic at any time for security and maintenance purposes. The Company retains the right to conduct periodic audits of networks and systems to ensure adherence to this policy. All documentation, including reports, is also considered the Company's property and should be handled accordingly.

2.3 Commercial Security Information

All information stored on Internet, Intranet, or Extranet systems must be classified in accordance with management's directives. Examples of confidential information include, but are not limited to, Company strategies, sensitive operational data, credit card information, customer lists, and research data.

Employees are responsible for taking all reasonable measures to prevent unauthorized access to such information. Passwords must be kept confidential and accounts must not be shared. Authorized users are fully accountable for the security of their accounts and passwords. Personal computers, laptops, and workstations must be secured with password-protected screensavers that activate automatically after no more than five minutes of inactivity, or by logging off when left unattended.

Where passwords alone are insufficient for protection, data must be encrypted using secure algorithms and proper key management procedures. Reports and documents containing sensitive or confidential information must not be left unattended in accessible areas and should be securely stored when not in use.

Information stored on portable devices should be restricted to business requirements, retained only for designated periods, and confidential data must be encrypted. Employee postings from Company email addresses to public forums or newsgroups must include disclaimers indicating personal opinions unless the communication is part of official duties. All devices connected to the Company's network, whether owned by the Company or employees, must have approved antivirus or endpoint protection software installed and kept up to date, except where specific departmental or Company policies dictate otherwise. Employees must exercise caution when opening email attachments or files from unknown or untrusted sources, as these may contain viruses, malware, or other security threats.

2.4 Protection of Players

All communication between the player and the Company must always occur through secure channels like HTTPS, TLS, etc.

2.5 Unacceptable Actions

The following activities are generally prohibited. Employees may be granted exceptions only when necessary to perform their lawful job duties (for example, system administration personnel may temporarily disable network access for a host causing disruptions to production services). Under no circumstances may any employee engage in activities that violate local or international law while using Company-owned resources. While the list below is not exhaustive, it highlights actions considered unacceptable.

The following activities are strictly prohibited without exception:

- Violating the rights of individuals or entities protected under copyright or other intellectual property laws, including the installation or distribution of unlicensed or unauthorized software products not approved for use by the Company.
- Unauthorized duplication or distribution of copyrighted materials, including digitizing and sharing photographs, books, music, or software without a valid license.
- Introducing harmful programs into the Company's network or systems, including viruses, malware, or other malicious software.
- Sharing account credentials or permitting others to use one's account, including family members or friends, whether working on-site or remotely.
- Transferring sensitive or confidential data between office or home equipment without prior authorisation from senior management.
- Conducting fraudulent activities using Company accounts, including promoting products, services, or items without approval.
- Performing security breaches or disrupting network communications, such as accessing data without authorization or logging into servers or accounts for which access has not been expressly granted, unless part of assigned job duties.
- Interfering with or denying services to any user, other than as necessary to support authorized operations.
- Disclosing information regarding Company employees or player accounts to external parties without explicit authorisation.

Employees found to have violated this policy may face disciplinary action, up to and including termination of employment.

2.6 Third-Party Controls

Overseas Gaming Management N.V. ("the Company") recognises that outsourcing services or relying on third-party providers can introduce additional risks to information security and operational resilience. To mitigate these risks, the Company implements a structured third-party risk management framework covering due diligence, contractual requirements, and ongoing oversight.

- Due Diligence - Prior to engaging any third-party service provider, the Company conducts a thorough risk-based due diligence assessment. This includes evaluating the provider's information security controls, regulatory compliance, financial stability, reputation, and history of security incidents. The assessment ensures that third parties meet the Company's minimum security and operational standards, consistent with Curaçao Gaming Authority (CGA) expectations and industry best practices.
- Service Level Agreements (SLAs) - All critical third-party relationships are governed by formal contracts or Service Level Agreements (SLAs) that clearly define:
 - Expected levels of service and performance;
 - Information security and data protection requirements;
 - Incident reporting obligations and response times;
 - Compliance with applicable regulatory and legal requirements.

SLAs also specify the responsibilities of the third party in maintaining system integrity, confidentiality, and availability of Company information, and include clauses for remediation in case of non-compliance.

- **Audit and Monitoring Rights** - The Company retains the right to audit and monitor third-party compliance with contractual and security obligations. This includes on-site or remote assessments, review of security policies and procedures, and verification of technical controls. Third parties are required to provide evidence of compliance, such as audit reports or certifications, and must cooperate fully during inspections. Regular reviews and risk assessments are conducted to ensure ongoing adherence to security, regulatory, and operational requirements.

3 Email Policy

The primary objective of email correspondence is to facilitate the Company's daily operations. This policy outlines the Company's guidelines regarding employee duties concerning electronic mail (email) communications transmitted or received through the Company's email systems. It encompasses both internal and external network systems and services utilized by the Company.

All email equipment and correspondence are assets owned by the Company. Any messages generated, transmitted, or received through the Company's email system are Company property. The Company retains the authority to access and divulge the contents of all messages created, transmitted, or received via its email system to pertinent entities.

3.1 Usage

All email correspondence should be treated with the same level of professionalism as a letter, memo, or any other form of business communication. Sensitive information or attachments mustn't be transmitted in clear text over the Internet to clients or colleagues. The use of the Company's email system for circulating commercial messages, employee solicitations, or messages about religious or political matters is strictly not permissible. Bulk forwarding of jokes, and similar materials, particularly to recipients outside the office, is not permitted.

Urgent virus warnings and/or emails that seem malicious should be promptly forwarded to IT or Technical Staff for authentication, as many such warnings are often false alarms. Employees are prohibited from accessing or reading emails not addressed to them unless authorized by the Company or the email recipient.

Additionally, employees must refrain from opening attachments in emails containing executable files, with extensions such as but not limited to .exe, .vbs, .com, etc, regardless of the sender. While incidental and infrequent personal use of email is allowed, such messages are considered Company property and are subject to the same regulations as any other business email.

Failure to adhere to this policy may lead to disciplinary measures, including termination of employment and/or legal action if deemed necessary. Employees are encouraged to report any instances of misuse of the Company's email system or violations of this policy to the appropriate Authority. The confidentiality of the reporting employee will be strictly maintained at all times. Employees need to recognize that computer misuse is considered a criminal offense and carries serious consequences.

4 Internet Security and Usage

The Company's guidelines regarding employee obligations concerning Internet usage via the Company's network. The Company provides employees with access to the Internet primarily to facilitate essential day-to-day business operations.

All computers and network components belong to the Company, along with the software installed on these computers. Additionally, any data stored on computers, devices, media, or the network is considered the property of the Company. The Company retains the authority to conduct checks on computers, network devices, and audit logs to verify appropriate usage when accessing the internet. Other forms of computer usage are subject to separate policies.

4.1 Usage

All employees requiring access to Internet services must utilize the Company's approved software and Internet gateways for this purpose. Accessing illicit sites, or any dubious websites is strictly prohibited. Furthermore, downloading any software or executable files is strictly forbidden.

Employees should be mindful that web browsers track all visited sites. Engineers requiring access to questionable sites for security monitoring or related activities must obtain explicit permission to do so. Such access should occur from systems empty of sensitive data, and technicians must exercise utmost caution at all times. Non-business browsing is permissible during work breaks, but adherence to the aforementioned usage rules remains mandatory.

Any breaches of this policy will prompt disciplinary measures, ranging from warnings to termination of employment, and potentially legal action if deemed necessary. Employees who observe any violations of this policy are required to promptly report them to the individual overseeing Information Security. The confidentiality of employees reporting violations will be strictly maintained at all times.

5 Network Firewalls

Implementing a DMZ or demilitarized zone is essential to filter and scrutinize all traffic, preventing direct access to the Internet. Firewalls must be deployed at each Internet connection and between the DMZ and the internal network zone. Database servers should be situated in an internal network zone, isolated from the DMZ. Additionally, firewalls should be installed and properly configured between any untrusted and trusted networks.

5.1 Firewall Rules Configuration

As a standard protocol, any inbound and outbound traffic, characterized by its source, destination, and port, that hasn't been explicitly permitted should be prohibited. Direct passage of traffic between the internal network zone and the Internet, or vice versa, must not be allowed. Internal addresses, such as IP addresses, should be restricted from flowing from the DMZ into the Internet. Additionally, firewalls must conduct network address translation for all IPv4 systems within the internal network, ensuring secure transmission. Firewall configurations should be meticulously secured and synchronized to maintain integrity and effectiveness.

5.2 Documented Firewall Rules

Every service and port allowed through Firewalls must be thoroughly documented, accompanied by a valid business rationale. Stringent security measures should be enforced for information transmitted via insecure protocols. Documentation of firewall and router rules should be maintained separately from the system. A current network diagram, encompassing all connections including wireless networks, must be readily available. Furthermore, regular reviews of all firewall and router access control rule sets should be conducted at least annually to ensure ongoing efficacy and compliance.

5.3 Network Security and Protection

The Company is committed to maintaining a secure and resilient network environment to protect its information systems and customer data. To achieve this, the Company deploys Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor network traffic, detect suspicious activity, and prevent potential security incidents. Alerts generated by these systems are subject to event correlation, allowing the Security team to analyse patterns across multiple sources and identify complex or coordinated threats. Procedures are in place to ensure timely investigation, escalation, and remediation of all detected incidents.

To further safeguard the network perimeter, the Company implements firewalls to control and restrict incoming and outgoing network traffic. Firewall configurations, rules, and access policies are reviewed regularly, with a minimum review interval of quarterly. This review ensures that all rules remain relevant, effective, and aligned with the Company's security objectives, and that any unnecessary or outdated permissions are promptly removed. All

changes to firewall configurations are documented, tested, and approved in accordance with the Company's change management procedures.

6 Cryptography Control

In accordance with the Company's Data Classification, as well as applicable legal, regulatory, and contractual obligations, the Company is committed to protecting information and IT systems through the use of cryptographic controls. All sensitive and critical data must be encrypted using approved standards, such as AES-256 for symmetric encryption and RSA-2048 for asymmetric encryption, in line with industry best practices. Encrypted data must be stored securely, with access restricted to authorised personnel, and archived or disposed of according to defined storage rules and retention schedules.

The Chief Security/Technical Officer (CTO/CSO) is responsible for defining the appropriate use of cryptographic tools and ensuring that all staff comply with these requirements when handling Company assets. The CTO/CSO is accountable for establishing and enforcing procedures for the secure management of cryptographic keys, which include, but are not limited to:

- Generation of cryptographic keys, including both private and public keys;
- Activation and distribution of cryptographic keys as required for business operations;
- Defining the validity period of cryptographic keys and ensuring their timely renewal;
- Secure storage and archiving of inactive keys necessary to maintain encrypted electronic records;
- Safe and verified destruction of cryptographic keys when they are no longer needed or have reached the end of their lifecycle.

All personnel must follow the CTO/CSO's directives regarding the use, storage, and management of cryptographic keys and related security measures, ensuring compliance with Curacao Gaming Authority (CGA) regulatory requirements and safeguarding the confidentiality, integrity, and availability of Company information.

7 Monitoring of System

The Company identifies business-critical systems and applications where event logging must be enabled to ensure effective monitoring, oversight, and regulatory compliance. All user access, including logins, logouts, and any high-risk activities, must be recorded, capturing user identities, timestamps, and relevant contextual information. Actions performed by system administrators and operators are fully logged and safeguarded against unauthorized alteration.

All security events, including those affecting the performance or effectiveness of deployed firewalls and other perimeter security controls, are logged in a secure, centralized location and are protected against unauthorized access or modifications. Logs are integrated into a Security Information and Event Management (SIEM) system, enabling real-time correlation, analysis, and alerting of potential threats. This integration ensures that anomalous patterns, coordinated attacks, or high-risk activities are detected and escalated promptly.

To support thorough assessment, investigation, and regulatory compliance, all logs are retained for a minimum period of twelve (12) months. Regular review and analysis of logs are conducted to verify operational effectiveness, detect suspicious activity, and maintain accountability. To ensure accuracy and consistency in event sequencing, clocks on all relevant information processing systems are synchronized with a single reference time source using Coordinated Universal Time (UTC).

All logging procedures, including SIEM integration and extended retention, are designed to comply with regulatory requirements, ensuring the integrity, availability, traceability, and accountability of the Company's information systems.

8 User Management

To strengthen system security and ensure accountability, the Company implements robust User Management controls with two primary objectives: preventing unauthorized access and limiting authorized users to the functions and data necessary for their roles.

This policy applies to all individuals who require access to the Company's systems or data, including employees, players, third-party service providers, and any other entities, regardless of their location or method of access. Access rights are assigned based on role-based principles and regularly reviewed to ensure compliance with the Company's security standards and Curacao Gaming Authority (CGA) regulatory requirements.

All users are responsible for safeguarding their access credentials and complying with the Company's directives on secure access and usage. Any suspected or actual unauthorized access must be reported immediately and addressed in accordance with Company procedures.

8.1 Policy Control and Authorisation

The Company strictly follows the principle of need-to-know, ensuring that access to information and information systems is granted only to authorized individuals with prior approval from designated senior officials.

The principle of segregation of duties is applied internally to minimize errors and prevent unauthorized or inappropriate actions during the access-granting process. Users are required to authenticate themselves using a unique username and a complex password.

Sharing of credentials is strictly prohibited. Passwords must meet minimum complexity requirements, containing at least eight characters, including numbers, symbols, and/or uppercase letters, and must not be identical to the username.

Where applicable, systems enforce multi-factor authentication (MFA) to further strengthen security. Access to critical systems follows the Just-in-Time (JIT) principle, granting privileges only when necessary, with all access and activities logged for accountability. Users must first create a unique user ID or username and verify their identity prior to accessing system resources to prevent impersonation. While standard passwords may suffice for internal networks, additional authentication measures are applied in high-risk environments.

Access rights are granted based on role, responsibilities, and the principle of least privilege, ensuring users and processes receive only the permissions necessary for their duties. Higher-privilege users may allocate access rights to others within their authorized scope, observing strict controls and approval procedures.

Determination of access rights takes into account both the content of files and the roles of the users involved. Access to additional resources, such as terminals, printers, and network services, is restricted based on operational requirements. Commands reserved for system administrators, security administrators, and database administrators are limited to a select group of authorized users and designated terminals.

Before granting access to any resource, the following steps are undertaken:

- Identification of the specific resources required by each individual or group and their necessary access rights (e.g., Read, Write, Execute).
- Standardization of user identifiers and task names, aligned with the relevant sections or departments of the Company.
- Establishment of naming conventions for files and resources based on associated processes, departments, or personnel.

All access control measures are designed to comply with Curacao Gaming Authority (CGA) regulatory requirements, ensuring the confidentiality, integrity, and accountability of the Company's information systems.

To maintain strict control over system access, the Company conducts quarterly reviews of all user access rights, verifying that permissions remain appropriate to current roles and responsibilities. In addition, a formal re-certification of privileges is carried out during these reviews, ensuring that access is granted only to authorised personnel and adjusted or revoked promptly when no longer required.

8.2 User Access Termination

Upon the termination of an employee's employment, it is essential for the CTO to meticulously follow specific protocols. Firstly, the CTO must guarantee the closure or deactivation of the employee's account to prevent any unauthorized access to company systems or sensitive information.

This action is vital for maintaining the integrity and security of the organization's digital infrastructure. Additionally, the CTO should diligently preserve all relevant correspondence related to the terminated employee, storing it securely for future reference. This documentation serves as a crucial record, assisting in the resolution of any potential disputes or inquiries that may arise following the termination. By adhering to these procedures, the CTO ensures compliance with organizational policies and legal requirements while safeguarding the company's interests and assets.

In addition to this, there is also inactive accounts which pose a significant risk to system security and should be promptly addressed to mitigate potential misuse. Necessary measures to manage such accounts should encompass a range of controls, which may include but are not limited to implementing procedures enabling users to request temporary suspension of their access rights, with subsequent restoration as needed to accommodate periods of leave or other temporary absences. Such step is essential for maintaining the integrity and security of the system while minimizing the likelihood of unauthorized access or misuse.

8.3 Automatic Log-off

To enhance security measures within the company's computing environment, it is imperative to implement an automatic workstation deactivation feature after a designated period of inactivity, through individual employee settings (maximum of 30 minutes). In addition to this automatic procedure, users should also have the capability to manually activate the screen lock program, providing an additional layer of security to safeguard sensitive information and prevent unauthorized access. By combining these measures, the company can effectively mitigate the risk of unauthorized access to workstations and laptops, bolstering overall data security protocols.

8.4 Login Attempts

The login process must enforce a lockout mechanism for individuals who enter an incorrect password a specified number of times. The allowable number of attempts before initiating a logout is set at 5 times. Users mustn't be granted access unless adequately authenticated, and automatic re-enabling after a set timeframe should be prohibited to prevent unauthorized access. This stringent approach to authentication and access control helps bolster security measures and safeguards against unauthorized entry to sensitive systems or data.

8.5 Adherence

Adherence to this Policy is principal, and any deviation should be minimized. If deviations are deemed essential, approval from senior management authority must be required, and comprehensive documentation of the justification for the deviation must be maintained. Employees are encouraged to promptly report any instances of misuse or abuse of authorization levels or user accounts, as well as any suspected unauthorized access.

Furthermore, if an employee discovers that they have access to resources they should not possess, they are obligated to report it and refrain from utilizing these access rights. Failure to comply with these guidelines will be considered a violation of this policy.

9 Anti-Virus

The Company implements anti-virus and anti-malware software to detect, prevent, and remove malicious programs, including viruses, spyware, and adware, across all IT systems and equipment. This policy establishes mandatory directives to ensure comprehensive protection in line with Curacao Gaming Authority (CGA) regulatory requirements.

- **Approved Software:** All servers, workstations, and PCs must be equipped with Company-approved anti-virus software wherever possible.
- **Automatic Updates:** Virus definition files must be updated automatically on a daily basis to ensure protection against emerging threats.
- **Regular Scans:** Anti-virus software must be configured to perform scheduled, periodic scans of systems to detect and remove potential threats.
- **Offline Updates:** In cases where devices cannot connect to the internet, virus definition files must be manually downloaded onto an alternative machine and securely transferred for installation.
- **Incident Reporting:** Users must immediately report to the IT Department if the anti-virus software is unable to remove a detected threat, so that appropriate remedial actions can be taken.

These measures are designed to maintain a high standard of security and protect the integrity, availability, and confidentiality of the Company's systems and data, in full compliance with CGA regulations.

10 Laptops and Portable Devices Security

Laptop computers and other portable devices represent critical assets for the Company's operations. Their portability, however, exposes them to risks such as theft, loss, or physical damage, particularly when used outside Company premises. Off-site use also increases exposure to potential malicious activity, underscoring the need for strict security measures to protect sensitive information and maintain business continuity.

The Company requires all employees to adhere to the following security procedures when using portable devices:

- Never leave laptops or portable devices unattended while logged in; always lock or log off before stepping away.

- Store devices securely and out of sight when not in use, avoiding visible exposure, especially in vehicles or public spaces.
- Transport devices in protective cases or briefcases to minimize the risk of accidental damage.
- Keep devices within sight whenever possible, exercising heightened caution in public areas such as airports, restaurants, and other communal locations.
- Use encryption to protect sensitive data whenever available.
- Perform regular backups, ideally weekly, by uploading critical data to the Company network or approved storage solutions.
- Do not share Company laptops or portable devices with third parties, including family members or friends.
- In the event of loss, theft, or suspected compromise of a device, immediately notify your manager and the IT Department to enable timely incident response.

These measures are designed to safeguard the confidentiality, integrity, and availability of the Company's information assets.

11 Removable Media

Employees are required to minimize the use of removable media devices whenever possible to reduce the risk of data breaches or unauthorized disclosure of Company information outside the organization. When the use of removable media is necessary, the following procedures must be strictly observed:

- Authorization must be obtained from the Chief Technology Officer (CTO) prior to using any removable media device to store or transfer confidential information.
- The IT Department should be involved in transferring any Company information to removable media to ensure secure handling.
- Confidential information must not be stored on removable media for extended periods unless using approved long-term storage solutions, such as encrypted backup tapes or other secure media.
- Any employee-owned or third-party devices used to provide information to the Company must be handed over to the IT Department for secure retrieval and safe disposal of the information and/or device.
- Following the completion of any external transfer of information, the sender must obtain confirmation from the recipient that the information and/or device has been securely disposed of or returned, using agreed-upon secure methods, once the information is no longer required.

12 Equipment and Media Disposal

The Company and its employees are required to follow strict procedures for the secure disposal of all media and storage devices to protect sensitive information and ensure regulatory compliance.

- **Paper Documents:** Any documents that have reached the end of their retention period must be securely shredded to prevent unauthorized access to confidential information.
- **Digital Storage Devices:** Hard drives, USB drives, external hard drives, and other electronic storage media containing Company data that is no longer required must be securely wiped using approved data-eradication software to ensure complete removal of information.
- **Equipment Decommissioning:** When equipment is removed from the Company's network, all storage media within the device must be securely decommissioned. This includes complete demagnetization or other approved techniques to render data permanently irrecoverable, safeguarding against potential data breaches or unauthorized access.

13 Data Classification

The Company has implemented a structured information classification framework to ensure the confidentiality, integrity, and appropriate handling of all information under its control. All information, whether generated internally or received from external sources, must be classified into one of the following categories: Public, Internal Use Only, Confidential, or Secret. All employees and relevant personnel are required to familiarize themselves with these classifications and follow the prescribed safeguards for each category.

If information is not explicitly classified, it will default to Internal Use Only, which does not require a sensitivity label. Information classified as Confidential or Secret is considered Sensitive and must be handled with additional security measures.

1. Public

Information designated as Public is intended for general release and its disclosure does not pose a risk to the Company, its clients, or business partners. Examples include marketing materials and content published on the Company website. Public disclosure requires explicit approval from senior management, a designated label, or adherence to an established precedent for public dissemination.

2. Internal Use Only

Internal Use Only information is intended for access strictly within the Company, and in specific cases, may be shared with authorized business partners. Unauthorized disclosure may contravene legal or regulatory requirements or negatively impact the Company, its clients, or partners. This category typically includes information widely shared internally

without explicit management authorization, such as internal email communications or the Company telephone directory.

3. Confidential

Confidential information is private or sensitive and should only be accessed by individuals with a legitimate business need. Unauthorized disclosure may violate legal obligations or cause significant impact to the Company, clients, or business partners. Access to Confidential information is controlled by the designated Information Asset Owner. Examples include customer account details, employee performance records, and correspondence with regulatory authorities such as the Curaçao Gaming Authority (CGA).

4. Secret

Secret information is of the highest sensitivity and requires continuous monitoring and strict control. Access is limited to individuals with explicit approval from Senior Management. Unauthorized disclosure may breach legal or regulatory requirements and could result in severe consequences for the Company, its clients, or affiliates. Examples include strategic merger and acquisition plans and legally privileged information.

Additional Security Measures

The Company also stores data that must remain inaccessible in readable form, such as:

- Passwords, which must be protected using strong hashing algorithms (e.g., SHA-512 or equivalent).
- Payment card data, where applicable, must be stored in compliance with applicable data protection and PCI DSS requirements.

All employees and contractors are responsible for handling information according to its classification and applying the appropriate security controls to protect Company information assets.

13.1 Asset Inventory

The Company maintains a comprehensive information asset inventory that includes all critical assets and systems. Each asset is clearly documented with relevant details such as type and classification. This inventory is regularly updated to ensure accuracy and completeness, reflecting changes such as new acquisitions, decommissioned systems, or modifications to existing assets.

Asset ownership roles are formally assigned for all information and technology assets. Asset owners are responsible for:

- Ensuring the protection of the asset in accordance with its classification and sensitivity;
- Defining and approving access rights;
- Ensuring appropriate security controls are implemented and maintained;
- Coordinating risk assessments and mitigating security risks related to the asset;
- Supporting audits and reviews of asset security and usage.

Asset / System	Asset Type	Owner / Responsible Role	Access Level / Permissions	Classification	Review Frequency
Player Database	Data	CISO	Restricted, read/write by authorised personnel	Confidential	Quarterly
Customer KYC / AML Records	Data	Compliance Officer	Restricted to compliance team only	Confidential	Quarterly
Payment Processing System	Application / Data	Finance Manager	Limited admin, audit-only access for IT	Confidential	Quarterly
Website / CMS	Software	Marketing Manager	Admin for content editors, read-only for IT	Internal Use	Bi-Annually
Network Infrastructure (servers, firewalls, switches)	Hardware	CTO / CISO	Restricted to network admins	Internal Use	Quarterly
Responsible Gambling Tools / Dashboards	Software / Data	Compliance Officer	Restricted to compliance teams	Confidential	Quarterly
Regulatory Reports / Compliance Records	Data	Compliance Officer	Restricted to compliance and audit teams	Confidential	Quarterly
Third-party Integrations / APIs	Software / Data	CTO	Admin access to IT team, monitored integration	Internal Use	Semi-Annual
Cryptocurrency Wallets / Payment Gateways	App/Data	Finance Manager	Restricted to finance and IT security team	Confidential	Monthly
Incident Response & Security Tools	Software	CISO	Restricted to IT security team	Internal Use	Monthly

14 Incident Response Plan

The Company maintains a structured and comprehensive Incident Response Plan (IRP) to effectively identify, manage, and mitigate information security incidents, ensuring minimal

disruption to operations and protection of player data. The IRP covers all types of security events, including cyberattacks, unauthorized access, data breaches, system failures, and any other incident impacting the confidentiality, integrity, or availability of Company information systems.

14.1 Triage and Identification

All potential security incidents are promptly identified through automated monitoring systems, including IDS/IPS, SIEM, firewalls, and application logs, as well as reports from staff or third parties. Each incident is triaged based on severity, impact, and likelihood, and assigned a priority level (Low, Medium, High, Critical) to determine the urgency of response. Initial documentation captures the date and time of detection, affected systems, suspected cause, and potential impact.

14.2 Escalation

Incidents are escalated according to defined protocols:

- Low/Medium severity: Managed by the relevant system or application owner under supervision of the CISO or designated security personnel.
- High/Critical severity: Immediately escalated to the CISO, CTO/CSO, and, where appropriate, the Board of Directors, ensuring rapid decision-making and allocation of resources.
- External parties, such as regulatory authorities or law enforcement, may be notified if required under Curaçao Gaming Authority (CGA) regulations or contractual obligations.

14.3 Containment and Mitigation

Upon escalation, the incident response team implements measures to contain and mitigate the impact of the incident. This may include:

- Isolating affected systems or networks to prevent further compromise;
- Blocking malicious activity or users;
- Applying temporary or permanent security controls;
- Preserving forensic evidence for analysis and compliance purposes.

All containment actions are documented, and affected systems are monitored until the threat is fully mitigated. Communication with internal stakeholders is managed according to pre-defined notification procedures.

14.4 Investigation and Analysis

The incident response team conducts a thorough investigation to determine the root cause, scope, and impact of the incident. Logs, network activity, and SIEM data are analysed to identify vulnerabilities, threat actors, and potential exposure of sensitive information.

Findings are documented in an incident report, including lessons learned and recommended corrective actions.

14.5 Review and Lessons Learned

After resolution, a post-incident review is conducted to evaluate the effectiveness of the response, identify gaps, and update policies, procedures, or technical controls. Recommendations may include additional staff training, system enhancements, or process changes. The IRP is updated periodically to incorporate lessons learned and reflect evolving threats, ensuring ongoing compliance with Curacao Gaming Authority (CGA) requirements and industry best practices.

14.6 Recordkeeping

All incidents, actions taken, and review outcomes are documented and retained for a minimum of twelve (12) months, or longer if required by regulatory or contractual obligations. Documentation supports accountability, audit readiness, and continuous improvement of the Company's information security posture.

15 Conclusion

The Company is committed to maintaining the highest standards of information security, ensuring the confidentiality, integrity, and availability of all information and IT systems in line with Curaçao Gaming Authority (CGA) regulatory requirements. This policy provides a structured framework for the classification, handling, protection, and disposal of information, as well as for the secure use of Company systems, devices, and networks.

All employees, contractors, and authorized third parties are required to comply with the measures outlined in this policy and to exercise due diligence in safeguarding Company information. Failure to adhere to these requirements may result in disciplinary action and, where applicable, legal consequences.

To ensure ongoing effectiveness and continuous improvement, the Company implements an annual internal audit schedule to evaluate compliance with this policy, assess the effectiveness of information security controls, and identify areas for enhancement. In addition, a formal management review cycle is conducted, where top management reviews audit findings, incident reports, risk assessments, and security performance metrics to approve corrective actions, update policies, and ensure alignment with business objectives and regulatory requirements.

By following the principles and procedures defined in this policy, including the internal audit and management review processes, the Company ensures robust operational security, supports regulatory compliance, and protects its business, clients, and partners from potential threats, breaches, or unauthorized disclosures. Continuous review and improvement of security measures

will be conducted to address emerging risks and maintain alignment with applicable laws, regulations, and best practices.

16 References

The following laws, regulations, standards, and guidance documents have informed the development of this Information Security Policy:

- Curacao Gaming Authority (CGA) Regulatory Framework – Applicable guidelines and requirements for licensed online gaming operators.
- General Data Protection Regulation (GDPR) (EU) 2016/679 – Standards for the protection of personal data and privacy.
- ISO/IEC 27001:2022 Information Security Management Systems – International standard for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).
- ISO/IEC 27002:2022 Code of Practice for Information Security Controls.
- Best Practice Guidelines for Online Gaming Operators – Industry standards for secure handling of player information, system security, and operational controls.