

**Code Harbor N.V.**  
**Information Security Policy**  
Version 2.0

*Aligned with the Curaçao Gaming Authority Information Security Control Requirements for CGA Licensees (B2C and B2B)*

|                       |                      |                                                                                               |                              |
|-----------------------|----------------------|-----------------------------------------------------------------------------------------------|------------------------------|
| Approving Official(s) | Oleg Latypov, CTO    | Signature:  | Date: 04.06.2026             |
| Responsible Office    | Technical Department | Document Owner                                                                                | Information Security Officer |
| Version               | 2.0                  | Supersedes                                                                                    | Version 1.0 (01.11.2025)     |
| Effective Date        | 04.06.2026           | Next Review Date                                                                              | 03.06.2027                   |

|                                                                  |           |
|------------------------------------------------------------------|-----------|
| <b>1. Policy Statement</b>                                       | <b>5</b>  |
| <b>2. Purpose</b>                                                | <b>5</b>  |
| <b>3. Scope and Applicability</b>                                | <b>5</b>  |
| <b>4. Definitions and Framework</b>                              | <b>6</b>  |
| <b>5. Responsibilities</b>                                       | <b>7</b>  |
| <b>6. IT Asset Policy</b>                                        | <b>8</b>  |
| 6.1. Purpose                                                     | 8         |
| 6.2. Scope                                                       | 8         |
| 6.3. Policy Definitions                                          | 8         |
| 6.4. Enterprise Asset Inventory                                  | 9         |
| 6.5. Detection of Unauthorised Devices                           | 9         |
| 6.6. Software Inventory and Supported Software                   | 9         |
| <b>7. Access Control Policy</b>                                  | <b>10</b> |
| 7.1. Purpose                                                     | 10        |
| 7.2. Scope                                                       | 10        |
| 7.3. Policy Definitions                                          | 10        |
| 7.4. Account Inventory and Periodic Review                       | 11        |
| 7.5. Multi-Factor Authentication                                 | 11        |
| 7.6. Access Distribution                                         | 11        |
| <b>8. Password Control Policy</b>                                | <b>12</b> |
| 8.1. Purpose                                                     | 12        |
| 8.2. Scope                                                       | 12        |
| 8.3. Policy Definitions                                          | 12        |
| <b>9. Email Policy</b>                                           | <b>13</b> |
| 9.1. Purpose                                                     | 13        |
| 9.2. Scope                                                       | 13        |
| 9.3. Policy Definitions                                          | 13        |
| <b>10. Internet Policy</b>                                       | <b>13</b> |
| 10.1. Purpose                                                    | 13        |
| 10.2. Scope                                                      | 13        |
| 10.3. Policy Definitions                                         | 13        |
| 10.4. DNS Filtering                                              | 14        |
| <b>11. Antivirus and Malware Defence Policy</b>                  | <b>14</b> |
| 11.1. Purpose                                                    | 14        |
| 11.2. Scope                                                      | 14        |
| 11.3. Policy Definitions                                         | 14        |
| 11.4. Removable Media                                            | 15        |
| <b>12. Information Classification and Data Management Policy</b> | <b>15</b> |
| 12.1. Purpose                                                    | 15        |
| 12.2. Scope                                                      | 15        |
| 12.3. Policy Definitions                                         | 15        |
| 12.4. Inventory of Sensitive Data Locations                      | 16        |
| 12.5. Data Retention and Secure Disposal                         | 16        |
| <b>13. Remote Access Policy</b>                                  | <b>16</b> |
| 13.1. Purpose                                                    | 16        |
| 13.2. Scope                                                      | 17        |

|                                                                          |           |
|--------------------------------------------------------------------------|-----------|
| 13.3. Policy Definitions.....                                            | 17        |
| <b>14. Third-Party and Outsourcing Policy .....</b>                      | <b>17</b> |
| 14.1. Purpose.....                                                       | 17        |
| 14.2. Scope.....                                                         | 17        |
| 14.3. Policy Definitions.....                                            | 17        |
| 14.4. Service Provider Inventory .....                                   | 18        |
| 14.5. B2B Certification Monitoring .....                                 | 18        |
| 14.6. Integrity of Externally Supplied Game Content and Data Feeds ..... | 19        |
| <b>15. Incident Management and Regulatory Notification .....</b>         | <b>19</b> |
| 15.1. Purpose.....                                                       | 19        |
| 15.2. Roles and Contacts.....                                            | 19        |
| 15.3. Reporting and Escalation.....                                      | 19        |
| 15.4. Mandatory CGA Notification .....                                   | 20        |
| 15.5. Post-Incident Review .....                                         | 20        |
| <b>16. Secure Configuration Management .....</b>                         | <b>20</b> |
| 16.1. Purpose.....                                                       | 20        |
| 16.2. Policy Definitions.....                                            | 20        |
| 16.3. Default Accounts.....                                              | 21        |
| <b>17. Vulnerability and Patch Management .....</b>                      | <b>21</b> |
| 17.1. Purpose.....                                                       | 21        |
| 17.2. Vulnerability Management .....                                     | 21        |
| 17.3. Patch Management.....                                              | 21        |
| <b>18. Logging, Monitoring and Audit Trails .....</b>                    | <b>21</b> |
| 18.1. Purpose.....                                                       | 21        |
| 18.2. Audit Log Management Process .....                                 | 22        |
| 18.3. Log Collection, Protection and Content .....                       | 22        |
| <b>19. Backup and Data Recovery .....</b>                                | <b>22</b> |
| 19.1. Purpose.....                                                       | 22        |
| 19.2. Data Recovery Strategy.....                                        | 22        |
| 19.3. Backup Execution and Protection .....                              | 22        |
| <b>20. Network Infrastructure Security .....</b>                         | <b>23</b> |
| 20.1. Purpose.....                                                       | 23        |
| 20.2. Policy Definitions.....                                            | 23        |
| <b>21. Security Awareness and Training .....</b>                         | <b>23</b> |
| 21.1. Purpose.....                                                       | 23        |
| 21.2. Awareness Programme .....                                          | 23        |
| 21.3. Role-Based Training .....                                          | 23        |
| <b>22. Physical and Environmental Security.....</b>                      | <b>24</b> |
| 22.1. Purpose.....                                                       | 24        |
| 22.2. Policy Definitions.....                                            | 24        |
| <b>23. Human Resource Security .....</b>                                 | <b>24</b> |
| 23.1. Purpose.....                                                       | 24        |
| 23.2. Policy Definitions.....                                            | 24        |
| <b>24. Legal and Regulatory Compliance .....</b>                         | <b>25</b> |
| 24.1. Purpose.....                                                       | 25        |
| 24.2. Policy Definitions.....                                            | 25        |

|                                                                 |           |
|-----------------------------------------------------------------|-----------|
| <b>25. Business Continuity and Operational Resilience .....</b> | <b>25</b> |
| 25.1. Purpose.....                                              | 25        |
| 25.2. Policy Definitions.....                                   | 25        |
| <b>26. Cryptographic Controls and Key Management .....</b>      | <b>25</b> |
| 26.1. Purpose.....                                              | 25        |
| 26.2. Policy Definitions.....                                   | 25        |
| <b>27. Security Governance and Oversight.....</b>               | <b>26</b> |
| 27.1. Purpose.....                                              | 26        |
| 27.2. Policy Definitions.....                                   | 26        |
| <b>28. Compliance Monitoring and Assurance .....</b>            | <b>26</b> |
| 28.1. Purpose.....                                              | 26        |
| 28.2. Policy Definitions.....                                   | 26        |
| <b>29. Policy History .....</b>                                 | <b>27</b> |

## 1. Policy Statement

Code Harbor N.V. (hereinafter — the Company) operates the online casino under a licence issued by the Curaçao Gaming Authority (CGA). This document specifies the level of security and the approach that must be established and applied across the Company for the safeguarding of data and information against threats.

The Company is subject to applicable Curaçao legislation, including the Landsverordening op de Kansspelen (LOK), the Landsverordening Casinowezen Curaçao (LCC), the National Ordinance on the Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance, the Kingdom Sanctions Act, and applicable personal data protection legislation. This Information Security Policy is issued in furtherance of the Company's obligations under its CGA licence conditions.

This Policy is designed to implement the CGA Information Security Control Requirements for CGA Licensees (B2C and B2B) (the "CGA Requirements"), which adopt the Center for Internet Security (CIS) Controls Implementation Group 1 (IG1) as the mandatory baseline and align with ISO/IEC 27001:2022. The Company acknowledges that compliance with the CGA Requirements constitutes a mandatory condition of licensure under the LOK.

**Regulatory interpretation.** Within this Policy, the terms "must", "shall" and "required" indicate binding obligations. The term "should" is used only where proportional or risk-based implementation is permitted.

**Maturity roadmap.** The Company implements CIS IG1 as its enforceable baseline and, in line with the CGA's stated expectation, plans progression towards IG2 maturity within 24 to 36 months. Progression planning is reviewed annually by the Information Security Officer and reported to senior management.

## 2. Purpose

The purpose of this Information Security Policy is to preserve an appropriate level of:

- Confidentiality: prevention of the unauthorised disclosure of information.
- Integrity: prevention of the unauthorised amendment or deletion of information.
- Availability: prevention of the unauthorised withholding of information or resources.

In addition, this Policy gives effect to the security objectives of the LOK, namely to ensure that gaming systems operate in a secure, controlled and auditable manner; that game outcomes, RNG processes and transaction records are protected against manipulation; that player data, payment data and responsible gaming records are safeguarded; that the Company maintains continuous operational control over outsourced and third-party systems; and that the CGA can effectively supervise, investigate and enforce compliance.

## 3. Scope and Applicability

This document applies to all users and employees in the Company, including temporary users, visitors with temporary access to services, and partners with limited or unlimited access time to services. Compliance with the policies in this document is mandatory. This Policy applies to all data, systems, and networks owned or operated by Code Harbor N.V.

The Company is licensed by the CGA as a Business-to-Consumer (B2C) online gaming operator. Where the Company relies on third-party platforms, hosting providers, game content aggregators, sports data feed providers or Business-to-Business (B2B) providers, the Company remains fully responsible under the LOK for compliance with the CGA Requirements. Contractual delegation of operational controls does

not transfer regulatory accountability; the nature of that accountability is one of due diligence, verification and reporting.

**Cloud-hosted infrastructure.** Where the Company uses cloud infrastructure services, hardware-specific controls are addressed through the shared responsibility model. The Company documents which controls are managed by the cloud provider, maintains evidence of the provider's compliance certifications (e.g. SOC 2, ISO/IEC 27001), and remains responsible for all controls within its own sphere of responsibility.

Controls in this Policy that relate exclusively to land-based gaming operations are not applicable to the Company; their non-applicability is documented in the control mapping at Annex A.

#### 4. Definitions and Framework

This Policy operates together with the Company's supporting procedures, standards and registers, including the asset inventory, account inventory, service provider inventory, data retention schedule, incident response plan, business continuity and disaster recovery plans, and the register of cryptographic controls.

Exceptions to the policies in this document may only be authorised by the Information Security Officer. Every exception must be logged with date, time, description, reason, compensating controls, risk acceptance rationale and review date, and must be reviewed at least annually.

All IT services must be used in compliance with the technical and security requirements defined in this and other referenced documents.

Infractions of this Policy may lead to disciplinary action, dismissal, prosecution, or notification to the CGA or other competent authorities.

| Term                 | Definition                                                                                                                                                                                                                                     |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Management    | The process responsible for allowing users to make use of IT services, data, or other assets.                                                                                                                                                  |
| B2B Provider         | A CGA-licensed Business-to-Business gaming technology provider supplying Remote Gaming Servers, game engines, game content or player management systems.                                                                                       |
| CGA                  | Curaçao Gaming Authority — the regulatory authority responsible for licensing and supervising gaming operators in Curaçao.                                                                                                                     |
| CGA Requirements     | The Information Security Control Requirements for CGA Licensees (B2C and B2B) issued by the CGA.                                                                                                                                               |
| CIS IG1              | Center for Internet Security Controls, Implementation Group 1 — the mandatory security baseline adopted by the CGA.                                                                                                                            |
| Confidentiality      | A security principle requiring that data is only accessible by authorised persons.                                                                                                                                                             |
| Critical Gaming Data | Game event outcomes, high-value transactions, jackpot triggers, sports data feeds and live odds, game results received from B2B providers or content aggregators, RNG output records, and aggregated content used to determine wager outcomes. |
| Data Feed Integrity  | The assurance that data received from an external source has not been altered, corrupted or manipulated during transmission or                                                                                                                 |

| <b>Term</b>             | <b>Definition</b>                                                                                                                                                                                                                                                                                                                    |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | processing, and accurately reflects the data as sent by the originating source.                                                                                                                                                                                                                                                      |
| FIU Curaçao             | Financial Intelligence Unit Curaçao — the competent authority for receiving unusual transaction reports under NORUT.                                                                                                                                                                                                                 |
| Game Content Aggregator | A third-party entity that integrates, distributes or provides access to game content from multiple B2B providers through a unified platform or API.                                                                                                                                                                                  |
| ISO                     | Information Security Officer — responsible for implementing and maintaining the Company's security programme.                                                                                                                                                                                                                        |
| Key Official            | The individual designated to the CGA as responsible for ongoing licence compliance.                                                                                                                                                                                                                                                  |
| LOK / LCC               | Landsverordening op de Kansspelen and Landsverordening Casinowezen Curaçao.                                                                                                                                                                                                                                                          |
| NOIS                    | National Ordinance on the Identification when Rendering Services (N.G. 2017, no. 92).                                                                                                                                                                                                                                                |
| NORUT                   | National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99).                                                                                                                                                                                                                                                     |
| Outsourcing             | Using an external service provider to manage IT services or functions.                                                                                                                                                                                                                                                               |
| Regulated Data          | Information subject to specific protection requirements under the LOK, LCC or other applicable legislation, including player personal and financial data, game event outcomes and transaction records, responsible gaming intervention data, anti-money laundering records, and system audit logs required for regulatory oversight. |
| Risk                    | A possible event that could cause harm or loss, or affect the ability to achieve objectives.                                                                                                                                                                                                                                         |
| SIEM                    | Security Information and Event Management — real-time monitoring and analysis of security events.                                                                                                                                                                                                                                    |
| Sports Data Feed        | A real-time or near-real-time electronic data service providing sports event information, results, odds or statistics used to determine the outcome of sports-related wagers.                                                                                                                                                        |
| VPN                     | Virtual Private Network — a secure encrypted connection for remote access to internal systems.                                                                                                                                                                                                                                       |

## 5. Responsibilities

| <b>Role</b>                             | <b>Responsibilities</b>                                                                                                                                                                                                                 |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chief Executive Officer                 | Overall direction towards information security and cyber-resilience. Holds executive responsibility for information security oversight. Accountable to the CGA for compliance with licence conditions relating to information security. |
| Chief Information Officer / IT Director | Accountable for all aspects of the Company's information security infrastructure, systems, and controls. Owns the asset, software and network inventories.                                                                              |

| <b>Role</b>                        | <b>Responsibilities</b>                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Compliance Officer                 | Responsible for ensuring the gaming system and all IT components are consistently in line with CGA regulations and licence conditions, including security requirements. Maintains the register of applicable legal and regulatory obligations. Responsible for notifying the CGA of material security incidents within the required timeframes.                        |
| Key Official                       | Accountable for ongoing licence compliance. Approves regulatory notifications to the CGA and confirms the Company's annual self-assessment submission.                                                                                                                                                                                                                 |
| Information Security Officer (ISO) | Responsible for the security of the IT infrastructure. Plans against threats, vulnerabilities, and risks. Implements and maintains Security Policy documents. Owns the vulnerability management, patch management, logging, backup, awareness and exception processes. Responds to incidents including regulatory notification. Assists in disaster recovery planning. |
| Information Owners                 | Assist with security requirements for their area. Determine privileges and access rights to resources within their areas. Perform periodic access recertification.                                                                                                                                                                                                     |
| IT Security Team                   | Implements and operates IT security controls. Manages access rights. Maintains logging, backup, patching and configuration baselines. Supports Security Policies.                                                                                                                                                                                                      |
| Human Resources                    | Operates pre-employment screening, confidentiality undertakings, security acknowledgements, and joiner/mover/leaver notifications to IT Security.                                                                                                                                                                                                                      |
| All Staff                          | Adhere to this Policy. Complete mandatory security awareness training. Report unusual behaviour or malicious activity to the IT Security Team without delay.                                                                                                                                                                                                           |

## **6. IT Asset Policy**

### **6.1. Purpose**

This section defines the requirements for the proper and secure handling and inventory of all IT assets in the Company, including those supporting the CGA-licensed gaming platform.

### **6.2. Scope**

Applies to all persons — including employees, temporary workers, visitors, partners, and suppliers — using or interacting with IT assets forming part of the Company's infrastructure.

### **6.3. Policy Definitions**

IT assets must only be used in connection with the business activities they are assigned and/or authorised for.

All IT assets must be classified according to the Company's security classification scheme.

Every user is responsible for the preservation and correct use of the IT assets assigned to them.

All IT assets must be located in areas with appropriate security access restrictions and physical conditions consistent with their security classification.

Access to assets is forbidden for non-authorised personnel. All access requests must be processed through the approved Service Request Management process.

All IT assets supporting the gaming system shall have their clocks synchronised with a single, reliable time source. Configuration of date or time is restricted to the IT Security team based on formal written approval. All date and time operations shall be recorded in an audit trail.

The IT Technical Teams are solely responsible for maintaining and upgrading configurations. No other users are authorised to modify hardware or install software.

Portable assets (laptops, mobile devices) shall be encrypted using full-disk encryption. When travelling by air, portable equipment must be carried as hand luggage. Special care must be taken regarding theft, temperature extremes, and physical damage.

Losses, theft, damage, tampering, or any other security-relevant incident must be reported immediately to the Information Security Officer.

Disposal of assets must follow specific procedures. Assets storing confidential information must be physically destroyed; assets storing sensitive information must be securely erased, both in the presence of an Information Security Team member. Approved disposal methods are cryptographic erasure, overwriting or degaussing, and physical destruction of media.

#### **6.4. Enterprise Asset Inventory**

The Company shall establish and maintain a complete and accurate inventory of all enterprise devices that interact with gaming data or systems. The inventory shall include:

- Application and infrastructure servers (gaming, financial, player management);
- Networking hardware (routers, switches, firewalls);
- End-user computing devices (desktops, laptops, tablets, smartphones);
- Virtual and cloud-hosted instances, containers and managed services;
- Internet of Things devices (e.g. surveillance cameras, sensors).

The following attributes shall be recorded for each device: static IP or MAC address; hostname or device identifier; asset owner or responsible business unit; and network approval or access status.

A formal inventory review shall be performed at least twice annually.

#### **6.5. Detection of Unauthorised Devices**

The Company shall operate a documented weekly procedure to identify and respond to unauthorised assets appearing within its networks or environments. Automated discovery tooling shall be used where technically feasible, supplemented by manual verification.

Mitigation actions shall include removing the device from the network, blocking remote access, or placing the device in a quarantined zone. A log of detections, actions taken and justifications for any exceptions shall be maintained.

Priority shall be given to identifying devices that could affect game fairness, manipulate outcomes, or introduce data protection risks.

#### **6.6. Software Inventory and Supported Software**

The Company shall maintain an inventory of all authorised software deployed within the organisation, including gaming software and platform components, operating systems, endpoint and server security tools, and reporting, management and compliance applications. For each entry the inventory shall

record title and variant, version and installation date, purpose and associated business function, and the number of licences or installations.

The software inventory shall be reviewed and updated bi-annually. Tracking shall include RNG-related software, game engines and other components subject to regulatory oversight that are operated by or integrated with the Company.

The Company shall conduct monthly checks to validate vendor support status for all approved software. Unsupported software shall be removed, or retained only under a documented exception recording the risk acceptance rationale and the compensating controls in place (for example network isolation or restricted access).

As a B2C operator using certified Remote Gaming Servers and game content from licensed B2B providers, the Company is not responsible for the B2B provider's game lifecycle management or certification process. The Company's obligations in this respect are set out in Section 14.

## **7. Access Control Policy**

### **7.1. Purpose**

This section defines the requirements for the proper and secure control of access to IT services and infrastructure, including systems supporting the CGA-licensed gaming platform.

### **7.2. Scope**

Applies to all persons including employees, temporary workers, visitors, partners, and suppliers with any level of access to services.

### **7.3. Policy Definitions**

A data owner shall be formally designated for every service supporting the Company's operations. All access requests must be approved by the designated data owner and processed through a single company-wide ticketing system. No access shall be granted without formal approval.

Unless technically impossible, all systems shall use a centralised authentication mechanism. All information repositories shall require authentication for access.

Any system handling valuable information must be protected with a password-based access control system. Systems handling confidential or sensitive information must additionally be protected by multi-factor authentication and network segmentation.

Access shall be granted under the principle of least privilege: each identity receives the minimum rights needed for its business function. Access to sensitive data shall be managed through role-based access control (RBAC) enforcing need-to-know restrictions.

**Employee accounts inactive for 45 (forty-five) days shall be automatically disabled** and reactivated only upon formal request approved by the data owner. Automated inactivity monitoring shall be implemented where technically feasible. Audit logs shall be retained and reactivation procedures documented.

Authenticated sessions inactive for 5 (five) minutes shall result in automatic session disconnection or endpoint locking. In no case shall the inactivity lock exceed 15 minutes on general systems or 2 minutes on mobile devices.

Session locking settings shall be applied through centralised configuration management tooling or group policy.

All system authentications and attempts shall be logged and forwarded to a Security Information and Event Management (SIEM) system.

All networks shall be segregated by function using VLANs or equivalent technologies. Access control list amendments are subject to logged, approved requests.

Employees are prohibited from tampering with or evading access controls to gain greater access than assigned.

New users: the resource's manager requests access, approved by the Information Security Officer, Key Official, and respective service owner. Access is granted by the system administrator holding privileged rights.

Access changes: the resource's manager logs a service request with reasons, approved by the Information Security Officer, Key Official, and service owner.

Leavers: the manager initiates termination; the user account is disabled on the last day of employment and all access revoked. Termination and transfer notifications from Human Resources shall trigger account disablement across on-premise and cloud-based systems. Accounts shall be disabled rather than deleted in order to preserve audit logs. Records of previously held access are retained in line with applicable requirements.

#### **7.4. Account Inventory and Periodic Review**

The Company shall maintain a complete and up-to-date inventory of all accounts across its environment, comprising standard user accounts, privileged administrative accounts, and system or service accounts used for automation and integrations. For each account the inventory shall record full name and department, username, and account creation and deactivation dates.

The Information Security Officer shall conduct quarterly reviews to confirm that all active accounts remain valid, are assigned to current personnel, and remain necessary. Information Owners shall recertify access rights to systems in their area at the same frequency.

Privileged access shall be restricted to dedicated administrative accounts used only for elevated functions. Privileged accounts shall not be used for general activities such as web browsing, email or document editing, and shall be prevented from accessing non-administrative resources.

#### **7.5. Multi-Factor Authentication**

Multi-factor authentication (MFA) is mandatory and shall be enforced for:

- all internet-facing or externally accessible applications and portals;
- all remote access methods, including VPN, RDP and equivalent;
- all administrative access to core gaming systems and infrastructure;
- all access to systems processing player personal data, payment data or AML/KYC records.

Acceptable authentication methods are time-based one-time password (TOTP) authenticator applications, hardware security tokens compliant with FIDO2/WebAuthn, and biometric identifiers. SMS-based one-time passwords shall not be used as a sole second factor for administrative access.

MFA solutions shall be selected so as not to interfere with emergency response procedures or the operational uptime of critical systems.

#### **7.6. Access Distribution**

| <b>Job Designation</b>                   | <b>Source Control</b> | <b>Remote Access (VPN)</b> | <b>Physical Access</b> | <b>Database Access</b>                                                         | <b>App Server Access</b> |
|------------------------------------------|-----------------------|----------------------------|------------------------|--------------------------------------------------------------------------------|--------------------------|
| System Development / Application Support | Granted               | Granted                    | Not Granted            | Granted (non-production only; production access requires break-glass approval) | Granted                  |
| Network / Systems Support                | Not Granted           | Granted                    | Granted                | Not Granted                                                                    | Granted                  |

Production database access by development and application support personnel is granted only through a documented break-glass procedure, approved by the Information Security Officer and the data owner, time-limited, and fully logged and reviewed. This preserves segregation of duties between development and production operations.

## **8. Password Control Policy**

### **8.1. Purpose**

This section defines the requirements for the proper and secure handling of passwords in the Company.

### **8.2. Scope**

Applies to all persons with any level of access to the Company's services.

### **8.3. Policy Definitions**

Every user must have a separate, private identity for accessing IT network services. Identities shall be centrally created and managed.

Each identity must have a strong, private, alphanumeric password of at least 15 characters. This exceeds the CGA minimum of 8 characters for MFA-protected accounts and 14 characters for accounts without MFA.

Passwords must be unique across all systems and accounts. Shared and default passwords are strictly prohibited.

Regular user passwords may be used for no more than 90 days and no less than 3 days. The same password may not be reused for at least one year.

All privileged account passwords must be changed at least every three months. All default passwords must be changed before deployment.

Passwords must not be transmitted via email or other electronic communication. Sharing of passwords is strictly forbidden.

Identities must be locked if password guessing is suspected. Compromised passwords must be changed immediately and a ticket raised with the Information Security Officer. Upon password change or identity revocation, all active sessions and OAuth tokens associated with the identity must be immediately revoked across all connected systems.

IT administrators must maintain two sets of credentials: one for administrative and one for non-privileged work.

Strong passwords must: contain upper and lowercase characters; include digits and punctuation; be at least 15 alphanumeric characters long; and not be based on dictionary words, personal information, or company name derivations. Passwords must never be written down or stored in plain text outside an approved secure password vault. Use of the approved password manager is required for all personnel.

## **9. Email Policy**

### **9.1. Purpose**

This section defines the requirements for the proper and secure use of electronic mail in the Company.

### **9.2. Scope**

Applies to all persons with access to Code Harbor N.V. email services.

### **9.3. Policy Definitions**

All assigned email addresses and mailbox storage must be used only for business purposes.

Use of email resources for unauthorised advertising, spam, political campaigns, or activities unrelated to the Company's business is strictly forbidden.

Email resources must not be used to disclose confidential or sensitive information to unauthorised recipients.

Sending unsolicited email, creating or forwarding chain letters, harassing individuals via email, or forging email header information are strictly prohibited.

Scanning technologies for viruses and malware must be in place on all endpoints and servers for inbound and outbound email.

Only fully supported and current versions of email clients shall be deployed on enterprise systems. Automatic updates shall be applied and unsupported clients removed promptly.

All security incidents involving email must be reported to the Information Security Officer immediately. Users must not attempt to respond to security attacks themselves.

Corporate mailbox content must be centrally stored in backed-up locations managed according to the Company's data retention procedures.

## **10. Internet Policy**

### **10.1. Purpose**

This section defines the requirements for the proper and secure access to the Internet by the Company's users.

### **10.2. Scope**

Applies to all users in the Company, including temporary users, visitors, and partners.

### **10.3. Policy Definitions**

Internet access is permitted for business purposes. Limited personal navigation is permitted provided it does not perceptibly consume system resources or impair productivity.

Access to pornographic, hacking, gambling circumvention, and other high-risk sites is forbidden.

No software shall be downloaded without prior approval from the Information Security Officer.

Only fully supported and up-to-date web browsers shall be deployed on enterprise systems. Automatic updates shall be enabled and unsupported browsers removed promptly. Compatibility of updates with web-based gaming platforms and administration portals shall be verified.

Inbound and outbound traffic must be regulated using firewalls. Back-to-back firewall configuration is strongly recommended. Host-based firewalls shall be installed and enabled on all supported servers and endpoints, configured with default-deny rules and allow-listing policies. All firewall rule changes, including exceptions, must be reviewed, approved and documented.

Internet traffic shall be monitored at firewalls. Attacks or abuse must be reported promptly to the Information Security Officer.

Activities such as denial-of-service attacks, spam, phishing, fraud, hacking, distribution of unlawful material, and copyright infringement are strictly forbidden.

#### **10.4. DNS Filtering**

DNS filtering shall be used to block access to known malicious or unauthorised domains. DNS filtering agents shall be deployed across all endpoints, both on-premises and remote. Threat intelligence feeds shall be integrated to maintain updated blocklists, and DNS activity shall be monitored for anomalies.

DNS filtering configurations shall be verified so as not to interfere with connectivity to legitimate gaming services, B2B platform integrations or cloud environments.

### **11. Antivirus and Malware Defence Policy**

#### **11.1. Purpose**

This section determines the direction for antivirus and other malware protection at Code Harbor N.V., and the control of removable media.

#### **11.2. Scope**

Applies to all users and all servers and other applicable equipment.

#### **11.3. Policy Definitions**

All computers and devices with access to the Company's network must have an antivirus client installed with real-time protection enabled.

All servers and workstations owned by the Company must have an approved, centrally managed antivirus solution with automatic signature and engine updates. Regular scanning of devices and file activity shall be enforced.

Files or macros attached to emails from unknown senders must not be opened. Files must never be downloaded from unknown or suspicious sources.

Visitor computers and all computers connecting to the Company's network must have a valid, updated antivirus solution installed.

The antivirus software must never be intentionally stopped or disabled. All update completions must be monitored and confirmed.

Vendor compatibility with gaming systems and platforms shall be verified, and protection tools confirmed not to introduce performance degradation.

#### **11.4. Removable Media**

Autorun and autoplay functionality shall be disabled for USB and other removable devices across all systems.

The use of removable media requires prior authorisation from the Information Security Officer. Documented procedures and technical controls shall govern authorisation, and all data transferred from external storage shall be scanned and validated before use.

Particular attention shall be given to exposed ports on administrative workstations and any terminals with physical access exposure.

## 12. Information Classification and Data Management Policy

### 12.1. Purpose

This section defines a framework for the classification, handling, retention and disposal of information according to its importance and associated risks, ensuring appropriate confidentiality, integrity, and availability of the Company's information assets in compliance with CGA requirements and applicable Curaçao data protection legislation.

### 12.2. Scope

Applies to all information created, owned, or managed by the Company, whether stored electronically or in paper form.

### 12.3. Policy Definitions

All Code Harbor N.V. information is categorised into two main classifications:

**Code Harbor Public:** information declared public by a person with authority to do so, which may be freely shared without causing damage to the Company's systems or reputation.

**Code Harbor Confidential:** all other information, including player data, financial data, source code, transaction records, AML/KYC documentation, game system configurations, Critical Gaming Data, and any other information integral to the success of the Company or its regulatory obligations. A subset is 'Code Harbor Third Party Confidential' — information entrusted by another organisation under non-disclosure agreements.

Classification levels within Code Harbor N.V. Confidential:

| Sensitivity    | Examples                                                                                                                                                                                                                                                                        | Access                                       | Storage                                                                                                     | Disposal                                  |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Most Sensitive | Critical Gaming Data (game event outcomes, jackpot triggers, RNG output records, sports data feeds and live odds, game results received from B2B providers or aggregators); trade secrets; source code; AML/KYC records; player financial data; security infrastructure details | Designated individuals with signed NDAs only | RBAC, physically secured and hardened environment; encrypted at rest and in transit; encrypted distribution | Degaussed, wiped, or physically destroyed |

| <b>Sensitivity</b>  | <b>Examples</b>                                                                                                       | <b>Access</b>                                                  | <b>Storage</b>                                                      | <b>Disposal</b>                                 |
|---------------------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|---------------------------------------------------------------------|-------------------------------------------------|
| More Sensitive      | Business, financial, technical, and personnel information; player personal data not falling within the category above | Employees and non-employees with signed NDAs and business need | Individual access controls; external distribution must be encrypted | Securely erased or physically destroyed         |
| Minimal Sensitivity | General corporate information, some personnel and technical information                                               | Employees and those with business need to know                 | Standard controls; keep away from unauthorised view                 | Deposit in marked bins; electronic data cleared |

Additional requirements: all player passwords and sensitive player information must be encrypted with industry-standard encryption. All communication with backend systems must use HTTPS; HTTP is not permitted. Users will be automatically logged off from backend systems after 15 minutes of inactivity, in line with Section 7.3.

Handling procedures for each classification — covering access restrictions, storage locations and protections, and sharing and transfer protocols — shall be documented and reviewed annually or upon any significant system, regulatory or process change.

#### **12.4. Inventory of Sensitive Data Locations**

The Company shall maintain an up-to-date record of all locations where sensitive and regulated data is stored, processed or transmitted, including on-premise databases and application servers, file systems and shared drives, cloud-based storage platforms, backup repositories, and data held or processed by third parties on the Company's behalf.

Each data store shall be labelled by data type and classification. Priority shall be given to accurate mapping of locations holding Critical Gaming Data and player personal data. The record shall be updated at least annually and upon any significant change to infrastructure.

#### **12.5. Data Retention and Secure Disposal**

The Company shall maintain a documented retention schedule specifying minimum and maximum retention periods for each data classification, established in line with regulatory requirements, licence conditions and business needs. As a minimum, gaming transaction records, player account records and AML/KYC documentation shall be retained for five years, or such longer period as required by applicable Curaçao legislation or the CGA.

Data shall be securely disposed of at end of life using cryptographic erasure, overwriting or degaussing, or physical destruction of media. Disposal shall be recorded.

### **13. Remote Access Policy**

#### **13.1. Purpose**

This section defines the requirements for secure remote access to the Company's internal resources, including systems supporting the CGA-licensed gaming platform.

#### **13.2. Scope**

Applies to all users and devices that require access to the Company's internal resources from remote locations.

### **13.3. Policy Definitions**

Remote access requires prior authorisation from IT Security. Only the responsible manager may request remote access; it is granted by Access Management.

The Company only permits network access to equipment management and servers via VPN. All remote access requests must be approved by the Key Official. Multi-factor authentication is mandatory for all remote access, in accordance with Section 7.5.

Only secure channels with mutual server-client authentication are permitted. Both server and client must use mutually trusted certificates.

Administrative and configuration activities shall be conducted exclusively over secure protocols such as SSH, SFTP and HTTPS. Insecure protocols including Telnet, HTTP and FTP shall be disabled unless explicitly required, risk-justified and documented as an exception.

All teleworking must be formally approved by the respective manager. Remote employees must: always connect via VPN; refrain from working in public places; ensure they are not subject to shoulder-surfing; adhere to all Code Harbor N.V. policies; and not disclose any information to bystanders including relatives and acquaintances.

Users must not connect from public computers.

## **14. Third-Party and Outsourcing Policy**

### **14.1. Purpose**

This section defines the requirements to minimise the risks associated with outsourcing IT services, functions and processes and with reliance on third-party providers, in line with the CGA's requirements regarding the use of third-party service providers by licensed operators.

### **14.2. Scope**

Applies to the Company, service providers to whom IT services are outsourced, B2B platform providers, game content aggregators, sports data feed providers, payment processors, cloud and hosting providers, and the outsourcing process itself.

### **14.3. Policy Definitions**

Where the Company relies on third-party platforms, hosting providers, game suppliers or managed security services, the Company remains fully responsible under the LOK for compliance with the CGA Requirements. Contractual delegation does not transfer regulatory accountability.

Before outsourcing any service, function, or process, a careful risk and financial evaluation must be conducted. A competitive selection process should be followed wherever possible.

Service providers must be selected after evaluating their reputation, regulatory standing, experience, and warranties. The CGA must be notified of material outsourcing arrangements where required by licence conditions.

A formal service contract and defined service levels must be agreed. The contract must include provisions for information security, data protection, data integrity guarantees, audit rights or the right to request evidence of compliance, and incident notification.

The service provider must obtain authorisation from the Company before engaging any sub-contractor.

Audits shall be planned in advance to evaluate the performance and compliance of the service provider both before and during the provision of the outsourced service.

#### **14.4. Service Provider Inventory**

The Company shall maintain a complete and current inventory of all service providers and vendors involved in delivering technical or operational support. The inventory shall separately identify:

- game content aggregators that supply or distribute game titles from multiple B2B studios;
- sports data feed providers that supply live results, odds, event data or statistics used in determining wager outcomes;
- B2B platform providers supplying Remote Gaming Servers, game engines or player management systems;
- cloud hosting and infrastructure providers;
- payment processors;
- security monitoring and support services.

For each provider the Company shall document: contract type and scope of services; internal contact or owner; classification of data or systems accessed; the nature and scope of data exchanged; contractual security and integrity obligations; certification or audit status; and procedures for detecting and responding to feed manipulation, data integrity failures or service disruptions.

The inventory shall be reviewed annually and upon any change to providers or services.

#### **14.5. B2B Certification Monitoring**

The B2B provider, as a CGA licensee in its own right, bears direct regulatory responsibility for obtaining, maintaining and renewing all required certifications for its gaming components, including RNG integrity, game logic and RGS platform security. The Company's obligations are those of due diligence, verification and reporting, and comprise:

- verifying the B2B provider's certification status at the point of onboarding and at defined intervals thereafter, at minimum annually;
- including contractual provisions requiring the B2B provider to maintain valid certifications and to notify the Company promptly of any lapse, withdrawal, scope change or pending renewal;
- contractual right-to-audit or right-to-request-evidence provisions;
- promptly notifying the CGA where the Company becomes aware that a B2B provider's certification has lapsed or been withdrawn;
- ceasing to offer game content from any B2B provider whose required certifications are no longer valid, until such certifications are restored;
- documented escalation procedures in the event of a certification lapse, including suspension of affected game content and notification to the CGA.

Where the CGA notifies the Company directly of a change to a B2B provider's certification status, the Company shall cease using the affected components within the timeframe specified by the CGA.

#### **14.6. Integrity of Externally Supplied Game Content and Data Feeds**

Where the Company relies on third-party providers for game content, sports data feeds, or aggregated results that influence wager outcomes, the following controls shall be implemented:

**Source authentication.** All data feeds shall be received over authenticated and encrypted channels. API connections shall use mutual TLS or an equivalent authentication mechanism.

**Data integrity validation.** Integrity checks shall be implemented on received data, using cryptographic signatures, hash verification or message authentication codes, to detect tampering or corruption in transit.

**Feed monitoring and anomaly detection.** The Company shall monitor feed availability, latency and data consistency, and shall maintain procedures to detect and respond to unexpected feed interruptions, result discrepancies or anomalous data patterns.

**Failover and suspension procedures.** The Company shall define and document procedures for suspending affected wagering markets or game offerings where feed integrity cannot be assured, and for resuming operations only after integrity has been re-established.

**Contractual assurances.** Agreements with feed providers and aggregators shall include requirements for security controls, incident notification, data integrity guarantees, and the right to audit or request evidence of compliance.

Where the Company offers sports betting, particular attention shall be given to the integrity of live event data feeds, as manipulation of such data can directly affect wager outcomes. Feed providers shall be able to demonstrate adequate controls against data manipulation at source.

## **15. Incident Management and Regulatory Notification**

### **15.1. Purpose**

This section defines the requirements for detecting, responding to and reporting information security incidents, including the obligation to notify the CGA and other competent authorities where required under Curaçao law.

### **15.2. Roles and Contacts**

The Company shall appoint a primary and a backup incident response manager. Roles shall be defined for IT, security, compliance, legal and communications functions, including roles for handling gaming-specific scenarios such as payout manipulation, feed manipulation or gaming integrity violations. Where external incident response services are used, internal oversight shall be retained.

The Company shall maintain and regularly update an incident contact directory covering internal stakeholders, the CGA, the FIU Curaçao, law enforcement, data protection authorities, insurers, B2B providers and vendors responsible for critical infrastructure.

Incident response roles and the contact directory shall be reviewed annually, or upon significant organisational or threat landscape changes.

### **15.3. Reporting and Escalation**

All information security incidents — including suspected breaches, unauthorised access, data loss, ransomware, or system compromise — must be reported immediately to the Information Security Officer.

The Information Security Officer shall conduct an initial assessment and escalate to the Key Official, the Compliance Officer and senior management as appropriate.

The Company shall define what constitutes a reportable incident, specify escalation criteria and reporting channels, maintain reporting templates, and make the reporting policy available to all employees and service providers.

#### **15.4. Mandatory CGA Notification**

**Pursuant to LOK Article 5, the Company shall notify the Curaçao Gaming Authority without undue delay, and in any event within 24 hours, of any security incident that:**

- compromises gaming integrity;
- affects player funds or personal data; or
- may impact regulatory reporting, system availability, or game fairness.

Failure to notify constitutes a breach of licence conditions under the LOK. The Compliance Officer is responsible for making the notification and the Key Official for approving it; in the absence of either, the Information Security Officer shall issue the notification within the required timeframe.

The notification shall include, as a minimum: the time of detection, the nature and suspected cause of the incident, the systems and data categories affected, the number of players affected or potentially affected, containment measures taken, and the planned remediation. Where full information is not available within 24 hours, an initial notification shall be made within the deadline and supplemented as the investigation progresses.

Where an incident involves a breach of player data, AML/KYC records, or any information protected under applicable Curaçao law, the Key Official shall additionally assess whether notification to the FIU Curaçao or other competent authorities is required, and act without undue delay.

#### **15.5. Post-Incident Review**

A post-incident review must be conducted following any material security incident. Findings, remediation actions, and lessons learned must be documented and retained for a minimum of five years. Remediation actions shall be tracked to closure by the Information Security Officer.

The Company maintains a documented incident response plan which is tested at least annually.

### **16. Secure Configuration Management**

#### **16.1. Purpose**

This section establishes the requirement to apply and maintain secure configurations across all enterprise systems, in order to reduce exposure arising from improperly configured systems.

#### **16.2. Policy Definitions**

The Company shall develop and maintain documented secure configuration standards (hardening guides) for the following asset categories: physical and virtual servers; cloud instances and container images; security appliances such as intrusion detection systems and firewalls; user endpoints; and network infrastructure.

Hardening standards shall be based on vendor-recommended templates or recognised industry baselines such as the CIS Benchmarks. Standards shall be reviewed and updated annually, and whenever new technologies are deployed.

Where possible, configurations shall be managed using version-controlled scripts and infrastructure-as-code methods.

Performance requirements for gaming systems shall be preserved when applying hardening standards; where a hardening measure would materially degrade performance, a compensating control shall be documented and approved by the Information Security Officer.

#### **16.3. Default Accounts**

Default accounts shall be disabled or renamed on all systems, applications and devices, and all default passwords changed upon deployment. The Company shall maintain a list of default accounts and document justifications and compensating controls for any account retained. Embedded default accounts in proprietary gaming devices and platforms shall be managed in coordination with the relevant vendor.

## **17. Vulnerability and Patch Management**

### **17.1. Purpose**

This section establishes a documented, risk-based approach to identifying, prioritising and remediating vulnerabilities across enterprise assets, and to applying security updates.

### **17.2. Vulnerability Management**

The Company shall maintain a formal vulnerability management programme covering asset discovery and classification, vulnerability scanning schedules, risk evaluation criteria, and time-bound remediation guidelines.

Vulnerability scans shall be conducted at least monthly, and more frequently for critical systems. Automated scanning tools shall be used to detect issues across operating systems, network infrastructure, web applications and third-party software.

Threat intelligence and vendor advisories shall be integrated to adjust prioritisation, including sources specific to gaming environments such as vendor notifications relating to platform, RGS and RNG-related components in use.

Penetration testing shall be conducted at least annually and following significant changes to the gaming platform or infrastructure. Findings shall be tracked to closure.

The programme shall be reviewed annually or following major environmental changes.

### **17.3. Patch Management**

The Company shall maintain an automated and repeatable process for applying patches and updates. Patches for operating systems, software and firmware shall be applied at least monthly. Critical and actively exploited vulnerabilities shall be remediated on an accelerated basis in accordance with the documented remediation timelines.

Updates shall be tested in a staging or non-production environment before deployment, and patch deployment shall be automated where feasible using endpoint or systems management tooling.

Documentation of patch approvals, deployment results and exceptions shall be maintained. Compatibility impacts on critical gaming systems shall be assessed in coordination with vendors, and updates scheduled to avoid peak operating hours, service disruption or regulatory audit periods.

## **18. Logging, Monitoring and Audit Trails**

### **18.1. Purpose**

This section establishes the requirements for generating, collecting, protecting and reviewing audit logs in support of incident detection, investigation and regulatory compliance.

### **18.2. Audit Log Management Process**

The Company shall maintain a documented audit log management process identifying logging requirements by system type and business function, defining minimum retention periods based on

regulatory and business requirements, and covering centralised log collection, periodic review for anomalies, and archival and secure storage.

Access to audit logs shall be restricted to authorised personnel. The process shall be reviewed annually or upon significant changes to systems or operations.

### **18.3. Log Collection, Protection and Content**

Audit logging shall be enabled on all enterprise assets, including endpoints, servers, applications and security tools. Systems shall be configured to forward logs to centralised, tamper-resistant storage within the Company's SIEM platform.

Log integrity shall be protected using cryptographic hashing or write-once storage mechanisms. Log storage shall meet the defined retention and access control requirements.

Critical gaming logs shall include, as a minimum:

- gameplay and betting transactions;
- jackpot wins and other high-value events;
- player account creation, verification, deposits, withdrawals and balance adjustments;
- responsible gaming interventions and self-exclusion actions;
- all authentication events and access attempts;
- administrative access and system configuration changes.

Audit logs relating to gaming transactions and regulatory records shall be retained for a minimum of five years, in line with the retention schedule at Section 12.5.

## **19. Backup and Data Recovery**

### **19.1. Purpose**

This section establishes the requirements to recover data and restore systems in the event of a cyber incident, hardware failure or data corruption.

### **19.2. Data Recovery Strategy**

The Company shall maintain a documented data recovery strategy identifying which data types and systems require backup, with emphasis on critical gaming operations, and documenting procedures for data backup, storage and recovery testing.

The strategy shall define recovery point objectives (RPOs) and recovery time objectives (RTOs) for each critical system, and the security measures applicable to backup data, including access restrictions and encryption.

Gaming transaction data, platform configuration files, player account records and player activity logs shall be expressly included in the backup scope.

The strategy shall be reviewed annually or when major systems or regulatory requirements change.

### **19.3. Backup Execution and Protection**

Backups of systems handling sensitive or regulated data shall be automated and performed at a minimum weekly frequency. Gaming transaction logs and financial data shall be backed up daily or in real time in order to meet regulatory retention requirements and avoid data loss.

Offline, off-site or immutable storage shall be used where feasible to prevent tampering or ransomware-related corruption. Backup data shall be subject to the same access controls and security protections as the original production data.

Restoration tests shall be performed at least annually and the results documented, including any deviation from the defined RPOs and RTOs.

## **20. Network Infrastructure Security**

### **20.1. Purpose**

This section establishes the requirement to keep network infrastructure secure, supported and up to date.

### **20.2. Policy Definitions**

The Company shall maintain an inventory of all network infrastructure, including routers, switches, firewalls, load balancers, VPN concentrators and equivalent cloud networking components.

Firmware and software version status shall be reviewed at least monthly, and updates or patches applied based on vendor advisories and risk impact. Only supported versions shall be used; end-of-life products shall not be operated in live environments.

Updates shall be coordinated with gaming system maintenance windows and support continuity with third-party vendors shall be ensured.

Networks shall be segregated by function in accordance with Section 7.3, and administrative interfaces shall be accessible only over secure protocols and from authorised networks.

## **21. Security Awareness and Training**

### **21.1. Purpose**

This section establishes the requirement to educate employees and stakeholders on cybersecurity, in order to prevent social engineering attacks and ensure secure practices are followed throughout operations.

### **21.2. Awareness Programme**

Baseline cybersecurity training shall be provided to all personnel during onboarding and repeated at least annually, or in response to policy or threat changes. Completion shall be recorded and evidence retained for inspection.

Training shall cover secure system and asset use, regulatory obligations and compliance expectations, and gaming-specific threats and use cases, including gaming fraud, data privacy, and social engineering techniques targeting online operators.

### **21.3. Role-Based Training**

Additional training shall be delivered to roles carrying elevated risk, covering:

- social engineering defence — recognition of phishing, business email compromise and pretexting;
- authentication practices — password hygiene, MFA use and credential protection;
- data handling — secure storage, transfer, archival and destruction;
- unintentional exposure — prevention of accidental data loss or misdelivery;

- incident awareness — how to detect and report potential incidents;
- security updates — reporting missing or failed software patches;
- network safety — risks of using insecure networks, particularly for remote access.

Simulated exercises involving gaming-specific threats and compliance-driven procedures, including phishing simulations, shall be conducted at least annually.

## **22. Physical and Environmental Security**

### **22.1. Purpose**

This section establishes physical and environmental controls protecting infrastructure, sensitive areas and equipment from unauthorised access, tampering and environmental threats.

### **22.2. Policy Definitions**

Physical access to secure areas, including offices housing administrative access to gaming systems and any server or communications rooms, shall be restricted using access cards, biometric scanners or equivalent controls.

Entry logs shall be maintained and reviewed periodically. Surveillance systems shall be deployed to cover critical locations where applicable.

Environmental safeguards, including climate controls, smoke detection and uninterruptible power supplies, shall be installed in areas housing Company equipment.

Clean desk and clear screen practices shall be enforced. Equipment stored or used off-premises shall be secured in accordance with Section 6.3.

Where infrastructure is hosted by a cloud or data centre provider, the Company shall obtain and retain evidence of the provider's physical security certifications, and shall document the allocation of physical security responsibilities under the shared responsibility model.

## **23. Human Resource Security**

### **23.1. Purpose**

This section establishes the management of security responsibilities throughout the employment lifecycle in order to reduce personnel-related risk.

### **23.2. Policy Definitions**

Background checks shall be conducted for new hires in critical or sensitive roles. Enhanced screening shall be applied to employees managing financial systems, player data, AML/KYC functions or gaming system oversight, and to holders of privileged administrative access.

Confidentiality obligations shall be included in all employment and contractor agreements.

Employees shall acknowledge their security responsibilities and confirm that they have read this Policy during onboarding and following any material revision. Records of acknowledgement shall be retained.

Disciplinary action shall be enforced for non-compliance with this Policy.

During offboarding, Company assets shall be reclaimed and all accounts disabled promptly in accordance with Section 7.3.

## **24. Legal and Regulatory Compliance**

### **24.1. Purpose**

This section establishes the requirement to identify and comply with all legal, regulatory and contractual information security obligations.

### **24.2. Policy Definitions**

The Compliance Officer shall maintain a register of applicable laws, regulations, licence conditions and contractual obligations, including the LOK, the LCC, the CGA Requirements, NOIS, NORUT, sanctions legislation and applicable personal data protection legislation.

Responsibility for tracking legal and regulatory changes shall be assigned, and the register reviewed at least annually and upon publication of new or amended regulatory instruments.

Controls shall be implemented to safeguard personal data and intellectual property, and data retention and disposal procedures shall be aligned with legal requirements as set out in Section 12.5.

The Company shall be able to demonstrate compliance during CGA inspections and shall support CGA reporting requirements.

## **25. Business Continuity and Operational Resilience**

### **25.1. Purpose**

This section establishes the requirement to maintain information security during disruptions and to ensure that critical systems remain available.

### **25.2. Policy Definitions**

Information security shall be integrated into the Company's business continuity and disaster recovery plans. Those plans shall be tested and reviewed at least annually, or when significant changes occur, and the results documented.

Failover and redundancy shall be implemented for mission-critical gaming systems. Transaction processing systems, real-time reporting tools and regulatory interfaces shall have defined fallback procedures.

Change management shall include a documented risk assessment for changes affecting gaming systems, player data or regulatory reporting.

Data masking and controlled access shall be used during audits, testing and development activities, in accordance with Section 26.

## **26. Cryptographic Controls and Key Management**

### **26.1. Purpose**

This section establishes the use of cryptographic protections and data masking to safeguard gaming, player and financial data.

### **26.2. Policy Definitions**

Sensitive and regulated data shall be encrypted at rest and in transit using secure, industry-standard algorithms and protocols. Deprecated algorithms and protocol versions shall not be used.

The Company shall operate a documented key management programme covering key generation, distribution, storage, rotation, use, revocation and retirement. Encryption keys shall be stored separately from the data they protect and access to key material shall be restricted and logged.

Data masking or synthetic data shall be applied in development, testing, QA and analytics environments. Production player data shall not be used in non-production environments without documented approval from the Information Security Officer and appropriate masking.

The Company shall maintain a register of cryptographic controls in use and of any approved exceptions. Player credentials, player financial data, RNG-related records and jackpot trigger data shall be encrypted and masked as appropriate.

## **27. Security Governance and Oversight**

### **27.1. Purpose**

This section establishes the governance structures and procedures ensuring that the information security programme remains effective, compliant and continuously improving.

### **27.2. Policy Definitions**

Executive responsibility for information security oversight is assigned to the Chief Executive Officer, supported by the Information Security Officer and the Compliance Officer.

Independent reviews of policy compliance and control effectiveness shall be conducted at least annually. Reviews may be performed by an internal function independent of IT operations or by an external assessor.

Documented operational procedures shall be maintained for key activities, including backups, user access administration, patching, logging and audits.

Corrective actions arising from reviews, audits, incidents and self-assessments shall be tracked to closure and their implementation monitored by the Information Security Officer.

Policies and standards shall be reviewed and approved on a recurring schedule, at minimum annually. Game audit data and compliance logs shall be governed with defined ownership and oversight.

## **28. Compliance Monitoring and Assurance**

### **28.1. Purpose**

This section sets out how the Company demonstrates compliance with the CGA Requirements.

### **28.2. Policy Definitions**

The Company shall demonstrate compliance through:

- annual self-assessment reports prepared using CGA-provided templates and confirmed by the Key Official;
- independent third-party security audits, which are mandatory for online operators;
- incident reporting in accordance with the CGA breach notification requirements set out at Section 15.4;
- cooperation with ongoing compliance monitoring by the CGA through reviews, inspections and technical validation, including unannounced assessments.

The Company shall maintain documentation demonstrating how each applicable control under the CGA Requirements is addressed, including controls implemented by cloud providers and B2B providers within the shared responsibility model. The control mapping at Annex A serves as the index to that documentation.

The Company acknowledges that failure to comply may result in formal written warnings, compliance orders, administrative financial penalties, enhanced security obligations, or temporary or permanent suspension of its licence.

The Company shall cooperate fully with CGA investigations and remediation timelines.

## 29. Policy History

| Version | Date       | Author / Owner               | Summary of Changes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|------------|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.0     | 01.11.2025 | Technical Department         | Initial issue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 2.0     | 04.06.2026 | Information Security Officer | Full revision to align with the CGA Information Security Control Requirements for CGA Licensees (B2C and B2B). Added enterprise asset, software, account and service provider inventories; unauthorised device detection; secure configuration and default account management; vulnerability and patch management; audit log management; backup and data recovery; network infrastructure security; DNS filtering and supported browsers/email clients; removable media controls; security awareness and role-based training; physical and environmental security; human resource security; legal and regulatory compliance register; business continuity; cryptographic controls and key management; security governance; and compliance monitoring. Introduced mandatory 24-hour CGA incident notification; aligned dormant account disablement to 45 days; made MFA mandatory for internet-facing, remote and administrative access; aligned inactivity timeouts; added Critical Gaming Data classification, sensitive data location inventory and retention schedule; expanded third-party management with B2B certification monitoring and data feed integrity controls; added CGA control mapping at Annex A. |

## **Annex A — Mapping to CGA Information Security Control Requirements**

The following table maps the sections of this Policy to the corresponding control requirements of the CGA Information Security Control Requirements for CGA Licensees (B2C and B2B).

| <b>CGA Requirement</b> | <b>Control Area</b>                                     | <b>Policy Section</b>                              |
|------------------------|---------------------------------------------------------|----------------------------------------------------|
| 1.9                    | Identify and Manage All Hardware and Software Assets    | 6.3, 6.4, 6.5, 6.6                                 |
| 1.10                   | Protect Sensitive and Regulated Data                    | 12.3, 12.4, 12.5, 6.3, 26                          |
| 1.11                   | Apply Secure Configuration to All Systems and Devices   | 16.2, 16.3, 7.3, 10.3, 13.3                        |
| 1.12                   | Manage User, Administrator and Privileged Accounts      | 7.3, 7.4, 8.3                                      |
| 1.13                   | Control and Monitor User Access to Systems and Data     | 7.3, 7.4, 7.5, 13.3                                |
| 1.14                   | Identify, Remediate and Patch Vulnerabilities           | 17.2, 17.3                                         |
| 1.15                   | Monitor and Safeguard System Activity Through Logging   | 18.2, 18.3                                         |
| 1.16                   | Protect Users from Web and Email Threats                | 9.3, 10.3, 10.4                                    |
| 1.17                   | Defend Against Malware and Unauthorized Removable Media | 11.3, 11.4                                         |
| 1.18                   | Ensure Recoverability of Critical Data and Systems      | 19.2, 19.3                                         |
| 1.19                   | Keep Network Infrastructure Secure and Updated          | 20.2                                               |
| 1.20                   | Educate Employees and Stakeholders on Cybersecurity     | 21.2, 21.3                                         |
| 1.21                   | Track and Manage Third-Party Service Providers          | 14.3, 14.4, 14.5, 14.6                             |
| 1.22                   | Prepare for and Respond to Security Incidents           | 15.2, 15.3, 15.4, 15.5                             |
| 1.23                   | Physical Security Controls                              | 22.2 (land-based specific controls not applicable) |
| 1.24                   | Human Resource Security Controls                        | 23.2                                               |
| 1.25                   | Legal and Regulatory Compliance Measures                | 24.2                                               |
| 1.26                   | Business Continuity and Operational Assurance           | 25.2                                               |

| <b>CGA Requirement</b> | <b>Control Area</b>                              | <b>Policy Section</b> |
|------------------------|--------------------------------------------------|-----------------------|
| 1.27                   | Security Governance and Oversight                | 27.2, 5               |
| 1.28                   | Cryptographic Controls and Data Masking          | 26.2                  |
| 1.8 / 1.35             | Compliance Requirements and Monitoring           | 28.2                  |
| 1.7                    | Scope, operating model and shared responsibility | 3                     |