

Information Security Policy

Cura Gaming B.V.

1. Purpose and Scope
2. Definitions
3. Information Security Objectives
4. Governance and Responsibilities
5. Risk Management
6. Data Classification and Handling
7. Access Control
8. Physical Security
9. Network Security
10. System Security and Hardening
11. Application Security
12. Third-Party and Partner Management
13. Incident Management and Reporting
14. Business Continuity and Disaster Recovery
15. Monitoring and Audit
16. Staff Training and Awareness
17. Policy Review and Continuous Improvement

1. Purpose and Scope

1.1 Purpose

This **Information Security Policy** (hereinafter the “Policy”) defines the framework for how **Cura Gaming B.V.** (hereinafter the “Company”) protects:

- Its **information assets**,
- The **confidentiality, integrity, and availability** of data,

- The **security of its systems, networks, and infrastructure**,
- The **privacy and rights of its Players and Partners**.

The Policy establishes:

- **Roles and responsibilities** for information security management,
- **Technical and organizational measures** to mitigate security risks,
- **Controls and procedures** to ensure compliance with:
 - Applicable **laws and regulations**,
 - **Licensing obligations** imposed by the Curaçao Gaming Control Board (GCB) and other relevant authorities,
 - Contractual obligations to **Partners, Players, and third parties**,
 - **ISO/IEC 27001** and recognized **industry best practices**.

This Policy supports the Company's strategic objectives by:

- Ensuring the **trust of Partners, Players, and regulatory authorities**,
- Reducing the risk of **information security incidents**,
- Protecting the Company's **brand reputation and commercial interests**,
- Enabling secure innovation and business growth.

1.2 Scope

This Policy applies to:

- **All employees, contractors, and consultants** of the Company,
- **All information systems**, networks, and services owned, operated, or controlled by the Company,
- **All data processed by the Company**, including but not limited to:
 - Player personal data,
 - Transactional data,
 - Game data,

- Financial data,
- Business and operational data,
- Partner data,
- Internal corporate data.
- **All locations** where the Company operates, including:
 - Corporate offices,
 - Remote/home-based work environments,
 - Data centers,
 - Cloud-hosted environments.
- **All third-party providers and Partners** with access to the Company's information assets, subject to appropriate contractual controls.

1.3 Relationship with Other Policies

This Policy shall be read and implemented in conjunction with:

- The Company's **Data Protection and Privacy Policy**,
- The Company's **Responsible Gaming Policy**,
- The Company's **Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Policy**,
- The Company's **B2B Responsible Gaming Policy**,
- Any other relevant internal policies, standards, and procedures.

1.4 Continuous Commitment

The Company recognizes that information security is a **continuous process**, not a static state.

Through this Policy, the Company commits to:

- Regularly reviewing and improving its information security controls,
- Staying aligned with evolving **threat landscapes** and **regulatory expectations**,

- Promoting a **culture of information security awareness and accountability** across the organization and Partner network.

2. Definitions

For the purposes of this Policy, the following definitions shall apply:

Information Asset

Any data, system, network, device, application, or process that stores, processes, transmits, or otherwise impacts the confidentiality, integrity, or availability of **Company information**.

Information Security

The preservation of:

- **Confidentiality** — ensuring that information is accessible only to those authorized to access it.
- **Integrity** — safeguarding the accuracy and completeness of information and processing methods.
- **Availability** — ensuring that authorized users have access to information and associated assets when required.

Confidential Data

Any data classified by the Company as **Confidential** or higher, including but not limited to:

- Player personal data,
- Financial transaction data,
- Game intellectual property (IP),
- Business strategy documents,
- Partner agreements and data,
- Any data subject to **privacy laws, contractual obligations, or regulatory requirements**.

Personal Data

Any information relating to an identified or identifiable natural person, as defined under the **General Data Protection Regulation (GDPR)** and other applicable privacy laws.

Data Owner

The designated individual or function responsible for:

- Classifying data,
- Defining access controls,
- Approving retention and disposal procedures,
- Ensuring appropriate protection of specific data sets.

Chief Information Security Officer (CISO)

The individual (or designated equivalent function) responsible for:

- Leading the Company's information security strategy,
- Overseeing the implementation of this Policy,
- Managing information security risks,
- Coordinating incident response.

Note: Where no dedicated CISO is appointed, the responsibilities are assigned to the Head of Compliance or designated Board-level owner.

Information Security Incident

Any identified occurrence or suspected occurrence that:

- Compromises, or has the potential to compromise, the confidentiality, integrity, or availability of Company information assets,
- Involves unauthorized access, disclosure, modification, destruction, or loss of information,
- Includes but is not limited to:
 - Cyberattacks,
 - Phishing attempts,
 - Data breaches,

- Insider threats,
- System outages caused by malicious acts.

Third Party

Any external entity, organization, or individual that:

- Provides services to the Company,
- Has access to the Company's information assets,
- Processes Company data under contract,
- Includes Partners, suppliers, vendors, contractors, and consultants.

Partner

For the purposes of this Policy, a Partner is a B2B entity that:

- Integrates, distributes, or operates the Company's gaming products,
- May have access to Company systems, APIs, or data,
- Is subject to contractual Responsible Gaming and Information Security obligations.

Risk Assessment

A systematic process to:

- Identify threats and vulnerabilities,
- Evaluate the potential impact of security risks,
- Define appropriate mitigation measures.

Security Control

A management, operational, or technical measure implemented to:

- Reduce security risks,
- Protect information assets,
- Ensure compliance with this Policy and applicable standards.

3. Information Security Objectives

3.1 General Principles

The Company recognizes that **information security** is a critical enabler of:

- **Business continuity**,
- **Regulatory compliance**,
- **Trust** among Partners, Players, and stakeholders,
- **Sustainable growth** in the global gaming ecosystem.

The objectives of this Policy and the broader Information Security Management System (ISMS) are to:

- Protect the Company's **information assets** from all forms of threat, whether internal or external, deliberate or accidental.
- Ensure that the Company meets and exceeds applicable **legal, regulatory, and contractual obligations** related to information security.
- Foster a **culture of security awareness and accountability** across the organization and Partner ecosystem.
- Enable **secure innovation** in the design, development, delivery, and operation of gaming products and services.

3.2 Core Information Security Objectives

The Company's core Information Security Objectives are as follows:

Confidentiality

- Ensure that **Confidential Data** is accessible only to authorized persons, whether internal staff or third parties.
- Prevent **unauthorized disclosure** of Player data, Partner data, and Company intellectual property.

Integrity

- Safeguard the **accuracy, completeness, and consistency** of information assets across their lifecycle.

- Protect systems and processes from **unauthorized or accidental modification**.

Availability

- Ensure that authorized users (internal and external) have **timely and reliable access** to information assets and services.
- Minimize the risk and impact of **service disruptions** due to security incidents or other factors.

Legal and Regulatory Compliance

- Comply fully with:
 - **Curaçao Gaming Control Board (GCB)** licensing requirements,
 - **General Data Protection Regulation (GDPR)** and other applicable privacy laws,
 - Relevant **cybersecurity and data protection laws** in key jurisdictions,
 - Contractual obligations to Partners, Players, and third parties.

Risk Management

- Maintain a formal, documented **Information Security Risk Management process**.
- Regularly assess and treat information security risks in alignment with **risk appetite** defined by the Board.

Secure System Development and Operations

- Embed **security by design** and **security by default** principles in:
 - Game development,
 - Platform development,
 - IT infrastructure and operations.
- Ensure that third-party systems and services integrated with the Company's products and infrastructure meet defined security standards.

Incident Preparedness and Response

- Maintain **robust incident detection, response, and recovery** capabilities.

- Minimize the impact of **Information Security Incidents** on:
 - Players,
 - Partners,
 - Company operations and reputation.

Continuous Improvement

- Continuously improve the Company's ISMS based on:
 - Internal audits,
 - Monitoring and metrics,
 - Lessons learned from incidents,
 - Evolving regulatory expectations,
 - Industry best practices (aligned with **ISO/IEC 27001** principles).

4. Governance and Responsibilities

4.1 General Principles

The Company is committed to maintaining a **clear and effective governance structure** to oversee the implementation, monitoring, and continuous improvement of its **Information Security Management System (ISMS)**.

Governance of information security is integrated into:

- The Company's **corporate governance framework**,
- The Company's **risk management framework**,
- The Company's **compliance and audit programs**.

The objective is to ensure that **information security responsibilities** are clearly defined and properly resourced at all levels of the organization.

4.2 Board of Directors

The **Board of Directors** has ultimate accountability for:

- Approving this Information Security Policy and any material updates.
- Setting the Company's **information security risk appetite**.
- Ensuring that **appropriate resources** are allocated to the ISMS.
- Overseeing the effectiveness of the Company's information security governance and risk management.

The Board receives:

- **Quarterly reports** on key information security risks, incidents, and metrics.
- **Annual reports** summarizing ISMS performance and improvement initiatives.

4.3 Risk Committee

The **Risk Committee** supports the Board by:

- Monitoring the Company's **information security risk exposure**.
- Reviewing the effectiveness of the ISMS and associated controls.
- Overseeing the alignment of information security with the Company's overall risk management strategy.
- Reviewing results of internal and external **information security audits**.

The Risk Committee meets at least **quarterly**.

4.4 Chief Information Security Officer (CISO)

The **Chief Information Security Officer (CISO)**, or designated equivalent, is responsible for:

- Developing and maintaining the Company's **Information Security Policy** and ISMS.
- Leading the implementation of security controls.
- Coordinating **information security risk assessments**.
- Managing the Company's **Information Security Incident Response** process.
- Ensuring that security awareness and training programs are effective.
- Advising management on **emerging threats** and appropriate mitigation strategies.

- Reporting regularly to:
 - The Risk Committee,
 - The Board of Directors.

If a formal **CISO** role is not yet appointed, the **Head of Compliance** or other designated Board-level owner assumes these responsibilities until such time as a dedicated CISO is established.

4.5 Compliance Team

The **Compliance Team** is responsible for:

- Ensuring that the Company meets applicable **regulatory and contractual obligations** relating to information security.
- Coordinating with the CISO on security-related compliance monitoring and audits.
- Supporting the Company's **Data Protection Officer (DPO)** in privacy-related aspects of information security.
- Facilitating **regulatory reporting** of Information Security Incidents where required.

4.6 Data Protection Officer (DPO)

The DPO, where appointed, is responsible for:

- Overseeing the privacy aspects of the ISMS.
- Ensuring that information security controls align with **GDPR** and other applicable data protection laws.
- Advising on **Privacy Impact Assessments** for new systems or data processing activities.
- Coordinating with the CISO on issues involving the intersection of **security and privacy**.

4.7 IT and Engineering Teams

The Company's **IT and Engineering Teams** are responsible for:

- Implementing **technical security controls** on infrastructure, applications, and networks.
- Conducting **secure software development** practices.
- Managing system and application **hardening and patch management**.
- Monitoring for **security events** and responding appropriately.

- Ensuring that **backup and recovery** systems are properly configured and tested.

IT and Engineering Teams work closely with the CISO to ensure that technical controls align with this Policy.

4.8 All Employees and Contractors

All employees and contractors of the Company have a responsibility to:

- Adhere to this Information Security Policy and related procedures.
- Complete mandatory **information security awareness training**.
- Protect Company information assets in accordance with their classification.
- Promptly report any suspected or actual **Information Security Incidents** to the appropriate channels.
- Cooperate with information security audits and investigations.

4.9 Third Parties and Partners

Third Parties and Partners with access to Company information assets must:

- Comply with **contractual information security obligations**,
- Implement **appropriate security controls** to protect Company data,
- Cooperate with the Company's monitoring, audit, and incident management processes.

Oversight of Third-Party and Partner information security is covered in **Section 12** of this Policy.

5. Risk Management

5.1 General Principles

The Company adopts a **risk-based approach** to managing information security.

Through a structured **Information Security Risk Management process**, the Company seeks to:

- Identify and assess information security risks that could impact:
 - The confidentiality, integrity, and availability of information assets,
 - Compliance with legal, regulatory, and contractual obligations,

- The trust of Players, Partners, and regulators,
- The Company's financial performance and reputation.
- Define and implement **appropriate controls** to mitigate identified risks to **acceptable levels**.
- Regularly monitor and review the information security risk landscape.
- Support informed **decision-making** at all levels of the organization.

5.2 Risk Assessment Process

The Company conducts formal **Information Security Risk Assessments**:

- **At least annually**, and
- **Ad hoc** when:
 - Significant changes are made to systems, infrastructure, or business processes,
 - New information security threats or vulnerabilities emerge,
 - New jurisdictions or regulatory requirements are introduced.

Risk assessments follow a documented methodology, including:

1. **Asset Identification**
 - Identify and classify information assets (per Section 6).
2. **Threat and Vulnerability Identification**
 - Identify relevant threat actors (external and internal).
 - Identify vulnerabilities in systems, processes, or controls.
3. **Risk Analysis**
 - Evaluate the likelihood and potential impact of each identified risk.
4. **Risk Evaluation**
 - Compare risk levels to the Company's defined **risk appetite**.
 - Prioritize risks requiring mitigation.
5. **Risk Treatment**

- Define and implement appropriate risk mitigation measures, which may include:
 - Technical controls,
 - Process changes,
 - Contractual controls on third parties,
 - Residual risk acceptance by senior management.

6. Documentation and Reporting

- Document risk assessments and treatments.
- Report significant risks to:
 - The CISO,
 - The Risk Committee,
 - The Board of Directors (for material risks).

5.3 Risk Appetite

The Company's **information security risk appetite** is defined by the Board of Directors and is based on the principle that:

- **No material risk to:**
 - The security of Player personal data,
 - The security of financial transactions,
 - The integrity of gaming outcomes,
 - The ability to meet regulatory and contractual obligations, will be knowingly accepted.

Where residual risks remain after applying reasonable controls, **formal risk acceptance** must be documented and approved by:

- The CISO, and
- The Risk Committee or Board (depending on severity).

5.4 Continuous Risk Monitoring

- The Company continuously monitors the information security risk landscape through:

- Threat intelligence feeds,
- Internal monitoring systems,
- Security testing results,
- Industry collaboration and regulator updates.
- The Information Security Risk Register is maintained as a **living document** and is reviewed:
 - **Quarterly** by the CISO and Compliance team,
 - **Quarterly** by the Risk Committee.

5.5 Integration with Enterprise Risk Management

Information Security Risk Management is fully integrated into the Company's **Enterprise Risk Management (ERM)** framework.

- Material information security risks are included in:
 - Enterprise risk reporting to the Board,
 - The Company's overall risk appetite framework.

6. Data Classification and Handling

6.1 General Principles

The Company applies a **data classification and handling framework** to ensure that:

- All information assets are appropriately protected according to their sensitivity and criticality.
- Controls for **confidentiality, integrity, and availability** are proportionate to the level of risk.
- Data handling practices comply with:
 - **Legal and regulatory requirements,**
 - **Partner contractual obligations,**

- **Privacy obligations** under **GDPR** and applicable data protection laws.

All employees, contractors, and third parties must adhere to this framework when handling Company data.

6.2 Data Classification Levels

The Company classifies data into the following categories:

1. Confidential Data

Definition:

- Data that, if disclosed or altered without authorization, could cause **material harm** to the Company, its Partners, Players, or stakeholders.

Examples:

- Player personal data,
- Financial transaction data,
- Intellectual property (game source code, algorithms),
- Partner contracts and data,
- Legal documents,
- Regulatory submissions,
- Security incident reports.

Handling Requirements:

- Must be encrypted at rest and in transit.
- Access restricted to **authorized personnel** only.
- Stored on **secure servers** with appropriate controls.
- Logging of access to critical systems.
- Prohibited from being stored on unsecured removable media.
- Prohibited from being transferred outside of approved jurisdictions without legal clearance.

2. Internal Data

Definition:

- Data that is not intended for public disclosure but does not require the highest level of protection.

Examples:

- Internal business processes,
- Project documentation,
- Internal communications,
- Non-confidential financial reports.

Handling Requirements:

- Access restricted to employees and contractors with a legitimate business need.
- Encryption recommended for external transmission.
- Internal systems access logged and monitored.

3. Public Data

Definition:

- Data that is intended for public release.

Examples:

- Website content,
- Marketing materials,
- Press releases,
- Regulatory disclosures explicitly designated as public.

Handling Requirements:

- No special protection requirements beyond ensuring **accuracy** and **integrity**.

6.3 Data Handling Principles

For all data classes, the following principles apply:

- **Data Minimization**

- Only the minimum necessary data shall be collected, processed, and retained.
- **Purpose Limitation**
 - Data shall only be used for explicitly defined and lawful purposes.
- **Retention and Disposal**
 - Data shall be retained only as long as necessary to fulfill:
 - Legal obligations,
 - Business needs,
 - Contractual requirements.
 - Data must be securely destroyed or anonymized when no longer required.
- **Access Control**
 - Access to data shall follow the **Principle of Least Privilege** — users are granted the minimum level of access necessary to perform their job functions.
- **Auditability**
 - Access to Confidential Data and sensitive Internal Data shall be logged and monitored.
 - Logs shall be retained and reviewed in accordance with the Company's audit procedures.

6.4 Special Considerations for Personal Data

In addition to the above:

- All processing of **Personal Data** must comply with:
 - **GDPR** (where applicable),
 - Other relevant data protection laws,
 - The Company's **Data Protection and Privacy Policy**.
- Any cross-border transfer of Personal Data must be subject to:
 - Appropriate **legal mechanisms** (e.g. Standard Contractual Clauses, adequacy decisions).

- Data Subject Rights requests (e.g. access, rectification, erasure) must be handled in coordination with the **Data Protection Officer (DPO)**.

6.5 Data Owner Responsibilities

Each **Data Owner** is responsible for:

- Classifying their data assets.
- Defining handling requirements consistent with this Policy.
- Reviewing data classifications periodically.
- Ensuring that access to their data is appropriate and reviewed regularly.

7. Access Control

7.1 General Principles

The Company implements a formal **Access Control framework** to ensure that:

- Access to information assets is granted **based on business need and role**,
- Users can only access data and systems required to perform their duties (**Principle of Least Privilege**),
- Access rights are **granted, reviewed, and revoked** in a controlled and auditable manner,
- Unauthorized access to Confidential Data and critical systems is **prevented and detected**.

7.2 User Access Management

User Provisioning

- Access to systems and data is granted only:
 - Upon receipt of a valid access request,
 - With approval from the designated **Data Owner** or system owner,
 - After completion of mandatory **security awareness training**.
- All user access requests must be documented and logged.

Authentication Requirements

- All users must be authenticated via:
 - **Unique user IDs** (no shared accounts),
 - Strong passwords complying with Company password standards,
 - Where applicable, **Multi-Factor Authentication (MFA)** — mandatory for access to:
 - Administrative accounts,
 - Remote access systems,
 - Cloud services.

User Privilege Management

- Administrative privileges (e.g. system admin, database admin, security admin) are:
 - Strictly controlled,
 - Granted only to authorized personnel,
 - Subject to heightened monitoring.
- Users are granted the **minimum level of access necessary** to perform their job functions.
- Privileged access must be:
 - **Time-limited** where possible,
 - Subject to regular review and revalidation.

Review of Access Rights

- User access rights are reviewed:
 - **Quarterly** for critical systems and Confidential Data,
 - **Annually** for all other systems.
- Reviews are conducted by:
 - System owners,
 - Data Owners,

- The CISO or designated security function.
- Access is adjusted or revoked based on review outcomes.

User Deprovisioning

- User access is revoked:
 - Immediately upon termination of employment or contract,
 - Upon change of role where existing access is no longer required.
- Deprovisioning is coordinated by:
 - Human Resources,
 - IT and Engineering teams,
 - Data Owners.

7.3 Access to Confidential Data

- Access to **Confidential Data** is subject to additional controls, including:
 - Explicit approval from the relevant Data Owner,
 - Access logging and monitoring,
 - Restriction to authorized networks and devices,
 - Encryption of data in transit and at rest.
- Any **external access** (by Partners, contractors, or third parties) to Confidential Data requires:
 - A valid contractual basis,
 - Approval by the CISO and Legal function,
 - Appropriate **Data Processing Agreements (DPAs)** where required by GDPR or other privacy laws.

7.4 Remote Access

- Remote access to Company systems is:
 - Restricted to authorized users,

- Permitted only through approved **secure channels** (e.g. VPN with MFA),
- Subject to monitoring and logging.
- Personal devices (BYOD) may only be used for remote access if:
 - Explicitly authorized,
 - Enrolled in Company-approved **Mobile Device Management (MDM)** or equivalent controls,
 - Compliant with Company security requirements.

7.5 Access Monitoring

- Access to critical systems and Confidential Data is:
 - Logged,
 - Monitored by the IT and Engineering teams and/or Security function,
 - Subject to periodic audit.
- Unusual or suspicious access patterns are:
 - Investigated promptly,
 - Escalated to the CISO and, where applicable, to the MLRO and/or Compliance team.

7.6 Segregation of Duties

- Where appropriate, the Company implements **segregation of duties** to:
 - Reduce the risk of malicious or accidental misuse of systems or data,
 - Ensure that no single individual has control over all aspects of critical processes (e.g. system configuration, access approval, transaction processing).
- Segregation of duties is reviewed as part of:
 - Role design,
 - Access reviews,
 - Internal audit.

8. Physical Security

8.1 General Principles

The Company implements **Physical Security controls** to protect its:

- **People,**
- **Facilities,**
- **Information assets,**
- **Systems and infrastructure,**

from unauthorized **physical access, damage, or interference.**

Physical Security is managed as an integral part of the Company's overall **Information Security Management System (ISMS).**

8.2 Scope

Physical Security controls apply to:

- Corporate offices,
- Data centers operated or controlled by the Company,
- **Cloud-hosted environments** (through contractual and compliance controls),
- Any third-party facilities processing or storing the Company's information assets,
- Remote work environments (minimum standards apply).

8.3 Physical Access Controls

Corporate Offices

- Offices must be protected by **controlled physical access systems**, such as:
 - Access card readers,
 - Keypad entry,
 - Biometric systems (where appropriate).

- Access rights are:
 - Granted only to authorized personnel,
 - Reviewed regularly,
 - Revoked immediately upon termination of employment or contract.
- Visitors must be:
 - Registered and logged,
 - Accompanied at all times while in restricted areas,
 - Issued **temporary visitor badges**,
 - Informed of security requirements.

Data Centers

- Data centers must meet industry best practices for **physical security**, including:
 - 24/7 security personnel,
 - CCTV surveillance,
 - Multi-factor access control,
 - Intrusion detection systems,
 - Environmental controls (fire suppression, temperature, humidity).
- Only authorized personnel may access Company systems and infrastructure housed in data centers.

Cloud Environments

- Where infrastructure is hosted in third-party cloud environments, the Company requires the provider to maintain:
 - **ISO/IEC 27001** or equivalent certifications,
 - Strong physical security controls as documented in third-party audit reports (e.g. **SOC 2**).
- The Company reviews provider security reports as part of **third-party risk management**.

8.4 Remote Work Environments

- Employees and contractors working remotely must:
 - Use **Company-approved secure devices**,
 - Work in **physically secure environments** (e.g. not in public spaces for Confidential Data access),
 - Protect devices from unauthorized access when unattended,
 - Report any loss or theft of Company devices immediately.

8.5 Equipment Protection

- All Company-owned laptops, desktops, and portable devices must be:
 - **Encrypted**,
 - Protected with strong authentication (passwords, MFA where applicable),
 - Locked when unattended.
- Servers and network equipment must be located in:
 - Secure, access-controlled rooms or cabinets,
 - With documented access procedures.

8.6 Environmental Security

- Critical facilities must be protected from:
 - Fire,
 - Flood,
 - Power failure,
 - Other environmental hazards.
- Appropriate **environmental controls and monitoring** must be in place.

8.7 Monitoring and Audit

- Physical access logs for:

- Corporate offices,
- Data centers,
- Other secure areas,
- must be maintained and periodically reviewed.
- The CISO and/or Security function may conduct:
 - **Physical security audits,**
 - Spot checks,
 - Investigations following physical security incidents.

8.8 Incident Response

- Physical security incidents (e.g. unauthorized access attempts, lost/stolen devices, facility breaches) must be:
 - Reported immediately to the CISO and Security function,
 - Investigated promptly,
 - Logged in the **Information Security Incident Register**,
 - Escalated where necessary to:
 - The Risk Committee,
 - The Board,
 - Regulatory authorities (where legally required).

9. Network Security

9.1 General Principles

The Company implements a layered **Network Security architecture** to:

- Protect its networks and systems from unauthorized access and attack,
- Ensure the **confidentiality, integrity, and availability** of data in transit,

- Monitor for **malicious or anomalous activity**,
- Support regulatory and contractual **security compliance requirements**.

Network Security is managed in alignment with **ISO/IEC 27001** and industry best practices.

9.2 Network Segmentation

- The Company maintains **network segmentation** to:
 - Separate production, development, and testing environments,
 - Isolate systems handling **Confidential Data** and **Personal Data**,
 - Limit lateral movement in the event of a breach.
- Access between network segments is:
 - Restricted by firewalls or equivalent controls,
 - Governed by strict **access control rules**,
 - Logged and monitored.

9.3 Perimeter Security

- Network perimeters are protected by:
 - **Next-Generation Firewalls (NGFW)**,
 - **Intrusion Detection and Prevention Systems (IDPS)**,
 - **Web Application Firewalls (WAF)** (for internet-facing services).
- Perimeter defenses are:
 - Configured to **deny by default**,
 - Regularly reviewed and updated,
 - Subject to continuous monitoring.

9.4 Encryption

- All network traffic carrying **Confidential Data** or **Personal Data** must be:
 - Encrypted using strong, industry-standard protocols (e.g. **TLS 1.2** or higher).

- Internal network traffic is encrypted where:
 - Data traverses untrusted or shared networks,
 - Regulatory or contractual requirements mandate encryption.
- Network devices and systems must support **secure cryptographic standards** — deprecated protocols (e.g. SSL, TLS <1.2) are prohibited.

9.5 Remote Access Security

- Remote access to Company networks is permitted only through:
 - **VPN connections** using strong encryption,
 - **Multi-Factor Authentication (MFA)**.
- Split tunneling is prohibited unless specifically approved by the CISO.
- Remote access traffic is subject to:
 - Logging,
 - Monitoring,
 - Periodic security review.

9.6 Wireless Network Security

- Corporate wireless networks must:
 - Use **strong authentication** and **encryption** (e.g. WPA3 or equivalent),
 - Be segmented from production systems and Confidential Data unless explicitly authorized,
 - Be monitored for unauthorized access attempts.
- **Guest wireless networks** are logically isolated from internal systems.

9.7 Network Monitoring and Logging

- The Company maintains **continuous network monitoring** to detect:
 - Unauthorized access attempts,
 - Malware or command-and-control traffic,

- Anomalous traffic patterns.
- Network logs are:
 - Generated for critical devices and systems,
 - Retained in accordance with the Company's log retention policy,
 - Protected against unauthorized modification or deletion.
- The CISO and Security function review **network security reports** regularly.

9.8 Network Security Testing

- The Company conducts **regular network security testing**, including:
 - **Vulnerability scanning**,
 - **Penetration testing** (at least annually and after significant network changes),
 - **Configuration reviews** of firewalls, routers, and switches.
- Identified vulnerabilities are:
 - Assessed for risk,
 - Remediated based on severity and business impact,
 - Tracked to closure under formal management oversight.

9.9 Third-Party Network Connectivity

- Any third-party connectivity to the Company's networks (including Partners and service providers) is:
 - Approved by the CISO and Legal/Compliance,
 - Subject to **network security controls** equivalent to those applied internally,
 - Monitored and periodically reviewed.
- Third-party access must:
 - Be limited to the minimum necessary,
 - Be time-bound where possible,
 - Be subject to strict access control and logging.

10. System Security and Hardening

10.1 General Principles

The Company implements **System Security and Hardening** controls to ensure that:

- All systems are securely configured to **minimize vulnerabilities**,
- **Malware protection** is applied and kept current,
- Systems are **patched** in a timely manner,
- Hardening standards are consistently enforced across the Company's infrastructure.

These controls are critical to:

- Preventing exploitation of known vulnerabilities,
- Reducing the attack surface,
- Ensuring **confidentiality, integrity, and availability** of the Company's information assets.

10.2 Scope

This section applies to:

- Servers (physical and virtual),
- Network devices,
- Workstations and laptops,
- Mobile devices where applicable,
- Cloud-based systems,
- Any third-party systems hosting or processing the Company's data.

10.3 Secure Configuration and Hardening

- All systems must be configured in accordance with documented **hardening standards**, aligned with industry best practices (e.g. **CIS Benchmarks**, vendor recommendations).
- Hardening standards include:

- Disabling unnecessary services and ports,
- Removing default accounts or changing default credentials,
- Enforcing strong authentication,
- Configuring secure logging,
- Implementing appropriate **file and directory permissions**,
- Enabling host-based firewalls where appropriate.
- Hardened system images are used for:
 - Servers,
 - End-user devices,
 - Virtual machines,
 - Cloud instances.
- System configurations are subject to:
 - **Baseline audits** at deployment,
 - **Periodic reviews** to ensure ongoing compliance.

10.4 Patch Management

- All systems must be kept **current with security patches**.
- The Company maintains a formal **Patch Management process** including:
 - Regular identification of applicable patches,
 - Risk assessment of patch applicability,
 - Timely deployment of critical security patches,
 - Testing of patches where necessary prior to production deployment.
- Patch timelines:
 - **Critical patches:** within 7 days of release (or sooner where feasible),
 - **High-risk patches:** within 14 days,
 - Other patches: as defined by the Patch Management schedule.

- Patch status is monitored and reported to:
 - The CISO,
 - The Risk Committee (summary view).

10.5 Malware Protection

- All endpoints (workstations, laptops, servers) must be protected by:
 - Current and centrally managed **anti-malware** solutions,
 - Real-time scanning,
 - Regular signature updates,
 - Automated malware removal/quarantine functionality.
- Malware protection effectiveness is:
 - Monitored continuously,
 - Reviewed regularly.
- Malware detection alerts are:
 - Investigated promptly,
 - Escalated where required.

10.6 Secure Software Development and Deployment

- For internally developed applications (including games and platform services), the Company applies **secure software development practices** including:
 - Code reviews,
 - Security testing (static and dynamic analysis),
 - Vulnerability scanning prior to release.
- Deployment processes include:
 - Verification of system hardening,
 - Application of relevant security patches,
 - Post-deployment validation checks.

10.7 Logging and Monitoring

- All systems must be configured to:
 - Generate security-relevant logs,
 - Protect logs from tampering,
 - Retain logs in accordance with the Company's **Log Management Policy**.
- The Security function monitors logs for:
 - Unauthorized changes to system configurations,
 - Indicators of compromise,
 - Other anomalous activities.

10.8 Third-Party System Requirements

- Where third-party providers host or process the Company's data:
 - The Company requires documented evidence that system hardening and patch management practices are in place and effective.
 - The Company reserves the right to audit or review such controls under **Third-Party Security Management** (see Section 12).

11. Application Security

11.1 General Principles

The Company adopts **Application Security** best practices to ensure that:

- Applications developed or operated by the Company are **secure by design**,
- Vulnerabilities are identified and mitigated during the **software development lifecycle (SDLC)**,
- Released applications do not expose the Company, its Players, or its Partners to **security risks**,
- Ongoing **monitoring and testing** are in place to maintain application security over time.

This applies to all applications, including:

- Company-developed games,
- Game platforms (e.g. Remote Gaming Servers, APIs),
- Internal business applications,
- Third-party integrated applications.

11.2 Secure Development Lifecycle (SDLC)

The Company implements a **Secure SDLC** framework that includes:

Design Phase

- Threat modeling conducted for critical applications.
- Security requirements defined during **application design**.
- Selection of secure architecture patterns.

Development Phase

- Adherence to **secure coding standards**, including but not limited to:
 - **OWASP Top 10** guidance,
 - Company internal development standards,
 - Industry best practices.
- Developers must complete **secure coding training** at least annually.

Testing Phase

- Security testing integrated into the SDLC:
 - **Static Application Security Testing (SAST)** — performed on source code.
 - **Dynamic Application Security Testing (DAST)** — performed on running applications.
 - **Manual security reviews** for critical applications.
- Identified vulnerabilities must be:
 - Assessed for risk,
 - Remediated prior to production release,

- Tracked to closure.
- Critical vulnerabilities must be remediated before application deployment.

Deployment Phase

- Secure configurations applied to production environments.
- Access to production systems restricted to authorized personnel.
- Post-deployment security validation conducted.

11.3 Third-Party and Open-Source Software

- Use of third-party libraries and **open-source components** is subject to:
 - Pre-use security review,
 - Ongoing monitoring for known vulnerabilities (e.g. via **Software Composition Analysis (SCA)** tools),
 - Timely patching or replacement of vulnerable components.

11.4 Penetration Testing

- The Company conducts **external penetration testing** of critical applications at least:
 - **Annually**, and
 - After major changes to application architecture or functionality.
- Penetration testing is performed by qualified, independent parties.
- Findings are:
 - Documented and risk-rated,
 - Remediated in accordance with the Company's vulnerability management process,
 - Reported to the CISO and the Risk Committee.

11.5 Application Vulnerability Management

- The Company maintains an **Application Vulnerability Management** process that includes:

- Regular scanning for vulnerabilities in applications,
- Tracking of vulnerabilities through to remediation,
- Reporting on outstanding vulnerabilities and remediation progress.
- Critical application vulnerabilities must be:
 - Addressed within 7 days (or sooner where feasible),
 - Subject to exception approval only at CISO level or above.

11.6 Application Logging and Monitoring

- Applications must generate **security-relevant logs**, including:
 - Authentication events,
 - Authorization failures,
 - Changes to critical data,
 - Suspicious activity patterns.
- Logs must be:
 - Protected against tampering,
 - Integrated with centralized **Security Information and Event Management (SIEM)** systems where applicable.
- The Security function monitors application logs to detect potential security events.

12. Third-Party and Partner Management

12.1 General Principles

The Company recognizes that **third-party service providers** and **Partners** can introduce **information security risks** to the organization.

Therefore, the Company applies **structured controls** to ensure that:

- Third parties and Partners with access to Company information assets, systems, or data:

- Meet defined **security standards**,
 - Comply with contractual **security obligations**,
 - Are subject to ongoing **security oversight**.
- Risks associated with third-party relationships are:
 - **Identified and assessed** prior to engagement,
 - **Mitigated** through appropriate controls,
 - **Monitored** throughout the lifecycle of the relationship.

This approach aligns with **ISO/IEC 27001** best practices and is required for compliance with:

- **GCB licensing obligations**,
- **GDPR** and other privacy laws,
- **Bank / PSP onboarding** requirements,
- **Operator / Partner due diligence** expectations.

12.2 Scope

This section applies to all third parties and Partners who:

- Process, store, or transmit **Company data** (including Confidential Data and Personal Data),
- Provide **IT infrastructure or services** to the Company,
- Access Company **networks or systems**,
- Integrate Company **gaming products** into their platforms,
- Provide **critical business services**.

Examples include:

- Cloud service providers,
- Game aggregators and operators,
- Payment processors,
- Customer support providers,

- Development partners,
- Marketing affiliates with access to data,
- Professional services firms with system or data access.

12.3 Third-Party Risk Assessment

Prior to entering into an agreement with a third party or Partner, the Company conducts a formal **Third-Party Risk Assessment**, including:

- **Information security posture** review:
 - Security certifications (e.g. ISO 27001, SOC 2),
 - Security policies and procedures,
 - Technical controls.
- **Data protection** and **privacy** compliance review:
 - GDPR / applicable privacy law compliance,
 - Data Processing Agreement (DPA) readiness.
- **Operational resilience**:
 - Business continuity and disaster recovery capabilities.
- **Incident response** processes and readiness.
- Any identified risks must be:
 - Documented,
 - Reviewed by the CISO and Compliance team,
 - Mitigated to an acceptable level before onboarding.

12.4 Contractual Security Requirements

All third-party and Partner contracts must include appropriate **information security clauses**, including but not limited to:

- Requirements to implement and maintain **industry-standard security controls**.
- Compliance with this **Information Security Policy** (where applicable).

- Requirements to comply with:
 - **Data protection and privacy laws,**
 - Relevant **Responsible Gaming obligations** (where applicable).
- Obligations to:
 - Promptly report **security incidents** affecting Company data,
 - Cooperate with the Company in **incident investigation and response,**
 - Undergo **security audits or assessments** by the Company or its designees.
- Prohibitions on:
 - Unauthorized **data transfers** outside approved jurisdictions,
 - Use of subcontractors without prior approval and risk assessment.

12.5 Ongoing Monitoring and Review

The Company maintains ongoing oversight of third-party and Partner security posture through:

- **Annual security reviews** of critical third parties,
- Periodic re-assessment of third-party risk levels,
- Monitoring of public sources for:
 - Reported security incidents,
 - Changes in certifications or compliance status.
- Regular review of:
 - Third-party incident reports,
 - Security test results where shared,
 - Audit findings.

12.6 Third-Party Access Control

- Third-party access to Company systems and data is:
 - **Approved** by the CISO and relevant Data Owner,

- **Limited** to the minimum necessary to perform contractual duties,
- **Time-bound** where appropriate,
- **Logged** and **monitored**.
- Access is reviewed:
 - Quarterly for critical systems,
 - Annually for all other systems.
- Third-party access is revoked immediately upon:
 - Contract termination,
 - Change of scope or business need,
 - Identified security risk or policy violation.

12.7 Incident Management for Third Parties

- Third parties and Partners must notify the Company **immediately** upon discovery of:
 - Any security incident affecting Company data or systems,
 - Any incident that may impact compliance with legal, regulatory, or contractual obligations.
- The Company's CISO will coordinate the joint response effort and reporting as appropriate.

12.8 Termination and Offboarding

Upon contract termination, third parties and Partners must:

- Return or securely destroy Company data,
- Provide written confirmation of data destruction where applicable,
- Cooperate in the decommissioning of any system integrations,
- Undergo a formal **offboarding review** to ensure that:
 - All access is revoked,
 - No residual data or system dependencies remain.

13. Incident Management and Reporting

13.1 General Principles

The Company maintains a formal **Information Security Incident Management** process to:

- Ensure timely detection and response to **Information Security Incidents**,
- Minimize potential harm to:
 - Players,
 - Partners,
 - Company operations,
 - Regulatory compliance,
 - Brand reputation,
- Ensure that incidents are:
 - **Fully investigated**,
 - **Documented**,
 - **Remediated**,
 - Used to drive **continuous improvement**.

The Incident Management process aligns with **ISO/IEC 27001**, GCB license requirements, GDPR obligations, and industry best practices.

13.2 Definition of an Information Security Incident

An **Information Security Incident** is any actual or suspected event that:

- Compromises, or has the potential to compromise, the **confidentiality, integrity, or availability** of:
 - Company information assets,
 - Player data,

- Partner data,
- Company systems or networks.

Examples include:

- **Data breaches** (confirmed or suspected),
- Unauthorized access attempts,
- Malware infections,
- Denial-of-Service (DoS/DDoS) attacks,
- Insider threats,
- Physical security breaches affecting systems or data,
- Loss or theft of devices containing Company data,
- Security failures of third-party services.

13.3 Roles and Responsibilities

CISO

- Owns the overall **Incident Management process**,
- Leads incident investigations,
- Coordinates communication with:
 - The Board and Risk Committee,
 - Regulators where required,
 - Affected Partners,
 - Legal counsel.

Security Team

- Conducts technical investigation and analysis,
- Implements **containment, eradication, and recovery** actions,
- Maintains the **Incident Register**,

- Supports post-incident reviews.

Data Protection Officer (DPO)

- Assesses whether a reported incident constitutes a **Personal Data Breach** under GDPR,
- Coordinates data breach notification to:
 - Data protection authorities,
 - Affected data subjects (where required).

Compliance Team

- Ensures that regulatory reporting obligations are met,
- Coordinates with legal counsel on regulatory engagement,
- Supports audit of the Incident Management process.

All Employees and Contractors

- Must **immediately report** suspected or actual Information Security Incidents to:
 - The CISO,
 - The Security Team,
 - A designated security incident reporting channel.
- Are expected to fully cooperate in investigations.

13.4 Incident Response Process

The Company follows a structured Incident Response process:

1. Identification

- Detection of potential incidents via:
 - Security monitoring systems,
 - User reports,
 - Third-party notifications.

2. Containment

- Immediate actions to limit the spread or impact of the incident.
- 3. **Eradication**
 - Removal of malicious elements,
 - Closure of exploited vulnerabilities.
- 4. **Recovery**
 - Restoration of affected systems and services,
 - Verification of system integrity.
- 5. **Notification**
 - Regulatory and contractual notification obligations are assessed and executed (see 13.5).
- 6. **Post-Incident Review**
 - Conduct a **lessons learned** session,
 - Identify root causes,
 - Define and implement corrective actions.
- 7. **Documentation**
 - Full incident record maintained in the **Information Security Incident Register**.

13.5 Regulatory and Contractual Notifications

The Company complies with all applicable notification obligations, including:

- **GDPR:**
 - Notify supervisory authorities within **72 hours** of becoming aware of a Personal Data Breach (unless unlikely to result in risk to data subjects).
 - Notify affected data subjects where required.
- **GCB license:**
 - Notify the **Curaçao Gaming Control Board** of security incidents as required under licensing conditions.
- **Partner contracts:**

- Notify Partners of incidents affecting their data or systems in accordance with contractual terms.
- **Bank / PSP agreements:**
 - Notify Banks/PSPs of relevant incidents per contractual and compliance obligations.

Notification content and timing are approved by the:

- CISO,
- DPO (for Personal Data Breaches),
- Legal/Compliance team.

13.6 Incident Register and Reporting

- The **Information Security Incident Register** records:
 - All reported incidents,
 - Investigation findings,
 - Remediation actions,
 - Regulatory/Partner notifications made,
 - Lessons learned.
- The CISO provides:
 - **Quarterly reports** on incident trends to the Risk Committee,
 - **Annual summary reports** to the Board.
- Material incidents are escalated immediately to:
 - The Board,
 - The MLRO (if there is an AML/CFT dimension),
 - The CISO.

13.7 Continuous Improvement

Following each material incident:

- A **post-incident review** is conducted to:
 - Identify root causes,
 - Recommend process and control improvements.
- The Company updates:
 - Security controls,
 - Policies and procedures,
 - Training programs.
- Incident learnings are shared internally to enhance **security awareness and preparedness**.

14. Business Continuity and Disaster Recovery

14.1 General Principles

The Company maintains a formal **Business Continuity and Disaster Recovery (BCP/DR)** framework to ensure that:

- Critical business functions can be maintained or restored in the event of a disruption,
- Essential services to **Players** and **Partners** are preserved,
- The confidentiality, integrity, and availability of information assets are protected,
- The Company can meet regulatory and contractual **business continuity obligations**.

This framework supports:

- **ISO/IEC 27001** compliance,
- **GCB licensing requirements**,
- Bank / PSP expectations,
- Major Partner due diligence standards.

14.2 Scope

BCP/DR applies to:

- All critical Company functions,
- All information systems supporting critical services,
- All third-party services supporting critical operations,
- Key personnel and operational processes.

14.3 Business Continuity Planning (BCP)

BCP Objectives

- Minimize disruption to:
 - Player services,
 - Financial transactions,
 - Partner integrations,
 - Regulatory reporting,
 - Internal operations.
- Ensure:
 - Player data is protected,
 - Game integrity is preserved,
 - Communications with stakeholders are managed appropriately.

BCP Process

- The Company maintains documented **Business Continuity Plans** that define:
 - Recovery priorities,
 - Recovery time objectives (RTO),
 - Recovery point objectives (RPO),
 - Roles and responsibilities,

- Communication plans.
- Plans are reviewed and updated at least **annually**.

14.4 Disaster Recovery (DR)

DR Objectives

- Ensure that critical systems and data can be:
 - **Recovered within defined timeframes,**
 - Restored to a known secure state.

DR Process

- The Company maintains **Disaster Recovery Plans** covering:
 - Infrastructure recovery,
 - Application recovery,
 - Data recovery,
 - Third-party service recovery.
- Critical systems are supported by:
 - **Data backups** with tested restore capabilities,
 - Redundant infrastructure where appropriate,
 - Cloud-based resilience where applicable.
- Backup frequency and retention:
 - Backups performed at least **daily** for critical data,
 - Backups retained in accordance with Company policy and regulatory requirements,
 - Backups encrypted and stored securely.

14.5 Testing and Validation

- The Company conducts **BCP/DR testing**:
 - At least annually,

- After material changes to systems or operations.
- Testing includes:
 - Simulation of realistic disruption scenarios,
 - Verification of recovery procedures,
 - Validation of stakeholder communication processes.
- Test results are:
 - Documented,
 - Reviewed by the CISO and Risk Committee,
 - Used to drive continuous improvement of BCP/DR capabilities.

14.6 Third-Party Dependencies

- The Company identifies and monitors critical **third-party dependencies**.
- Contracts with critical third parties include:
 - **BCP/DR obligations**,
 - Requirements for periodic testing,
 - Reporting of BCP/DR test results to the Company where appropriate.
- The Company monitors third-party BCP/DR readiness as part of:
 - **Third-Party Risk Management** (see Section 12).

14.7 Continuous Improvement

- BCP/DR plans are updated based on:
 - Lessons learned from disruptions and tests,
 - Changes to Company operations or systems,
 - Regulatory and Partner feedback,
 - Industry best practices.

15. Monitoring and Audit

15.1 General Principles

The Company maintains a formal **Monitoring and Audit framework** to ensure that:

- The effectiveness of **Information Security controls** is continuously monitored,
- Compliance with this Information Security Policy is verified through systematic audits,
- Security risks are proactively identified and addressed,
- The Company meets regulatory, contractual, and **ISO/IEC 27001** obligations.

15.2 Security Monitoring

The Company implements **continuous security monitoring** across its:

- Networks,
- Systems,
- Applications,
- Cloud environments.

Monitoring capabilities include:

- **Intrusion Detection and Prevention Systems (IDPS)**,
- **SIEM (Security Information and Event Management)** tools,
- Network traffic analysis,
- Application activity monitoring,
- Endpoint security monitoring,
- Log aggregation and analysis.

Monitoring is designed to:

- Detect **unauthorized access attempts**,
- Identify **malicious activity**,

- Detect **policy violations**,
- Support **incident investigation** (see Section 13).

Monitoring findings are:

- Reviewed regularly by the Security team,
- Reported to the CISO,
- Escalated to the Risk Committee and Board as appropriate.

15.3 Internal Audits

The Company conducts **Internal Information Security Audits**:

- At least **annually**,
- Following major changes to:
 - Systems,
 - Infrastructure,
 - Business operations.

Internal audits cover:

- Compliance with this Policy and related procedures,
- Effectiveness of technical and organizational controls,
- Status of remediation of previously identified issues,
- Compliance with **ISO/IEC 27001** and GCB requirements,
- Alignment with contractual obligations to:
 - Partners,
 - Banks/PSPs,
 - Third parties.

Audit findings are:

- Documented,
- Reviewed by the CISO and Compliance team,

- Reported to the Risk Committee and Board.

Corrective actions are:

- Tracked through to closure,
- Subject to follow-up verification.

15.4 External Audits and Assessments

- The Company engages qualified **external auditors** to perform:
 - Independent Information Security assessments,
 - Penetration tests (see Section 11),
 - Gap analyses against relevant standards (e.g. ISO 27001, SOC 2).
- External audits may be:
 - Scheduled (e.g. annual ISO review),
 - Triggered by regulatory or contractual obligations,
 - Initiated based on Partner requests or risk triggers.
- External audit results are:
 - Reviewed by the CISO, Compliance team, and Board,
 - Used to drive continuous improvement.

15.5 Partner and Third-Party Audits

- The Company reserves the right to:
 - Conduct **security audits** of critical third parties and Partners,
 - Request evidence of third-party compliance with this Policy and contractual security obligations.
- Partner/Third-party audits may include:
 - Security questionnaires,
 - Document reviews,
 - On-site inspections (where contractually agreed).

15.6 Continuous Improvement

- The CISO leads a formal process of **continuous improvement** based on:
 - Internal and external audit findings,
 - Monitoring data,
 - Incident lessons learned,
 - Regulatory and Partner feedback,
 - Changes in threat landscape and best practices.
- Improvements are documented in:
 - Updated security controls,
 - Revised policies and procedures,
 - Enhanced training and awareness programs.

16. Staff Training and Awareness

16.1 General Principles

The Company recognizes that **employee awareness** is one of the most critical defenses against information security threats.

The Company is committed to ensuring that:

- All employees and contractors understand their **Information Security responsibilities**,
- Appropriate training and awareness programs are provided and maintained,
- Security culture is embedded across all levels of the organization.

This approach supports compliance with:

- **ISO/IEC 27001**,
- GCB licensing requirements,
- GDPR obligations (for Personal Data protection),
- Bank/PSP and Partner contractual obligations.

16.2 Scope

This section applies to:

- All employees (permanent and temporary),
- All contractors and consultants,
- Third-party service providers where required by contract.

16.3 Mandatory Security Awareness Training

All employees and contractors must complete **mandatory Information Security Awareness Training**:

- Upon onboarding (before being granted access to Company systems and data),
- At least **annually** thereafter,
- **Ad hoc**, where:
 - Significant security policy updates occur,
 - Specific threats require targeted awareness campaigns,
 - Role changes require additional security training.

16.4 Training Content

Training programs cover, at a minimum:

Core Topics

- The Company's **Information Security Policy**,
- **Data classification and handling** (Section 6),
- **Access control responsibilities** (Section 7),
- **Acceptable use of Company systems**,
- **Password management** and authentication best practices,
- **Malware awareness**,
- **Phishing and social engineering prevention**,

- **Incident reporting procedures** (Section 13),
- **Physical security** (Section 8),
- **Remote work security requirements**,
- GDPR and data privacy principles (in collaboration with the DPO).

Role-Specific Topics

- Developers: **secure coding** and **application security** (Section 11),
- System administrators: **system hardening** and **patch management** (Section 10),
- Security team: advanced threat awareness and **incident response**,
- Managers: security leadership and promoting a security culture.

16.5 Specialized Training

- The Company provides specialized training for staff in **high-risk roles**, including:
 - CISO and Security team members,
 - IT and Engineering teams,
 - Developers,
 - MLRO and Compliance staff,
 - Customer Support teams (handling Player data and Responsible Gaming concerns).
- Specialized training content is defined based on:
 - Role requirements,
 - Threat landscape,
 - Regulatory expectations.

16.6 Monitoring and Effectiveness

- Completion of mandatory training is:
 - Tracked by the CISO and Human Resources,
 - Reported to the Risk Committee.

- Non-compliance with mandatory training requirements results in:
 - Escalation to management,
 - Potential disciplinary action.
- Training effectiveness is assessed through:
 - **Knowledge assessments,**
 - Phishing simulations (where appropriate),
 - Feedback from staff.
- Lessons learned from incidents and audits feed into continuous improvement of training content.

16.7 Security Culture

The Company promotes a strong **Security Culture** by:

- Encouraging all staff to take ownership of Information Security,
- Reinforcing key security messages through:
 - Internal communications,
 - Security awareness campaigns,
 - Recognition of positive security behaviors.
- Fostering an environment where staff feel empowered to:
 - Report suspected security incidents,
 - Raise security concerns,
 - Suggest improvements.

17. Policy Review and Continuous Improvement

17.1 General Principles

The Company is committed to ensuring that this **Information Security Policy**:

- Remains aligned with evolving **threat landscapes**,
- Reflects current **regulatory and contractual requirements**,
- Incorporates **industry best practices** (ISO/IEC 27001 and beyond),
- Supports the Company's strategic objectives and risk appetite.

Continuous improvement is a core principle of the Company's Information Security Management System (ISMS).

17.2 Policy Review Cycle

This Policy shall be formally reviewed:

- At least **annually**, and
- **Ad hoc**, where:
 - Significant changes occur to Company systems, operations, or structure,
 - New legal or regulatory requirements are introduced,
 - Material security incidents or audit findings warrant updates,
 - Lessons learned indicate opportunities for improvement.

17.3 Review and Approval Process

The review and approval process is as follows:

- The **CISO** (or designated security lead) initiates and manages the review process.
- Proposed updates are developed in consultation with:
 - The Compliance team,
 - The DPO (for privacy-related impacts),
 - The Legal function,
 - IT and Engineering teams,
 - Other relevant stakeholders.
- The updated draft Policy is:

- Reviewed and endorsed by the **Risk Committee**,
- Submitted to the **Board of Directors** for formal approval.

17.4 Communication of Updates

- Material updates to this Policy are communicated to:
 - All employees and contractors (mandatory awareness updates),
 - Relevant third parties and Partners (where applicable to contractual obligations).
- Associated **training materials and security procedures** are updated accordingly.

17.5 Continuous Improvement

Continuous improvement of the Information Security Policy and broader ISMS is informed by:

- **Internal and external audit findings**,
- Outcomes of security monitoring and testing,
- Post-incident reviews and lessons learned,
- Regulatory feedback,
- Emerging threats and new technologies,
- Evolving industry best practices,
- Feedback from employees, Partners, and third parties.

The Company promotes a culture of **ongoing security maturity**, recognizing that information security is a **dynamic, evolving discipline**.