



CANARY ALLEY B.V.

INFORMATION SECURITY POLICY

Version:

Approved By:

Review Frequency:

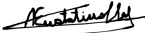
Effective Date:

2.0

Board of Directors

Annual or upon material regulatory change

09/06/2026

Previous Version	Current Version	Edit Date	Changes	Editor	Signature
---	1.0	10/07/2025	First Version	MO	
1.0	2.0	09/06/2026	Second version – rewritten to comply with LOK 24th December 2024 - Official English Translation, Information Security Control Requirements for CGA Licensed for CGA Licensees (B2C and B2B) April 2026	MO	Signed by:  8737E2B30CF043F... Director: Signed by:  E9C1A4A3F74E4ED... Director:



SECTION 1

GOVERNANCE & INFORMATION SECURITY MANAGEMENT SYSTEM

1.1 Purpose

The purpose of this Information Security Management System Manual ("ISMS Manual") is to establish the governance framework, security controls, procedures and responsibilities necessary to ensure the confidentiality, integrity and availability of Canary Alley B.V.'s information assets, gaming systems, player information and supporting infrastructure.

The ISMS has been designed to support:

- compliance with applicable legal and regulatory obligations;
- protection of player information;
- protection of player funds;
- secure operation of gaming systems;
- operational resilience;
- prevention and detection of cyber threats;
- protection of intellectual property;
- maintenance of trust and confidence in the Company's services.

Information security shall be regarded as a business-critical function and an integral component of the Company's risk management framework.

1.2 Objectives

The Company's information security programme shall seek to achieve the following objectives:

Confidentiality

Information shall only be accessible to authorised persons and systems.

Integrity

Information shall be protected against unauthorised modification, corruption or destruction.

Availability

Information and systems shall remain available to authorised users when required.

Accountability

Actions performed within Company systems shall be attributable to identifiable individuals or processes.

Resilience



The Company shall maintain the capability to withstand, respond to and recover from disruptive events.

Compliance

The Company shall maintain compliance with all applicable regulatory, contractual and legal requirements.

1.3 Scope

This ISMS applies to:

Personnel

- Directors
- Employees
- Contractors
- Consultants
- Temporary staff
- Third-party personnel

Information Assets

- Player information
- Financial information
- AML records
- Responsible Gaming records
- Employee information
- Intellectual property
- Commercial information

Technology Assets

- AWS cloud infrastructure
- Production environments
- Testing environments
- Development environments
- Databases
- APIs



- Source code repositories
- End-user devices
- Corporate systems

Third Parties

- Platform suppliers
- Hosting providers
- Payment providers
- KYC providers
- Security vendors
- Managed service providers

1.4 Regulatory Framework

The ISMS shall be maintained having regard to:

- National Ordinance on Games of Chance (LOK);
- Curaçao Gaming Authority Information Security Control Requirements;
- Curaçao Gaming Authority licence conditions;
- applicable data protection legislation;
- contractual security obligations;
- recognised industry standards.

Where multiple requirements apply, the most stringent requirement shall be adopted unless otherwise approved by the Compliance Officer.

1.5 Information Security Governance Structure

The Company shall maintain a formal information security governance structure.

Ultimate responsibility for information security rests with the Board of Directors.

Day-to-day responsibility rests with the Compliance Officer acting as Information Security Officer.

Management shall be responsible for implementing and maintaining security controls within their areas of responsibility.

All employees share responsibility for protecting Company information.



1.6 Board Responsibilities

The Board shall:

- approve this Manual;
- approve material security policies;
- review significant security incidents;
- review annual information security reports;
- ensure adequate resourcing;
- oversee information security risk management;
- review material cyber risks;
- monitor remediation of significant findings.

The Board shall receive information security reporting at least annually and more frequently where significant risks arise.

1.7 Information Security Officer

The Compliance Officer shall fulfil the role of Information Security Officer.

Responsibilities include:

Governance

- maintaining the ISMS;
- maintaining security policies;
- coordinating security reviews;
- overseeing implementation of controls.

Risk Management

- maintaining the Information Security Risk Register;
- coordinating risk assessments;
- monitoring remediation activities.

Incident Management

- overseeing incident response activities;
- coordinating investigations;
- assessing regulatory notification obligations.

Supplier Oversight



- reviewing security due diligence;
- monitoring supplier security performance.

Reporting

- preparing management reports;
 - preparing annual ISMS reviews;
 - reporting significant issues to the Board.
-

1.8 Management Responsibilities

Managers shall:

- ensure implementation of applicable controls;
 - ensure employees comply with security requirements;
 - review access requests;
 - participate in risk assessments;
 - support investigations;
 - ensure remediation activities are completed.
-

1.9 Employee Responsibilities

All personnel shall:

- comply with this Manual;
- protect information assets;
- report security incidents immediately;
- complete mandatory training;
- comply with access control requirements;
- protect authentication credentials;
- avoid unauthorised software installation;
- follow security procedures.

Failure to comply with security requirements may result in disciplinary action.

1.10 Information Security Management System



The Company shall maintain a documented Information Security Management System comprising:

Governance Documents

- Information Security Manual
- Security Policies
- Standards
- Procedures

Operational Documents

- Risk Register
- Asset Register
- Incident Register
- Vulnerability Register
- Supplier Register

Monitoring Activities

- Access Reviews
- Vulnerability Reviews
- Security Monitoring
- Audit Activities

Assurance Activities

- Penetration Testing
- Disaster Recovery Testing
- Business Continuity Testing
- Supplier Reviews

1.11 Security Policy Framework

The ISMS shall be supported by subordinate policies including:

- Access Control Policy;
- Password Standard;
- Secure Development Standard;
- Vulnerability Management Procedure;



- Incident Response Plan;
- Business Continuity Plan;
- Disaster Recovery Plan;
- Supplier Security Procedure;
- Change Management Procedure;
- Data Retention Standard.

All subordinate documents shall be reviewed at least annually.

1.12 Continuous Improvement

The Company shall continually improve the effectiveness of its ISMS through:

- risk assessments;
- incident reviews;
- audit findings;
- penetration testing;
- supplier reviews;
- regulatory developments;
- management reviews.

Corrective actions shall be documented, assigned and tracked to completion.

This is now the beginning of a genuine audit-grade manual.

Next section should be:

Section 2 – Information Security Risk Management (approximately 6–8 pages)

which will define:

- risk methodology,
- likelihood/impact scoring,
- inherent vs residual risk,
- risk acceptance,
- treatment plans,
- risk register standards,



- annual risk assessment procedures,
- supplier risk assessment,
- cloud risk assessment,
- change-related risk assessment.

That section is one of the most important parts of the entire manual because almost every CGA security control flows from it.



SECTION 2

INFORMATION SECURITY RISK MANAGEMENT

2.1 Purpose

The purpose of the Information Security Risk Management Framework is to ensure that information security risks are identified, assessed, treated, monitored and reported in a consistent and documented manner.

The Company recognises that effective risk management forms the foundation of the Information Security Management System and supports compliance with regulatory requirements, protection of player information, operational resilience and the secure operation of gaming systems.

Information security risk management shall be integrated into the Company's wider enterprise risk management framework.

2.2 Risk Management Principles

The Company shall apply the following principles when managing information security risk:

Risk-Based Decision Making

Security controls shall be implemented based upon risk exposure rather than solely upon technical preference.

Proportionality

Controls shall be proportionate to:

- the nature of the threat;
- the likelihood of occurrence;
- the potential impact;
- the sensitivity of the affected assets.

Continuous Assessment

Risk assessments shall be reviewed regularly and whenever material changes occur.

Accountability

All identified risks shall have an assigned owner responsible for monitoring and remediation.

Documentation

Risk decisions shall be formally documented and retained for audit and regulatory purposes.



2.3 Risk Management Process

The Company shall operate a formal risk management process comprising:

Step 1 – Asset Identification

Identification of:

- systems;
- applications;
- databases;
- infrastructure;
- information assets;
- third-party services.

Step 2 – Threat Identification

Identification of threats including:

- cyber attacks;
- insider threats;
- fraud;
- data breaches;
- denial of service attacks;
- supplier failures;
- cloud failures;
- operational errors.

Step 3 – Vulnerability Assessment

Assessment of weaknesses that may be exploited by identified threats.

Step 4 – Risk Assessment

Evaluation of:

- likelihood;
- impact;
- overall risk exposure.

Step 5 – Risk Treatment

Selection and implementation of appropriate controls.



Step 6 – Monitoring

Ongoing review of risk status and effectiveness of controls.

2.4 Risk Categories

Information security risks shall be classified into the following categories.

Cybersecurity Risks

Including:

- malware;
- ransomware;
- phishing;
- credential theft;
- account compromise;
- denial of service attacks.

Technology Risks

Including:

- infrastructure failures;
- hardware failures;
- software defects;
- cloud platform failures.

Data Protection Risks

Including:

- unauthorised disclosure;
- accidental disclosure;
- loss of personal information;
- improper processing.

Operational Risks

Including:

- human error;
- inadequate procedures;



- inadequate training.

Supplier Risks

Including:

- third-party service failures;
- supplier security breaches;
- outsourced service disruptions.

Regulatory Risks

Including:

- failure to comply with regulatory requirements;
- inadequate security controls;
- failure to notify incidents.

2.5 Risk Assessment Methodology

The Company shall utilise a documented methodology to assess information security risks.

Risk assessments shall consider:

Likelihood

The probability that a threat will exploit a vulnerability.

Impact

The severity of consequences should the event occur.

Control Effectiveness

The extent to which existing controls reduce risk.

Residual Risk

The remaining risk after controls are applied.

2.6 Likelihood Ratings

Likelihood shall be assessed using the following scale.

Rating Description

- | | |
|---|----------|
| 1 | Rare |
| 2 | Unlikely |



Rating Description

- 3 Possible
- 4 Likely
- 5 Almost Certain

2.7 Impact Ratings

Impact shall be assessed using the following scale.

Rating Description

- 1 Insignificant
- 2 Minor
- 3 Moderate
- 4 Major
- 5 Severe

Impact assessments shall consider:

- financial impact;
- regulatory impact;
- player impact;
- operational impact;
- reputational impact.

2.8 Risk Matrix

Overall risk ratings shall be determined using the Company's approved risk matrix.

Likelihood × Impact Risk Level

- 1–4 Low
- 5–9 Medium
- 10–16 High
- 17–25 Critical



The Information Security Officer may increase a rating where regulatory or player protection concerns justify doing so.

2.9 Risk Treatment Options

Following assessment, risks shall be treated through one or more of the following approaches.

Mitigate

Implement controls designed to reduce risk.

Transfer

Transfer risk through contractual arrangements or insurance.

Avoid

Discontinue the activity creating the risk.

Accept

Accept the residual risk following formal approval.

2.10 Risk Acceptance

Only residual risks may be accepted.

Risk acceptance shall require:

Low Risk

Business owner approval.

Medium Risk

Department manager approval.

High Risk

Information Security Officer approval.

Critical Risk

Board approval.

All risk acceptance decisions shall be documented.

2.11 Risk Treatment Plans

Where remediation is required, a Risk Treatment Plan shall be prepared.

The plan shall include:



- risk reference;
- description;
- treatment actions;
- owner;
- target completion date;
- expected residual risk.

Progress shall be monitored until completion.

2.12 Information Security Risk Register

The Company shall maintain an Information Security Risk Register.

At a minimum, the register shall contain:

- Risk ID;
- Risk Description;
- Asset Affected;
- Threat;
- Vulnerability;
- Likelihood;
- Impact;
- Inherent Risk;
- Existing Controls;
- Residual Risk;
- Risk Owner;
- Treatment Plan;
- Target Date;
- Review Date.

The register shall be maintained by the Information Security Officer.

2.13 Risk Assessment Frequency

Formal information security risk assessments shall be performed:



Annually

Comprehensive ISMS risk review.

Following Significant Change

Including:

- major system changes;
- infrastructure changes;
- acquisitions;
- outsourcing arrangements.

Following Major Security Incidents

To identify lessons learned and control improvements.

Following Significant Regulatory Changes

To ensure continued compliance.

2.14 Project Risk Assessments

Information security risk assessments shall be conducted for:

- new systems;
- major software releases;
- infrastructure projects;
- cloud migrations;
- new suppliers.

Security risks shall be considered before implementation approval.

2.15 Third-Party Risk Assessments

The Company shall assess information security risks associated with third parties.

Assessment criteria shall include:

- access to Company systems;
- access to player data;
- security maturity;
- regulatory status;



- geographic location;
- subcontracting arrangements.

Third-party risk assessments shall be reviewed periodically.

2.16 Cloud Risk Assessments

The Company shall conduct specific assessments relating to cloud-hosted environments.

Assessments shall consider:

- access controls;
- cloud misconfigurations;
- data residency;
- encryption;
- resilience;
- backup arrangements;
- shared responsibility obligations.

2.17 Change-Related Risk Assessments

Material changes shall undergo security risk assessment before implementation.

Assessments shall evaluate:

- confidentiality impacts;
- integrity impacts;
- availability impacts;
- compliance impacts;
- rollback capability.

No material production change shall proceed without appropriate approval.

2.18 Risk Reporting

The Information Security Officer shall provide periodic risk reporting to management.

Reports shall include:

- critical risks;



- overdue remediation actions;
- emerging threats;
- supplier risks;
- security trends.

Material risks shall be escalated promptly.

2.19 Board Reporting

The Board shall receive an annual information security risk report.

The report shall include:

- significant risks;
 - critical vulnerabilities;
 - major incidents;
 - regulatory concerns;
 - remediation progress;
 - recommended improvements.
-

2.20 Continuous Risk Monitoring

Risk management shall be an ongoing process.

Risk assessments shall be updated whenever:

- threat landscapes change;
- vulnerabilities emerge;
- incidents occur;
- business activities change;
- regulatory expectations change.

The Information Security Officer shall ensure the Risk Register remains accurate, current and reflective of the Company's actual risk profile.



SECTION 3

ASSET MANAGEMENT AND INFORMATION CLASSIFICATION

3.1 Purpose

The purpose of this section is to establish the framework through which Canary Alley B.V. identifies, classifies, manages, protects and disposes of information assets throughout their lifecycle.

Effective asset management is essential to:

- protect player information;
- protect gaming systems;
- support regulatory compliance;
- facilitate incident response;
- support business continuity planning;
- maintain operational resilience.

The Company shall maintain accurate records of all material information assets and ensure appropriate controls are applied based upon asset classification and criticality.

3.2 Asset Management Principles

The Company shall ensure that:

- all material assets are identified;
- all material assets have an assigned owner;
- assets are classified according to sensitivity;
- assets are protected appropriately;
- asset inventories remain accurate;
- assets are reviewed periodically;
- assets are securely disposed of when no longer required.

Asset management controls shall apply throughout the asset lifecycle.

3.3 Asset Categories

Assets shall be categorised according to type.

Information Assets



Including:

- player information;
 - KYC documentation;
 - AML records;
 - Responsible Gaming records;
 - financial records;
 - corporate records;
 - contracts;
 - source code;
 - intellectual property.
-

Hardware Assets

Including:

- servers;
 - laptops;
 - desktops;
 - network devices;
 - firewalls;
 - storage devices;
 - backup devices;
 - mobile devices.
-

Software Assets

Including:

- gaming platforms;
- operating systems;
- databases;
- cloud services;
- monitoring tools;



- security tools;
 - productivity software.
-

Service Assets

Including:

- AWS services;
 - payment services;
 - KYC providers;
 - email platforms;
 - managed service providers;
 - monitoring services.
-

3.4 Asset Ownership

Every material asset shall have an identified owner.

Asset owners shall be responsible for:

- classification;
- access approval;
- security requirements;
- lifecycle management;
- periodic review;
- disposal approval.

Ownership shall be documented within the Asset Register.

3.5 Asset Register

The Company shall maintain a comprehensive Asset Register.

The register shall be maintained by the Information Security Officer.

At a minimum, the Asset Register shall contain:

- Asset ID;
- Asset Name;



- Asset Type;
- Owner;
- Classification;
- Environment;
- Criticality;
- Location;
- Supplier;
- Review Date.

The register shall be reviewed at least annually.

3.6 Hardware Asset Management

The Company shall maintain an inventory of hardware assets.

The inventory shall include:

- serial numbers;
- assigned users;
- locations;
- device status;
- encryption status.

Hardware inventories shall be reviewed periodically.

Lost or stolen devices shall be reported immediately.

3.7 Software Asset Management

The Company shall maintain a Software Asset Register.

The register shall include:

- software name;
- version;
- owner;
- licensing information;
- support status.



The Company shall take reasonable steps to prevent:

- unauthorised software installation;
- unsupported software use;
- unlicensed software use.

3.8 Cloud Asset Management

Cloud resources shall be inventoried and managed.

The inventory shall include:

- AWS accounts;
- virtual servers;
- storage services;
- databases;
- security services;
- networking components.

Cloud assets shall be reviewed periodically to identify:

- orphaned resources;
- excessive permissions;
- unnecessary services;
- security risks.

3.9 Information Classification Framework

Information shall be classified according to sensitivity and business impact.

Classification shall determine:

- handling requirements;
 - access requirements;
 - storage requirements;
 - transmission requirements;
 - retention requirements.
-



3.10 Public Information

Public information includes information approved for unrestricted disclosure.

Examples include:

- published marketing content;
- public terms and conditions;
- published policies;
- regulatory disclosures.

Public information may be shared externally without restriction once approved.

3.11 Internal Information

Internal information includes information intended for use within the Company.

Examples include:

- internal procedures;
- operational reports;
- meeting notes;
- internal communications.

Internal information shall not be publicly disclosed without authorisation.

3.12 Confidential Information

Confidential information includes information whose disclosure could adversely affect:

- the Company;
- players;
- suppliers;
- regulators.

Examples include:

- commercial agreements;
- financial information;
- internal investigations;
- supplier assessments;



- security documentation.

Confidential information shall be restricted to authorised personnel.

3.13 Restricted Information

Restricted information represents the highest classification level.

Examples include:

- player personal data;
- KYC documents;
- payment information;
- authentication credentials;
- cryptographic keys;
- security logs;
- vulnerability reports;
- source code repositories.

Restricted information shall receive enhanced protection.

3.14 Information Handling Requirements

Personnel shall handle information according to its classification.

Requirements may include:

- encryption;
- access restrictions;
- secure storage;
- transmission controls;
- disposal controls.

The Information Security Officer may define additional handling requirements where appropriate.

3.15 Data Storage Requirements

Confidential and Restricted information shall only be stored within approved systems.

Personnel shall not store Company information within:



- unauthorised cloud storage;
- personal email accounts;
- personal storage devices;
- unapproved applications.

3.16 Data Transmission Requirements

Confidential and Restricted information transmitted electronically shall be protected through appropriate encryption.

Personnel shall verify recipients before transmitting sensitive information.

The use of unsecured communication methods for Restricted information is prohibited.

3.17 Removable Media

Use of removable media shall be restricted.

Where removable media is required:

- business justification shall exist;
- encryption shall be utilised;
- information shall be removed when no longer required.

The Information Security Officer may prohibit removable media where risks outweigh benefits.

3.18 Printing Controls

Printing of Confidential or Restricted information shall be limited to legitimate business purposes.

Printed materials shall:

- be secured appropriately;
- not be left unattended;
- be disposed of securely.

3.19 Information Retention

Information shall be retained in accordance with:

- legal requirements;



- regulatory requirements;
- business requirements;
- contractual obligations.

Retention schedules shall be documented and reviewed periodically.

3.20 Secure Disposal

Information shall be securely destroyed when no longer required.

Approved disposal methods may include:

Electronic Records

- secure deletion;
- cryptographic erasure.

Physical Records

- cross-cut shredding;
- secure destruction services.

Hardware

- certified destruction;
- secure wiping.

Evidence of disposal shall be retained where appropriate.

3.21 Data Transfer Controls

Transfers of Confidential or Restricted information to third parties shall require:

- legitimate business purpose;
- appropriate authorisation;
- appropriate contractual protection;
- appropriate security controls.

The Company shall maintain records of material data-sharing arrangements.

3.22 Information Asset Reviews

Asset owners shall periodically review assets under their responsibility.



Reviews shall confirm:

- ownership remains appropriate;
- classification remains appropriate;
- access remains appropriate;
- retention remains appropriate.

Material issues shall be escalated.

3.23 Shadow IT Prevention

The Company shall take reasonable measures to identify and prevent unauthorised technology usage.

Examples include:

- unapproved software;
- unauthorised cloud services;
- unsanctioned file-sharing solutions;
- unapproved collaboration tools.

Personnel shall not introduce technology solutions without appropriate approval.

3.24 Asset Lifecycle Management

Asset management controls shall apply throughout the lifecycle of an asset:

Acquisition

Security requirements identified.

Deployment

Secure configuration applied.

Operation

Monitoring and maintenance performed.

Change

Changes controlled and documented.

Retirement

Secure disposal completed.

Lifecycle activities shall be documented where appropriate.



3.25 Management Reporting

The Information Security Officer shall periodically report to management regarding:

- asset inventory completeness;
- classification compliance;
- disposal activities;
- unauthorised technology usage;
- asset-related risks.

Material deficiencies shall be remediated promptly.

3.26 Compliance Monitoring

Compliance with asset management and classification requirements shall be reviewed periodically through:

- access reviews;
- internal audits;
- security assessments;
- management reviews.

Deficiencies shall be documented and tracked to completion.

SECTION 4

ACCESS CONTROL AND IDENTITY MANAGEMENT

4.1 Purpose

The purpose of this section is to establish the controls governing authentication, authorisation, access provisioning, access review and identity management within Canary Alley B.V.

Access control is a fundamental security control designed to ensure that access to Company systems, information and infrastructure is granted only to authorised individuals for legitimate business purposes.

The Company shall operate a least-privilege access model supported by documented approval, monitoring and review processes.

4.2 Access Control Principles

The Company shall apply the following principles:

Least Privilege



Users shall receive only the minimum level of access necessary to perform their duties.

Need-to-Know

Access to information shall only be granted where a legitimate business requirement exists.

Accountability

All access shall be attributable to an identifiable individual or authorised system process.

Segregation of Duties

High-risk functions shall be separated to reduce opportunities for fraud, error and abuse.

Periodic Review

Access rights shall be reviewed regularly to ensure continued appropriateness.

4.3 Identity Management Framework

The Company shall maintain processes governing:

- user creation;
- user modification;
- user removal;
- authentication;
- authorisation;
- access review;
- privileged access management.

Identity management shall cover:

- employees;
- contractors;
- consultants;
- suppliers;
- service accounts.

4.4 Access Categories

Access shall be categorised as:

Standard User Access

Access required for ordinary business activities.

Elevated Access



Additional permissions required to perform specialist functions.

Administrative Access

Privileged access capable of altering systems, configurations or security controls.

Service Account Access

System-to-system access used by applications and automated processes.

4.5 Access Request Process

All access requests shall:

- be documented;
- identify the systems required;
- identify the business justification;
- identify the required access level;
- identify the approving manager.

Access shall not be granted without appropriate approval.

4.6 Access Approval Requirements

Access approvals shall be granted by:

Standard Access

Relevant manager.

Elevated Access

Relevant manager and system owner.

Administrative Access

System owner and Information Security Officer.

Production Access

System owner and Information Security Officer.

4.7 User Account Creation

User accounts shall:

- be uniquely identifiable;
- be assigned to a specific individual;
- be documented;



- be linked to approved access requests.

Anonymous user accounts are prohibited.

4.8 Joiner Process

Prior to granting access:

Employment Verification

Employment or engagement shall be confirmed.

Role Determination

Required access shall be determined.

Approval

Appropriate approvals shall be obtained.

Provisioning

Access shall be provisioned in accordance with approved roles.

Recording

The access granted shall be recorded within the Access Register.

4.9 Mover Process

When personnel change roles:

- access rights shall be reviewed;
- obsolete permissions shall be removed;
- new permissions shall require approval;
- segregation of duties conflicts shall be assessed.

Role changes shall not result in cumulative access rights without review.

4.10 Leaver Process

Upon termination of employment or engagement:

Immediate Actions

- accounts disabled;
- MFA revoked;
- privileged access removed;
- remote access revoked.



Asset Recovery

- laptops returned;
- devices returned;
- credentials surrendered.

Verification

Completion shall be documented.

Access removal should occur on the final working day unless circumstances require earlier action.

4.11 Role-Based Access Control

The Company shall utilise Role-Based Access Control ("RBAC") wherever practical.

Roles shall be defined according to job responsibilities.

Examples include:

- Customer Support;
- Compliance;
- Finance;
- Marketing;
- Developers;
- Infrastructure Administrators;
- Information Security Officer.

Access shall be granted through approved role profiles where possible.

4.12 Segregation of Duties

The Company shall implement segregation of duties controls for critical processes.

Examples include:

Access Administration

Separate from access approval.

Development

Separate from production approval.

Payments

Separate from reconciliation activities.

Security Monitoring



Separate from system administration where feasible.

Exceptions shall be documented and approved.

4.13 Authentication Standards

All users shall be authenticated before access is granted.

Authentication mechanisms shall be appropriate to the sensitivity of the information being protected.

Authentication controls shall be reviewed periodically.

4.14 Multi-Factor Authentication

MFA shall be mandatory for:

- AWS administrative access;
- production environments;
- VPN access;
- source code repositories;
- privileged accounts;
- cloud administration portals;
- email administration platforms.

The Information Security Officer may require MFA for additional systems.

4.15 Password Standards

Passwords shall:

- be sufficiently complex;
- be resistant to guessing attacks;
- not contain obvious personal information;
- not be reused across critical systems.

Passwords shall never be shared.

4.16 Password Storage

Passwords shall:

- never be stored in plain text;
- be protected through approved cryptographic methods;



- be managed securely.

The Company shall utilise password management solutions where appropriate.

4.17 Shared Accounts

Shared accounts are prohibited unless:

- technically unavoidable;
- formally approved;
- subject to enhanced monitoring.

The use of shared accounts shall be minimised.

4.18 Service Accounts

Service accounts shall:

- have a documented owner;
- have a documented purpose;
- be restricted to required permissions;
- be reviewed periodically.

Service account credentials shall be protected appropriately.

4.19 Privileged Access Management

Privileged access shall be tightly controlled.

Examples include:

- AWS root-level access;
- database administration;
- server administration;
- security administration.

Privileged access shall only be granted where necessary.

4.20 Administrative Accounts

Personnel requiring administrative access shall maintain separate:

Standard User Account

Used for normal business activities.



Administrative Account

Used only when performing administrative functions.

Administrative accounts shall not be used for routine activities such as email or web browsing.

4.21 Production Environment Access

Production access represents a high-risk permission.

Access shall:

- require documented approval;
- be restricted to authorised personnel;
- be reviewed regularly;
- be logged.

Production access shall not be granted solely for convenience.

4.22 AWS Administrative Controls

AWS administrative access shall be subject to enhanced controls.

Requirements include:

- MFA;
- unique accounts;
- logging;
- least privilege;
- periodic review.

Use of root accounts shall be minimised and restricted.

4.23 Emergency Access

Emergency access may be granted where required to:

- restore service;
- investigate incidents;
- mitigate critical risks.

Emergency access shall:

- be documented;
- be time limited where possible;



- be reviewed after use.

4.24 Dormant Accounts

Accounts that are no longer required shall be disabled.

Periodic reviews shall identify:

- inactive accounts;
- orphaned accounts;
- unnecessary accounts.

Identified accounts shall be investigated and removed where appropriate.

4.25 Access Reviews

Formal access reviews shall occur at least quarterly.

Reviews shall confirm:

- continued business need;
- appropriate access levels;
- removal of unnecessary permissions;
- segregation of duties compliance.

Results shall be documented.

4.26 Privileged Access Reviews

Privileged access reviews shall occur at least quarterly.

The review shall confirm:

- business justification;
- appropriateness of permissions;
- compliance with policy.

The Information Security Officer shall review the results.

4.27 Access Register

The Company shall maintain an Access Control Register.

The register shall contain:

- user name;



- role;
- systems accessed;
- access level;
- approval date;
- approver;
- review date.

The register shall be retained for audit purposes.

4.28 Authentication Logging

Authentication events shall be logged where technically feasible.

Examples include:

- successful logins;
- failed logins;
- password resets;
- MFA events;
- privileged access activity.

Logs shall be protected against unauthorised alteration.

4.29 Third-Party Access

Third-party access shall:

- be documented;
- be approved;
- be limited to legitimate business requirements;
- be reviewed periodically.

Supplier access shall be removed when no longer required.

4.30 Access Control Violations

Suspected access control violations shall be treated as security incidents.

Examples include:

- credential sharing;
- unauthorised access;



- attempted privilege escalation;
- misuse of administrative accounts.

Violations shall be investigated and escalated appropriately.

4.31 Compliance Monitoring

Compliance with access control requirements shall be assessed through:

- access reviews;
- audit activities;
- security monitoring;
- incident investigations.

Deficiencies shall be documented and remediated.

4.32 Management Reporting

The Information Security Officer shall periodically report on:

- privileged accounts;
- access review completion;
- dormant accounts;
- access control violations;
- authentication trends.

Material issues shall be escalated to management and the Board where appropriate.



SECTION 5

INFRASTRUCTURE, CLOUD AND NETWORK SECURITY

5.1 Purpose

The purpose of this section is to establish the technical security controls required to protect the Company's infrastructure, cloud environments, networks, gaming platforms and supporting systems.

The Company shall maintain secure infrastructure capable of protecting:

- player information;
- gaming transactions;
- payment information;
- authentication systems;
- regulatory records;
- operational systems.

Infrastructure security controls shall be designed to support confidentiality, integrity, availability and resilience objectives.

5.2 Security Architecture Principles

Infrastructure shall be designed in accordance with the following principles:

Defence in Depth

Multiple layers of security controls shall be implemented.

Least Privilege

Infrastructure access shall be restricted to authorised personnel.

Secure by Default

Systems shall be deployed using secure baseline configurations.

Segmentation

Critical systems shall be logically separated.

Resilience

Systems shall be capable of continuing operation during adverse events.

Monitoring

Security-relevant activities shall be monitored and logged.

5.3 Infrastructure Ownership



All infrastructure components shall have designated owners.

Responsibilities include:

- security oversight;
- configuration management;
- patch management;
- monitoring;
- lifecycle management.

Ownership shall be documented within the Asset Register.

5.4 Cloud Security Governance

The Company utilises cloud-hosted infrastructure and shall maintain governance controls appropriate to the risks associated with cloud computing.

Cloud governance shall include:

- account management;
 - access management;
 - logging;
 - encryption;
 - monitoring;
 - configuration management;
 - resilience controls.
-

5.5 AWS Governance

AWS environments shall be managed using documented security standards.

The Company shall maintain:

AWS Account Inventory

Documenting:

- production accounts;
- development accounts;
- testing accounts;
- management accounts.

AWS Ownership



Each AWS account shall have an assigned owner.

AWS Security Reviews

AWS configurations shall be reviewed periodically.

5.6 AWS Root Account Controls

AWS root accounts represent the highest level of privilege.

The Company shall:

- minimise use of root accounts;
- enable MFA;
- securely store credentials;
- monitor root account activity.

Root account use shall be restricted to exceptional circumstances.

5.7 Environment Separation

The Company shall maintain logical separation between:

Production

Live gaming operations.

User Acceptance Testing

Pre-production testing.

Development

Software development activities.

Disaster Recovery

Recovery environments.

Access rights shall reflect the differing sensitivity of each environment.

5.8 Production Environment Security

Production environments shall be subject to enhanced controls.

Requirements include:

- restricted access;
- MFA;
- enhanced logging;



- change management controls;
- monitoring.

Production environments shall not be used for development activities.

5.9 Network Architecture

The Company shall maintain documented network architecture diagrams.

Network documentation shall identify:

- critical systems;
- network boundaries;
- internet-facing systems;
- security controls;
- cloud connectivity.

Network diagrams shall be reviewed periodically.

5.10 Network Segmentation

Network segmentation shall be implemented where practical.

Segmentation objectives include:

- reducing attack surface;
- restricting lateral movement;
- protecting critical systems.

Examples include separation between:

- production systems;
 - development systems;
 - management systems;
 - security systems.
-

5.11 Firewall Management

Firewalls shall be deployed to restrict unauthorised traffic.

Firewall rules shall:

- be documented;
- be approved;



- be reviewed periodically.

Firewall configurations shall be based upon business requirements.

Unnecessary services shall be blocked.

5.12 Web Application Firewalls

Internet-facing applications shall be protected by Web Application Firewall ("WAF") technology where appropriate.

The WAF shall assist in detecting and blocking:

- malicious requests;
- common web attacks;
- automated abuse.

5.13 DDoS Protection

The Company shall implement measures designed to reduce the impact of denial-of-service attacks.

Measures may include:

- cloud-native protections;
- traffic filtering;
- rate limiting;
- upstream mitigation services.

DDoS resilience shall form part of business continuity planning.

5.14 Secure Configuration Standards

Systems shall be configured according to documented baseline standards.

Baseline standards shall address:

- unnecessary services;
- unnecessary ports;
- default accounts;
- default credentials;
- insecure protocols.

5.15 Configuration Reviews



System configurations shall be reviewed periodically.

Reviews shall identify:

- configuration drift;
- unauthorised changes;
- insecure settings.

Material findings shall be remediated.

5.16 Endpoint Security

The Company shall implement security controls for:

- laptops;
- desktops;
- mobile devices;
- administrative workstations.

Controls shall include:

- anti-malware;
- endpoint detection;
- encryption;
- patching.

5.17 Endpoint Detection and Response

Where implemented, EDR solutions shall support:

- threat detection;
- incident investigation;
- response activities.

Alerts shall be reviewed according to risk.

5.18 Anti-Malware Protection

Company-managed endpoints shall utilise anti-malware protection.

Protection shall:

- update regularly;
- perform scans;



- generate alerts.

Exceptions shall be documented.

5.19 Device Encryption

Portable devices containing Company information shall utilise full-disk encryption.

Encryption shall protect:

- player information;
- business information;
- authentication information.

Lost devices shall be reported immediately.

5.20 Remote Access Infrastructure

Remote access shall only occur through approved methods.

Remote access solutions shall:

- utilise encryption;
- require authentication;
- require MFA;
- generate logs.

5.21 Secure Administrative Workstations

Personnel performing administrative activities shall use appropriately secured devices.

Administrative devices shall receive enhanced protections.

Administrative activities should not be performed from unmanaged devices.

5.22 Vulnerability Scanning

Infrastructure shall undergo periodic vulnerability scanning.

Scanning shall cover:

- cloud infrastructure;
- servers;
- network devices;
- applications.



Findings shall be managed in accordance with the Vulnerability Management Procedure.

5.23 Encryption Standards

The Company shall utilise strong encryption standards for:

- data in transit;
- data at rest;
- backup media.

Encryption standards shall be reviewed periodically.

5.24 Data in Transit

Sensitive information transmitted across networks shall utilise encrypted communication channels.

Examples include:

- HTTPS;
- TLS;
- VPN technologies.

Unencrypted transmission of Restricted information is prohibited.

5.25 Data at Rest

Restricted information shall be encrypted at rest wherever technically feasible.

This includes:

- databases;
 - storage services;
 - backup repositories.
-

5.26 Cryptographic Key Management

Cryptographic keys shall be:

- protected;
- restricted;
- monitored.

Key management responsibilities shall be documented.

Compromised keys shall be rotated immediately.



5.27 Security Monitoring Architecture

The Company shall maintain monitoring capabilities capable of identifying:

- suspicious activity;
- authentication anomalies;
- system failures;
- security incidents.

Monitoring architecture shall support incident response activities.

5.28 Infrastructure Logging

Infrastructure components shall generate logs where technically feasible.

Examples include:

- authentication logs;
- firewall logs;
- cloud logs;
- administrative activity logs.

Logs shall be retained and protected.

5.29 Capacity Management

Infrastructure capacity shall be monitored.

Monitoring shall consider:

- utilisation;
- growth trends;
- resilience requirements.

Capacity issues shall be addressed before service degradation occurs.

5.30 Backup Infrastructure

Backup systems shall be protected using security controls equivalent to those protecting production systems.

Access to backups shall be restricted.

Backup repositories shall be monitored.



5.31 Infrastructure Resilience

Critical systems shall be designed to minimise single points of failure.

Resilience measures may include:

- redundancy;
- replication;
- failover mechanisms;
- backup systems.

The Information Security Officer shall periodically review resilience arrangements.

5.32 Third-Party Infrastructure

Where infrastructure services are provided by third parties, the Company shall:

- assess associated risks;
- review security controls;
- maintain contractual protections.

Critical suppliers shall be subject to enhanced oversight.

5.33 Compliance Monitoring

Infrastructure and cloud security controls shall be reviewed periodically through:

- vulnerability assessments;
- configuration reviews;
- audits;
- penetration testing.

Deficiencies shall be documented and remediated.

5.34 Management Reporting

The Information Security Officer shall periodically report on:

- infrastructure risks;
- cloud risks;
- vulnerability trends;
- resilience issues;



- major findings.

Material issues shall be escalated promptly.

5.35 Continuous Improvement

Infrastructure and cloud security controls shall be continuously improved based upon:

- incidents;
- threat intelligence;
- audits;
- penetration testing;
- regulatory developments.

Improvement actions shall be tracked through completion.



SECTION 6

SECURE DEVELOPMENT LIFECYCLE (SDLC)

6.1 Purpose

The purpose of this section is to establish the security requirements governing the design, development, testing, deployment and maintenance of software and technology solutions operated by Canary Alley B.V.

The Company recognises that secure software development is critical to:

- protecting player information;
- protecting gaming systems;
- maintaining platform integrity;
- preventing fraud;
- maintaining regulatory compliance;
- reducing operational risk.

Security shall be integrated throughout the entire software lifecycle rather than applied solely at the testing stage.

6.2 Scope

This section applies to:

- internally developed software;
- APIs;
- gaming integrations;
- web applications;
- mobile applications;
- infrastructure-as-code;
- automation scripts;
- CI/CD pipelines;
- third-party software modifications.

The requirements apply to:

- developers;
- testers;
- DevOps personnel;



- contractors;
- third-party development providers.

6.3 Secure Development Principles

Development activities shall be based upon the following principles.

Secure by Design

Security requirements shall be considered during design.

Least Privilege

Applications shall operate using the minimum permissions necessary.

Defence in Depth

Multiple security controls shall be implemented.

Separation of Environments

Development, testing and production shall remain separated.

Change Control

Changes shall follow documented approval procedures.

Accountability

All code changes shall be attributable to identifiable individuals.

6.4 Software Development Governance

The Company shall maintain governance over software development activities.

Governance shall include:

- development standards;
- code review procedures;
- release procedures;
- security testing requirements;
- vulnerability remediation requirements.

Development activities shall be subject to management oversight.

6.5 Security Requirements Definition

Security requirements shall be identified during project initiation.

Requirements may include:



- authentication controls;
- authorisation controls;
- encryption requirements;
- audit logging requirements;
- privacy requirements;
- regulatory requirements.

Security requirements shall be documented.

6.6 Security Design Reviews

Material projects shall undergo security review during design.

The review shall consider:

- architecture;
- attack surface;
- trust boundaries;
- authentication mechanisms;
- data flows;
- third-party dependencies.

Findings shall be documented.

6.7 Secure Coding Standards

Developers shall follow documented secure coding practices.

Development standards shall address:

- input validation;
- output encoding;
- authentication;
- authorisation;
- error handling;
- session management;
- cryptography.

Secure coding guidance shall be reviewed periodically.



6.8 Common Vulnerabilities

Developers shall take reasonable measures to prevent common vulnerabilities including:

- SQL injection;
- command injection;
- cross-site scripting;
- cross-site request forgery;
- authentication bypass;
- insecure direct object references;
- insecure deserialisation.

Training shall include awareness of common attack techniques.

6.9 Source Code Repositories

All source code shall be maintained within approved repositories.

Repositories shall:

- require authentication;
- require MFA;
- maintain audit trails;
- restrict access appropriately.

The Company shall maintain ownership of production source code.

6.10 GitHub Security Controls

Where GitHub is utilised:

- MFA shall be mandatory;
- branch protection shall be enabled;
- privileged access shall be restricted;
- repository ownership shall be documented.

Administrative permissions shall be limited.

6.11 Branch Protection

Protected branches shall be utilised for production releases.

Controls shall include:



- restricted direct commits;
- pull request requirements;
- review requirements;
- status checks.

Exceptions shall be documented.

6.12 Pull Request Controls

Code changes shall normally be submitted through pull requests.

Pull requests shall:

- identify the change;
- identify the author;
- include testing evidence;
- include reviewer approval.

Approvals shall be retained within repository history.

6.13 Code Review Requirements

Security-sensitive changes shall undergo peer review.

Reviewers shall consider:

- coding quality;
- security implications;
- compliance with standards;
- testing completeness.

The reviewer should not normally be the original author.

6.14 Segregation of Duties

Where practical:

- development;
- testing;
- deployment;
- production approval

shall be performed by different individuals.



Conflicts shall be documented and approved.

6.15 Secrets Management

Credentials shall not be hardcoded into source code.

Examples include:

- passwords;
- API keys;
- tokens;
- cryptographic keys.

Approved secrets management solutions shall be utilised.

6.16 Dependency Management

Open-source and third-party components shall be managed appropriately.

The Company shall:

- maintain visibility of dependencies;
- monitor security advisories;
- remove unsupported components.

Dependencies shall be reviewed periodically.

6.17 Software Composition Analysis

Where available, automated tools shall be utilised to identify:

- vulnerable libraries;
- outdated dependencies;
- licensing concerns.

Material findings shall be remediated.

6.18 Development Environment Security

Development environments shall be secured appropriately.

Requirements include:

- authenticated access;
- least privilege;



- logging;
- endpoint protection.

Development environments shall not expose production information unnecessarily.

6.19 Test Environment Security

Test environments shall be separated from production.

Test environments shall not be publicly accessible unless required.

Security controls shall be proportionate to risk.

6.20 Production Data Usage

Production data shall not be used within development environments unless:

- a legitimate requirement exists;
- appropriate controls are implemented;
- approval is obtained.

Where possible, test data shall be anonymised or synthetic.

6.21 Security Testing

Applications shall undergo security testing before production deployment.

Testing may include:

- vulnerability scanning;
- manual review;
- dynamic testing;
- static analysis.

Results shall be documented.

6.22 Static Application Security Testing

Where available, SAST solutions shall be utilised to identify security weaknesses within source code.

Findings shall be reviewed and addressed according to risk.

6.23 Dynamic Application Security Testing

DAST solutions may be utilised to assess running applications.



Testing shall focus upon:

- authentication;
- authorisation;
- session management;
- input validation.

6.24 Manual Security Testing

Automated testing shall not replace manual review.

Security-sensitive systems shall receive manual assessment where appropriate.

6.25 Release Management

All production releases shall follow a documented release process.

The process shall include:

- approval;
- testing;
- rollback planning;
- deployment verification.

Release records shall be retained.

6.26 Production Deployment Controls

Production deployments shall:

- be authorised;
- be logged;
- be traceable.

Emergency deployments shall be reviewed retrospectively.

6.27 Change Traceability

The Company shall maintain traceability between:

- requirements;
- code changes;
- testing;



- deployment.

Evidence shall be retained for audit purposes.

6.28 CI/CD Security

Continuous Integration and Continuous Deployment pipelines shall be protected.

Controls shall include:

- MFA;
- access restrictions;
- secrets protection;
- audit logging.

CI/CD permissions shall be reviewed periodically.

6.29 Infrastructure as Code

Infrastructure-as-Code configurations shall be treated as production code.

Requirements include:

- version control;
- review;
- testing;
- approval.

Infrastructure changes shall remain auditable.

6.30 Vulnerability Disclosure

The Company shall maintain procedures for receiving reports of security vulnerabilities.

Reports may originate from:

- employees;
- suppliers;
- security researchers;
- regulators.

Reported vulnerabilities shall be assessed and tracked.

6.31 Remediation of Security Defects



Security defects identified during development shall be prioritised according to risk.

Critical vulnerabilities shall receive immediate attention.

Remediation activities shall be documented.

6.32 Developer Security Training

Developers shall receive periodic training covering:

- secure coding;
- common vulnerabilities;
- secure design;
- dependency management.

Training records shall be retained.

6.33 Audit and Compliance

Compliance with SDLC requirements shall be assessed through:

- audits;
- code reviews;
- security testing;
- release reviews.

Deficiencies shall be documented and remediated.

6.34 Management Reporting

The Information Security Officer shall receive periodic reporting regarding:

- release activity;
- security testing results;
- vulnerability trends;
- code review compliance;
- dependency risks.

Material issues shall be escalated.

6.35 Continuous Improvement

The SDLC shall be reviewed periodically to identify opportunities for improvement.



Inputs may include:

- incidents;
- vulnerabilities;
- audit findings;
- penetration testing;
- regulatory developments.

Improvement actions shall be tracked to completion.



SECTION 7

VULNERABILITY MANAGEMENT AND PATCH MANAGEMENT

7.1 Purpose

The purpose of this section is to establish the framework through which Canary Alley B.V. identifies, assesses, prioritises, remediates and monitors security vulnerabilities affecting its information systems, infrastructure, applications and third-party services.

The Company recognises that vulnerabilities represent one of the primary causes of cybersecurity incidents and therefore requires a proactive and risk-based vulnerability management programme.

The objective of the programme is to:

- identify vulnerabilities before they are exploited;
 - reduce the Company's attack surface;
 - support regulatory compliance;
 - minimise operational disruption;
 - protect player information and gaming systems.
-

7.2 Scope

The Vulnerability Management Programme applies to:

Infrastructure

- AWS environments;
- virtual servers;
- containers;
- databases;
- storage systems.

Applications

- gaming platforms;
- websites;
- APIs;
- internal applications.

Endpoints

- laptops;
- desktops;



- administrative workstations.

Network Devices

- firewalls;
- switches;
- routers;
- VPN infrastructure.

Third-Party Components

- open-source libraries;
- software dependencies;
- externally hosted services.

7.3 Vulnerability Management Governance

The Information Security Officer shall be responsible for overseeing the Vulnerability Management Programme.

Responsibilities include:

- maintaining vulnerability procedures;
- reviewing vulnerability reports;
- monitoring remediation activities;
- reporting significant vulnerabilities;
- maintaining the Vulnerability Register.

System owners shall remain responsible for remediation within their environments.

7.4 Vulnerability Sources

Vulnerabilities may be identified through:

Vulnerability Scanning

Automated scanning tools.

Penetration Testing

Internal and external testing.

Threat Intelligence

Security advisories and intelligence feeds.

Vendor Notifications



Supplier security bulletins.

Internal Reviews

Configuration assessments and audits.

Security Researchers

Responsible disclosure reports.

Security Incidents

Findings identified during investigations.

7.5 Vulnerability Scanning Programme

The Company shall maintain a vulnerability scanning programme.

Scanning shall be performed against:

- production environments;
- internet-facing systems;
- internal infrastructure;
- cloud services;
- applications.

Scanning frequency shall be risk-based and proportionate to the criticality of the systems involved.

7.6 Authenticated Scanning

Where practical, vulnerability scans shall utilise authenticated credentials.

Authenticated scans provide improved visibility into:

- missing patches;
 - configuration weaknesses;
 - software versions;
 - insecure settings.
-

7.7 External Vulnerability Scanning

Internet-facing systems shall be assessed periodically for vulnerabilities.

Examples include:

- websites;
- APIs;



- VPN gateways;
- cloud-hosted services.

Critical findings shall be prioritised for remediation.

7.8 Internal Vulnerability Scanning

Internal infrastructure shall undergo periodic scanning.

The scope may include:

- servers;
- databases;
- network devices;
- administrative systems.

Results shall be reviewed and documented.

7.9 Cloud Vulnerability Assessment

Cloud-hosted infrastructure shall be reviewed for:

- exposed services;
- insecure configurations;
- excessive permissions;
- unsupported software.

Cloud vulnerability assessments shall complement traditional scanning activities.

7.10 Application Vulnerability Assessments

Applications shall be assessed for security weaknesses.

Testing may include:

- automated scanning;
- manual review;
- penetration testing;
- code analysis.

Application findings shall be managed through the Vulnerability Register.

7.11 Vulnerability Classification



All vulnerabilities shall be classified according to severity.

The Company shall utilise a documented classification methodology.

Severity assessments shall consider:

- exploitability;
 - business impact;
 - exposure;
 - affected assets;
 - regulatory implications.
-

7.12 Critical Vulnerabilities

Critical vulnerabilities are those capable of causing:

- system compromise;
- unauthorised access;
- significant data exposure;
- major service disruption.

Critical vulnerabilities require immediate attention.

7.13 High-Risk Vulnerabilities

High-risk vulnerabilities represent significant security risks and require prioritised remediation.

Examples include:

- authentication bypass;
 - privilege escalation;
 - remote code execution.
-

7.14 Medium-Risk Vulnerabilities

Medium-risk vulnerabilities present meaningful but less urgent risks.

Remediation shall occur within planned maintenance cycles.

7.15 Low-Risk Vulnerabilities

Low-risk vulnerabilities may be addressed through:

- routine maintenance;



- compensating controls;
- future releases.

Acceptance shall be documented where appropriate.

7.16 Vulnerability Remediation Targets

The Company shall maintain remediation targets.

Severity Target

Critical Immediate remediation or mitigation

High Priority remediation

Medium Planned remediation

Low Risk-based remediation

The Information Security Officer may accelerate remediation where circumstances warrant.

7.17 Compensating Controls

Where immediate remediation is not possible, compensating controls may be implemented.

Examples include:

- firewall restrictions;
- access restrictions;
- monitoring enhancements;
- service isolation.

Compensating controls shall be documented.

7.18 Vulnerability Exceptions

A vulnerability may only remain unresolved where:

- remediation is technically impractical;
- compensating controls exist;
- risk acceptance has been approved.

All exceptions shall be documented.

7.19 Vulnerability Register



The Company shall maintain a Vulnerability Register.

The register shall contain:

- Vulnerability ID;
- Discovery Date;
- Description;
- Affected Assets;
- Severity;
- Owner;
- Remediation Plan;
- Target Date;
- Status;
- Closure Date.

The register shall be reviewed regularly.

7.20 Vulnerability Reporting

The Information Security Officer shall provide periodic reporting covering:

- outstanding vulnerabilities;
- overdue remediation;
- vulnerability trends;
- recurring weaknesses.

Critical findings shall be escalated immediately.

PATCH MANAGEMENT

7.21 Patch Management Objectives

The Company shall maintain a Patch Management Programme designed to:

- reduce exposure to known vulnerabilities;
- maintain system stability;
- support regulatory compliance.

Patch management shall apply to all supported systems.



7.22 Patch Sources

Patches may originate from:

- operating system vendors;
- application vendors;
- cloud service providers;
- hardware manufacturers.

Patch sources shall be verified before implementation.

7.23 Patch Assessment

New patches shall be assessed to determine:

- security relevance;
- operational impact;
- affected systems;
- deployment urgency.

Assessments shall be documented where appropriate.

7.24 Patch Testing

Patches shall be tested before deployment where practical.

Testing shall evaluate:

- compatibility;
- stability;
- functionality.

Emergency circumstances may require accelerated deployment.

7.25 Production Patch Deployment

Production deployments shall follow change management procedures.

Patch deployments shall:

- be approved;
- be documented;
- be verifiable.

Deployment records shall be retained.



7.26 Emergency Patching

Emergency patching may occur where:

- critical vulnerabilities exist;
- active exploitation is occurring;
- regulatory obligations require urgent action.

Emergency changes shall undergo retrospective review.

7.27 Unsupported Software

Unsupported software presents elevated security risk.

The Company shall:

- identify unsupported software;
- maintain inventories;
- remove unsupported software where feasible.

Exceptions require documented approval.

7.28 End-of-Life Systems

End-of-life systems shall be subject to enhanced review.

The Company shall seek to:

- replace;
- upgrade;
- retire

such systems where practicable.

7.29 Zero-Day Vulnerabilities

The Company shall maintain procedures for responding to zero-day vulnerabilities.

Response activities may include:

- emergency risk assessment;
- compensating controls;
- monitoring enhancements;
- emergency patching.



Material zero-day risks shall be escalated immediately.

7.30 Threat Intelligence

The Company shall monitor relevant threat intelligence sources.

Threat intelligence may inform:

- vulnerability prioritisation;
- incident response;
- security monitoring.

Relevant intelligence shall be reviewed by the Information Security Officer.

7.31 Recurring Vulnerability Analysis

The Company shall periodically review vulnerability trends.

Reviews shall identify:

- recurring weaknesses;
- systemic issues;
- process failures.

Corrective actions shall be documented.

7.32 Audit and Assurance

The Vulnerability Management Programme shall be reviewed through:

- internal audits;
- penetration testing;
- management reviews;
- compliance assessments.

Deficiencies shall be remediated.

7.33 Management Reporting

The Information Security Officer shall report on:

- vulnerability volumes;
- critical vulnerabilities;
- overdue remediation;



- patch compliance;
- vulnerability trends.

Reports shall be provided to management periodically.

7.34 Continuous Improvement

The Vulnerability Management and Patch Management Programmes shall be continually improved through:

- incident reviews;
- audits;
- threat intelligence;
- regulatory developments;
- penetration testing findings.

Improvement activities shall be documented and tracked.

SECTION 8

LOGGING, MONITORING AND INCIDENT RESPONSE

8.1 Purpose

The purpose of this section is to establish the framework through which Canary Alley B.V. detects, investigates, responds to and recovers from information security events and incidents.

The Company recognises that prevention alone cannot eliminate all security risks. Accordingly, the Company shall maintain monitoring, logging and incident response capabilities designed to:

- detect security events;
- identify suspicious activity;
- investigate incidents;
- minimise operational impact;
- protect players;
- support regulatory obligations;
- facilitate timely recovery.

8.2 Incident Response Objectives

The Company's incident response capability shall seek to:

Detect



Identify security events promptly.

Contain

Limit damage and prevent escalation.

Investigate

Determine root cause and impact.

Recover

Restore normal operations safely.

Learn

Implement improvements to prevent recurrence.

8.3 Security Event vs Security Incident

The Company distinguishes between security events and security incidents.

Security Event

A security-relevant occurrence that may require investigation.

Examples include:

- failed logins;
- malware alerts;
- firewall alerts;
- unusual traffic;
- account lockouts.

Security Incident

An event that compromises or threatens:

- confidentiality;
- integrity;
- availability;
- regulatory compliance.

Examples include:

- unauthorised access;
- malware infection;
- credential compromise;



- ransomware attack;
- data breach;
- denial-of-service attack.

LOGGING FRAMEWORK

8.4 Logging Requirements

The Company shall maintain logging sufficient to:

- support investigations;
- support regulatory compliance;
- identify suspicious activity;
- reconstruct events;
- support forensic analysis.

Logging shall be enabled wherever technically feasible.

8.5 Systems Subject to Logging

Logging shall include:

Infrastructure

- AWS services;
- servers;
- network devices;
- firewalls.

Applications

- gaming platforms;
- web applications;
- APIs.

Authentication Systems

- login systems;
- MFA systems;
- identity providers.

Administrative Systems



- cloud administration;
 - database administration;
 - security administration.
-

8.6 Authentication Logging

Authentication logs shall record:

- successful logins;
- failed logins;
- password resets;
- MFA activity;
- account lockouts.

Authentication anomalies shall be reviewed.

8.7 Administrative Activity Logging

Administrative activities shall be logged.

Examples include:

- account creation;
- account deletion;
- permission changes;
- configuration changes;
- security control modifications.

Administrative activity shall be attributable to individual users.

8.8 Application Logging

Applications shall generate logs sufficient to support:

- troubleshooting;
- investigations;
- fraud detection;
- security monitoring.

Logging shall be proportionate to risk.



8.9 Database Logging

Where supported, databases shall log:

- administrative activity;
- access attempts;
- configuration changes;
- privileged actions.

Database logging shall support incident investigations.

8.10 AWS CloudTrail Requirements

AWS CloudTrail shall be enabled for production AWS environments.

Logging shall include:

- API activity;
- administrative activity;
- configuration changes;
- access events.

CloudTrail logs shall be protected against unauthorised modification.

8.11 AWS Security Logging

Where available, AWS security services may be utilised, including:

- CloudTrail;
- GuardDuty;
- Security Hub;
- CloudWatch.

Security events shall be reviewed according to risk.

8.12 Firewall Logging

Firewall logging shall be enabled where practical.

Logs may include:

- blocked connections;
- denied traffic;
- configuration changes;



- suspicious activity.

Firewall logs shall support security investigations.

8.13 Log Protection

Logs shall be protected against:

- deletion;
- modification;
- unauthorised access.

Log integrity is critical to incident investigation.

8.14 Log Retention

Security logs shall be retained for a period consistent with:

- regulatory requirements;
- operational requirements;
- investigative requirements.

Log retention periods shall be documented.

SECURITY MONITORING

8.15 Security Monitoring Programme

The Company shall maintain a security monitoring capability designed to identify:

- suspicious activity;
- unauthorised access;
- security incidents;
- operational anomalies.

Monitoring shall be risk-based.

8.16 Security Alerts

Monitoring systems shall generate alerts for events including:

- repeated failed logins;
- administrative activity;



- privilege escalation;
- unusual geographic access;
- malware detections.

Alerts shall be reviewed appropriately.

8.17 Alert Prioritisation

Alerts shall be categorised according to severity.

Critical

Immediate response required.

High

Priority investigation required.

Medium

Investigation required.

Low

Monitoring and review.

8.18 Monitoring Responsibilities

The Information Security Officer shall oversee monitoring activities.

Operational review may be performed by:

- IT personnel;
- managed service providers;
- security service providers.

Responsibilities shall be documented.

INCIDENT RESPONSE FRAMEWORK

8.19 Incident Response Team

The Company shall maintain an Incident Response Team.

Depending on the nature of the incident, the team may include:

- Information Security Officer;
- Compliance Officer;



- Technical personnel;
- Senior Management;
- External specialists.

Roles and responsibilities shall be defined.

8.20 Incident Classification

Security incidents shall be classified according to severity.

Critical

Examples:

- compromise of player data;
 - ransomware;
 - widespread service disruption;
 - compromise of production infrastructure.
-

High

Examples:

- privilege escalation;
 - malware affecting critical systems;
 - unauthorised administrative access.
-

Medium

Examples:

- isolated malware incidents;
 - limited account compromise.
-

Low

Examples:

- policy violations;
 - minor procedural breaches.
-

8.21 Incident Identification



Security incidents may be identified through:

- monitoring systems;
- employee reports;
- supplier notifications;
- player reports;
- regulators;
- threat intelligence.

All personnel shall report suspected incidents immediately.

8.22 Incident Reporting

Personnel shall report incidents immediately to:

- Information Security Officer;
- Compliance Officer;
- designated reporting channels.

Delays in reporting may increase risk.

8.23 Incident Response Process

The Company shall utilise the following incident response lifecycle:

Identification

Determine whether an incident exists.

Containment

Limit further impact.

Investigation

Determine cause and scope.

Eradication

Remove the threat.

Recovery

Restore normal operations.

Lessons Learned

Implement improvements.



8.24 Containment Procedures

Containment actions may include:

- account suspension;
- system isolation;
- network blocking;
- credential resets.

Containment decisions shall consider operational impact.

8.25 Investigation Procedures

Investigations shall seek to determine:

- what occurred;
- when it occurred;
- how it occurred;
- who was affected;
- what systems were affected.

Investigations shall be documented.

8.26 Forensic Preservation

Where appropriate, evidence shall be preserved.

Evidence may include:

- logs;
- screenshots;
- memory captures;
- system images.

Evidence shall be protected from alteration.

8.27 External Specialists

The Company may engage external specialists where necessary.

Examples include:

- forensic investigators;
- cybersecurity consultants;



- legal advisers.

Engagement decisions shall be documented.

8.28 Recovery Procedures

Recovery activities shall:

- restore services safely;
- validate system integrity;
- verify security controls.

Recovery shall not occur until containment is sufficient.

8.29 Data Breach Response

Incidents involving unauthorised disclosure of information shall receive enhanced review.

The Company shall assess:

- affected individuals;
 - affected data;
 - regulatory obligations;
 - notification requirements.
-

8.30 Regulatory Notification

The Information Security Officer shall determine whether notification is required to:

- Curaçao Gaming Authority;
- competent authorities;
- law enforcement;
- affected parties.

Notification decisions shall be documented.

8.31 Communication Management

External communications regarding incidents shall be controlled.

Only authorised personnel may communicate externally regarding incidents.

Unauthorised disclosure of incident information is prohibited.



8.32 Incident Register

The Company shall maintain a Security Incident Register.

The register shall include:

- Incident ID;
- Date;
- Severity;
- Description;
- Systems Affected;
- Root Cause;
- Actions Taken;
- Closure Date.

The register shall be reviewed periodically.

8.33 Post-Incident Review

All material incidents shall undergo post-incident review.

The review shall identify:

- root causes;
- control failures;
- lessons learned;
- improvement opportunities.

Reviews shall be documented.

8.34 Root Cause Analysis

Material incidents shall include formal root cause analysis.

Analysis shall seek to identify:

- technical failures;
- process failures;
- human factors;
- supplier failures.

Corrective actions shall be assigned.



8.35 Incident Metrics

The Company shall monitor:

- incident volumes;
- incident severity;
- response times;
- recovery times;
- recurring causes.

Metrics shall support continuous improvement.

8.36 Incident Reporting to Management

Management shall receive periodic reporting regarding:

- significant incidents;
- trends;
- unresolved issues;
- remediation activities.

Critical incidents shall be escalated immediately.

8.37 Testing of Incident Response Capability

Incident response capabilities shall be tested periodically.

Testing may include:

- tabletop exercises;
- simulation exercises;
- disaster scenarios;
- cyber-attack scenarios.

Results shall be documented.

8.38 Continuous Improvement

The logging, monitoring and incident response framework shall be reviewed periodically.

Improvements shall be driven by:

- incidents;
- audits;



- penetration testing;
- regulatory developments;
- threat intelligence.

Actions shall be documented and tracked.



SECTION 9

THIRD-PARTY SECURITY AND SUPPLIER RISK MANAGEMENT

9.1 Purpose

The purpose of this section is to establish the framework through which Canary Alley B.V. identifies, assesses, manages and monitors information security risks arising from third-party relationships.

The Company recognises that third-party providers form a critical component of its operating model and may have access to:

- player information;
- financial information;
- gaming systems;
- cloud infrastructure;
- operational processes;
- regulatory records.

Third-party risks shall therefore be managed throughout the entire supplier lifecycle.

9.2 Scope

This section applies to all suppliers, service providers and outsourced service arrangements, including:

Technology Providers

- hosting providers;
- cloud providers;
- software vendors;
- infrastructure providers.

Gaming Suppliers

- platform providers;
- sportsbook providers;
- game providers;
- trading providers;
- odds providers.

Compliance Providers

- KYC providers;
- AML providers;



- sanctions screening providers.

Payment Providers

- payment gateways;
- PSPs;
- banking partners.

Professional Service Providers

- auditors;
- consultants;
- managed service providers;
- legal advisers.

9.3 Supplier Risk Management Principles

The Company shall apply the following principles:

Risk-Based Oversight

Supplier oversight shall be proportionate to risk.

Due Diligence

Appropriate due diligence shall be conducted before engagement.

Contractual Protection

Security obligations shall be documented contractually.

Ongoing Monitoring

Suppliers shall be reviewed throughout the relationship.

Accountability

Each supplier shall have an identified business owner.

9.4 Supplier Lifecycle Management

Supplier management shall cover:

Selection

Due diligence and risk assessment.

Contracting

Security obligations and requirements.

Monitoring



Ongoing review and oversight.

Renewal

Periodic reassessment.

Exit

Secure termination and information recovery.

9.5 Supplier Risk Classification

Suppliers shall be classified according to risk.

Tier 1 – Critical Suppliers

Suppliers whose failure could materially impact:

- gaming operations;
- player funds;
- player information;
- regulatory compliance.

Examples:

- AWS;
- core gaming platform providers;
- payment processors.

Tier 2 – High-Risk Suppliers

Suppliers with access to:

- Confidential information;
- Restricted information;
- production systems.

Examples:

- KYC providers;
- fraud monitoring providers;
- managed service providers.

Tier 3 – Standard Suppliers



Suppliers with limited access and limited operational impact.

Examples:

- office software vendors;
- marketing providers.

9.6 Supplier Inventory

The Company shall maintain a Supplier Register.

The register shall include:

- supplier name;
- service provided;
- risk classification;
- contract owner;
- contract date;
- review date;
- security assessment date.

The register shall be reviewed periodically.

9.7 Pre-Engagement Due Diligence

Prior to onboarding material suppliers, the Company shall conduct appropriate due diligence.

Due diligence shall be proportionate to risk.

9.8 Security Due Diligence Areas

Assessments may consider:

Corporate Information

- legal entity details;
- ownership;
- regulatory status.

Security Governance

- security programme;
- policies;
- certifications.



Operational Security

- access controls;
- vulnerability management;
- incident management.

Resilience

- business continuity;
- disaster recovery.

Data Protection

- data handling practices;
 - privacy controls.
-

9.9 Information Security Questionnaires

The Company may require suppliers to complete security questionnaires.

Questionnaires may cover:

- governance;
- infrastructure security;
- application security;
- monitoring;
- incident management.

Responses shall be reviewed and retained.

9.10 Security Certifications

Where available, the Company may consider certifications including:

- ISO 27001;
- SOC 2;
- PCI DSS;
- equivalent security frameworks.

Certifications shall not replace due diligence.

9.11 Supplier Risk Assessments

Material suppliers shall undergo documented risk assessment.



Assessments shall consider:

- data access;
- system access;
- operational dependency;
- regulatory impact;
- geographic risk.

Results shall be documented.

9.12 Contractual Security Requirements

Contracts shall contain security obligations appropriate to risk.

Requirements may include:

- confidentiality obligations;
 - access restrictions;
 - security controls;
 - incident notification obligations;
 - audit rights.
-

9.13 Confidentiality Agreements

Personnel and suppliers with access to Company information shall be subject to confidentiality obligations.

Confidentiality provisions shall survive termination where appropriate.

9.14 Data Protection Obligations

Where suppliers process Company information, contractual provisions shall address:

- authorised use;
 - information protection;
 - retention;
 - deletion;
 - incident reporting.
-

9.15 Security Incident Notification Requirements



Material suppliers shall be required to notify the Company promptly regarding incidents affecting:

- Company information;
- Company systems;
- operational services.

Notification requirements shall be documented contractually.

9.16 Right to Audit

Where appropriate, contracts shall provide the Company with audit rights.

Audit rights may include:

- documentation reviews;
- security assessments;
- certification reviews.

Use of audit rights shall be risk-based.

9.17 Subcontractor Controls

Suppliers shall remain responsible for subcontractors utilised in delivering services.

Material subcontracting arrangements shall be disclosed where appropriate.

The Company may require equivalent security standards to apply to subcontractors.

9.18 AWS Supplier Oversight

AWS represents a critical supplier.

The Company shall:

- review AWS security documentation;
 - understand shared responsibility obligations;
 - monitor AWS service advisories;
 - maintain AWS governance controls.
-

9.19 Payment Provider Security

Payment providers shall be subject to enhanced review.

Assessment areas include:

- regulatory status;



- fraud controls;
- resilience;
- incident management.

Critical findings shall be escalated.

9.20 KYC and AML Provider Security

Providers processing player identity information shall be subject to enhanced oversight.

Assessments shall consider:

- information security controls;
 - privacy controls;
 - operational resilience.
-

9.21 Gaming Supplier Security

Gaming suppliers providing:

- sportsbook services;
- gaming content;
- gaming platforms;
- odds services

shall be subject to security assessment proportionate to risk.

9.22 Supplier Access Controls

Supplier access to Company systems shall:

- be approved;
- be documented;
- be restricted;
- be reviewed periodically.

Supplier access shall be removed when no longer required.

9.23 Ongoing Supplier Monitoring

Material suppliers shall undergo periodic review.

Reviews may consider:



- incidents;
 - service performance;
 - certifications;
 - audit reports;
 - regulatory developments.
-

9.24 Annual Supplier Reviews

Tier 1 and Tier 2 suppliers shall undergo annual review.

Reviews shall assess:

- continued suitability;
- risk exposure;
- control effectiveness.

Results shall be documented.

9.25 Supplier Security Incidents

Supplier-related incidents shall be recorded within the Security Incident Register.

Investigations shall consider:

- supplier controls;
 - contractual obligations;
 - remediation requirements.
-

9.26 Supplier Termination

Supplier termination shall be managed through documented procedures.

The Company shall ensure:

- access removal;
 - return of information;
 - secure destruction of information;
 - contract closure.
-

9.27 Information Return and Destruction

Upon termination, suppliers shall return or securely destroy Company information as required.



Evidence may be requested where appropriate.

9.28 Supplier Exit Reviews

The Company shall assess whether termination activities have been completed.

Reviews may include:

- access verification;
 - information verification;
 - contract verification.
-

9.29 Supplier Risk Reporting

The Information Security Officer shall periodically report on:

- supplier risks;
- supplier incidents;
- supplier assessments;
- overdue reviews.

Material risks shall be escalated.

9.30 Audit and Assurance

Supplier security controls shall be assessed through:

- due diligence;
- audits;
- certifications;
- management reviews.

Deficiencies shall be documented and remediated.

9.31 Continuous Improvement

The Third-Party Risk Management Programme shall be reviewed periodically.

Improvements shall be driven by:

- incidents;
- audits;
- regulatory developments;



- emerging threats.

Actions shall be documented and tracked.



SECTION 10

BUSINESS CONTINUITY MANAGEMENT, DISASTER RECOVERY AND BACKUP MANAGEMENT

10.1 Purpose

The purpose of this section is to establish the framework through which Canary Alley B.V. maintains operational resilience and ensures the continued delivery of critical services during disruptive events.

The Company recognises that interruptions to gaming services may adversely impact:

- players;
- player funds;
- regulatory compliance;
- operational stability;
- commercial operations;
- reputation.

The Company shall therefore maintain documented Business Continuity and Disaster Recovery arrangements designed to minimise disruption and support recovery objectives.

10.2 Business Continuity Objectives

The Company's Business Continuity Management ("BCM") programme shall seek to:

Protect Players

Maintain critical player-facing services wherever possible.

Protect Player Funds

Ensure player balances remain secure and recoverable.

Maintain Regulatory Compliance

Support continued compliance during disruptive events.

Minimise Downtime

Restore critical services within defined recovery objectives.

Protect Information Assets

Prevent loss, corruption or unauthorised disclosure of information.

Support Organisational Resilience

Enable continued operation during adverse circumstances.

10.3 Business Continuity Governance



The Board shall maintain oversight of Business Continuity arrangements.

The Information Security Officer shall coordinate:

- continuity planning;
- testing;
- reviews;
- reporting.

Department managers shall maintain continuity arrangements relevant to their operational areas.

10.4 Business Continuity Management Framework

The BCM framework shall include:

- Business Impact Analysis;
- Recovery Strategies;
- Business Continuity Plans;
- Disaster Recovery Plans;
- Testing Programmes;
- Crisis Management Procedures;
- Supplier Continuity Reviews.

The framework shall be reviewed periodically.

10.5 Business Impact Analysis

The Company shall maintain a documented Business Impact Analysis ("BIA").

The BIA shall identify:

- critical services;
- critical systems;
- critical suppliers;
- recovery priorities;
- acceptable downtime;
- recovery dependencies.

The BIA shall be reviewed at least annually.

10.6 Critical Business Functions



The following functions shall normally be considered critical:

Gaming Operations

Operation of player-facing gaming services.

Payment Processing

Deposits and withdrawals.

Customer Support

Support for players and regulatory obligations.

AML Operations

Customer due diligence and transaction monitoring.

Responsible Gaming Operations

Player protection activities.

Information Security

Monitoring and incident response activities.

The Company may identify additional critical functions.

10.7 Recovery Time Objectives (RTO)

Recovery Time Objectives shall be established for critical services.

RTOs represent the maximum acceptable downtime before recovery.

Examples may include:

Service	Example RTO
Gaming Platform	4 Hours
Payments	8 Hours
Customer Support	24 Hours
Corporate Systems	48 Hours

Actual targets shall be determined through the BIA.

10.8 Recovery Point Objectives (RPO)

Recovery Point Objectives shall define acceptable data loss.

RPOs shall consider:

- player transactions;



- player balances;
- financial information;
- regulatory records.

The Company shall seek to minimise data loss wherever practical.

10.9 Continuity Strategies

The Company shall identify strategies capable of supporting continuity objectives.

Strategies may include:

- cloud redundancy;
- infrastructure redundancy;
- alternative suppliers;
- remote working capability;
- backup communications.

10.10 Continuity Plan Documentation

Business Continuity Plans shall include:

- incident escalation procedures;
- recovery priorities;
- key contacts;
- communication plans;
- recovery activities.

Plans shall be maintained and reviewed periodically.

DISASTER RECOVERY

10.11 Disaster Recovery Objectives

Disaster Recovery ("DR") arrangements shall support recovery of critical technology services.

Objectives include:

- restoration of systems;
- restoration of information;
- restoration of connectivity;



- restoration of gaming services.

10.12 Disaster Recovery Scope

The DR programme shall cover:

- AWS infrastructure;
- databases;
- applications;
- network services;
- authentication services;
- security monitoring systems.

10.13 Disaster Recovery Plan

The Company shall maintain a Disaster Recovery Plan.

The plan shall include:

- activation criteria;
- responsibilities;
- recovery procedures;
- escalation procedures;
- testing requirements.

10.14 Disaster Recovery Team

The Company shall identify personnel responsible for recovery activities.

Responsibilities may include:

- technical recovery;
- communications;
- supplier coordination;
- management oversight.

Roles shall be documented.

10.15 Recovery Prioritisation

Recovery activities shall be prioritised according to business criticality.



Priority shall normally be given to:

1. Player balances;
2. Gaming operations;
3. Security monitoring;
4. Payment processing;
5. Regulatory systems.

10.16 AWS Recovery Controls

AWS-hosted environments shall incorporate resilience features where appropriate.

Examples include:

- multi-availability-zone deployment;
- snapshots;
- replication;
- infrastructure-as-code recovery.

Recovery arrangements shall be reviewed periodically.

10.17 Recovery Verification

Following recovery, the Company shall verify:

- system integrity;
- application functionality;
- information integrity;
- security controls.

Verification activities shall be documented.

BACKUP MANAGEMENT

10.18 Backup Objectives

The Company shall maintain backups sufficient to support recovery objectives.

Backups shall support:

- operational recovery;
- disaster recovery;



- incident response;
- regulatory requirements.

10.19 Backup Scope

Backups shall include:

Databases

Player and operational databases.

Application Configurations

System settings and deployment configurations.

Security Configurations

Firewall and security settings.

Regulatory Records

AML, RG and compliance records.

Corporate Information

Critical business records.

10.20 Backup Frequency

Backup frequency shall be determined according to business requirements and recovery objectives.

The Company shall document backup schedules.

10.21 Backup Security

Backups shall be protected against:

- unauthorised access;
- deletion;
- modification;
- corruption.

Access shall be restricted to authorised personnel.

10.22 Backup Encryption

Sensitive backup data shall be encrypted.

Encryption requirements shall align with the Information Security Policy.



10.23 Backup Monitoring

Backup jobs shall be monitored.

Monitoring shall identify:

- failures;
- corruption;
- missed backups.

Backup failures shall be investigated promptly.

10.24 Backup Retention

Backup retention periods shall be documented.

Retention requirements shall consider:

- operational needs;
 - legal obligations;
 - regulatory obligations.
-

10.25 Backup Restoration Testing

The Company shall perform periodic restoration testing.

Testing shall verify:

- recoverability;
- completeness;
- integrity.

Results shall be documented.

CRISIS MANAGEMENT

10.26 Crisis Management Framework

The Company shall maintain procedures for managing major disruptive events.

Examples include:

- cyber incidents;
- supplier failures;



- infrastructure failures;
- regulatory emergencies.

10.27 Crisis Management Team

A Crisis Management Team shall be established.

The team may include:

- Directors;
- Compliance Officer;
- Information Security Officer;
- Technical Leads;
- External Advisers.

Responsibilities shall be documented.

10.28 Incident Command Structure

During major incidents:

Strategic Level

Board and Senior Management.

Tactical Level

Incident leadership and coordination.

Operational Level

Technical recovery and implementation.

Roles shall be clearly defined.

10.29 Communication Plans

Business Continuity Plans shall include communication procedures.

Communication plans shall address:

- employees;
- suppliers;
- regulators;
- players where necessary.

Only authorised personnel may issue external communications.



10.30 Alternative Working Arrangements

The Company shall maintain the capability for remote operation where practical.

Alternative working arrangements may include:

- remote access;
- remote communications;
- cloud-hosted services.

TESTING AND EXERCISES

10.31 Business Continuity Testing

The Company shall test Business Continuity arrangements periodically.

Testing may include:

- tabletop exercises;
- scenario testing;
- walkthrough exercises.

10.32 Disaster Recovery Testing

Disaster Recovery arrangements shall be tested at least annually.

Testing may include:

- backup restoration;
- recovery simulation;
- failover testing.

Results shall be documented.

10.33 Test Reporting

Test reports shall include:

- objectives;
- participants;
- findings;
- lessons learned;



- corrective actions.

Reports shall be retained.

10.34 Corrective Actions

Deficiencies identified during testing shall be:

- documented;
- assigned;
- remediated;
- tracked to completion.

10.35 Supplier Continuity Reviews

Critical suppliers shall be reviewed periodically for resilience.

Reviews may consider:

- continuity capabilities;
- recovery arrangements;
- recent incidents.

Material concerns shall be escalated.

10.36 Management Reporting

The Information Security Officer shall periodically report on:

- continuity risks;
- testing results;
- supplier resilience;
- recovery readiness.

Material concerns shall be escalated promptly.

10.37 Continuous Improvement

The BCM and DR programmes shall be continually improved through:

- testing;
- incidents;
- audits;



- regulatory developments;
- supplier reviews.

Improvement actions shall be documented and tracked.



SECTION 11

SECURITY AWARENESS, TRAINING, AUDIT, COMPLIANCE MONITORING AND MANAGEMENT REPORTING

11.1 Purpose

The purpose of this section is to establish the framework through which Canary Alley B.V. ensures personnel understand their information security responsibilities, compliance with information security requirements is monitored, and management receives sufficient information to oversee the effectiveness of the Information Security Management System ("ISMS").

The Company recognises that information security depends not only upon technology but also upon competent personnel, effective governance and continuous oversight.

11.2 Objectives

The objectives of the Security Awareness and Compliance Programme are to:

- promote a security-conscious culture;
 - reduce human error;
 - support regulatory compliance;
 - improve detection and reporting of security incidents;
 - ensure employees understand their responsibilities;
 - monitor compliance with security requirements;
 - support continual improvement of the ISMS.
-

SECURITY AWARENESS PROGRAMME

11.3 Security Awareness Framework

The Company shall maintain a documented Security Awareness Programme.

The programme shall be proportionate to:

- organisational size;
- operational complexity;
- risk exposure;
- regulatory requirements.

Training content shall be reviewed periodically to ensure continued relevance.



11.4 Mandatory Training Requirement

Information security training shall be mandatory for all personnel.

Training obligations apply to:

- employees;
- contractors;
- consultants;
- temporary workers;
- privileged users.

Completion shall be tracked and documented.

11.5 Induction Training

All new personnel shall receive security awareness training as part of onboarding.

Training shall be completed before or shortly after access to Company systems is granted.

Topics shall include:

- information security principles;
 - acceptable use;
 - password security;
 - MFA requirements;
 - phishing awareness;
 - incident reporting;
 - data classification;
 - confidentiality obligations.
-

11.6 Annual Refresher Training

Personnel shall complete refresher training at least annually.

Refresher training shall address:

- emerging threats;
- policy updates;
- lessons learned from incidents;
- regulatory developments.

Training records shall be retained.



11.7 Role-Specific Training

Additional training shall be provided where personnel perform specialist functions.

Examples include:

Developers

Secure coding and SDLC requirements.

Infrastructure Personnel

Cloud security and administrative controls.

Compliance Personnel

Regulatory security obligations.

Customer Support Personnel

Information handling and social engineering awareness.

11.8 Privileged User Training

Personnel with elevated or administrative access shall receive enhanced training.

Training shall address:

- privileged access responsibilities;
 - system administration risks;
 - logging and monitoring;
 - incident response.
-

11.9 Developer Security Training

Developers shall receive training covering:

- secure coding;
- common vulnerabilities;
- dependency management;
- secrets management;
- code review expectations.

Training shall be refreshed periodically.

11.10 Phishing Awareness



The Company shall provide awareness regarding:

- phishing;
- spear-phishing;
- business email compromise;
- social engineering.

Personnel shall be encouraged to report suspicious communications.

11.11 Remote Working Security

Personnel working remotely shall receive guidance regarding:

- secure remote access;
- device security;
- public Wi-Fi risks;
- information handling.

11.12 Training Records

The Company shall maintain records of:

- training completion;
- attendance;
- training content;
- assessment results where applicable.

Records shall be retained for audit purposes.

COMPLIANCE MONITORING

11.13 Compliance Monitoring Framework

The Company shall maintain activities designed to assess compliance with:

- this Manual;
- supporting policies;
- regulatory requirements;
- contractual obligations.

Monitoring shall be risk-based.



11.14 Compliance Reviews

Compliance reviews may assess:

- access control compliance;
- asset management compliance;
- vulnerability management compliance;
- supplier oversight;
- incident management activities.

Findings shall be documented.

11.15 Control Effectiveness Reviews

The Information Security Officer shall periodically assess whether controls remain effective.

Reviews may consider:

- incidents;
- vulnerabilities;
- audit findings;
- regulatory developments.

Where deficiencies are identified, remediation shall be initiated.

INTERNAL AUDIT

11.16 Internal Audit Programme

The Company shall maintain an Internal Audit Programme for information security.

Audits may be performed:

- internally;
- by independent consultants;
- by specialist auditors.

Audit frequency shall be risk-based.

11.17 Audit Scope

Audit activities may include:



- governance reviews;
- access reviews;
- cloud security reviews;
- incident management reviews;
- supplier reviews;
- disaster recovery reviews.

The scope shall be documented.

11.18 Audit Independence

Where practical, auditors shall be independent of the activities being reviewed.

Conflicts of interest shall be disclosed.

11.19 Audit Findings

Audit findings shall be categorised according to risk.

Categories may include:

Critical

Immediate remediation required.

High

Priority remediation required.

Medium

Remediation required within planned timeframes.

Low

Risk-based remediation.

11.20 Corrective Actions

Audit findings shall result in documented corrective actions.

Actions shall:

- identify ownership;
- identify deadlines;
- be tracked through completion.

The Information Security Officer shall monitor progress.



KPI AND KRI FRAMEWORK

11.21 Security KPI Framework

The Company shall maintain Key Performance Indicators ("KPIs") to measure security performance.

Examples include:

- training completion rates;
- access review completion rates;
- patch compliance rates;
- vulnerability remediation performance;
- backup testing completion.

KPIs shall be reviewed periodically.

11.22 Security KRI Framework

The Company shall maintain Key Risk Indicators ("KRIs") designed to identify increasing risk exposure.

Examples include:

- critical vulnerabilities;
- overdue remediation;
- security incidents;
- failed backups;
- supplier incidents.

Material trends shall be escalated.

11.23 Security Dashboard

The Information Security Officer may maintain a security dashboard summarising:

- incidents;
- vulnerabilities;
- audit findings;
- training status;
- supplier risks.

The dashboard shall support management oversight.



MANAGEMENT REPORTING

11.24 Operational Reporting

The Information Security Officer shall provide periodic operational reporting.

Reports may include:

- vulnerabilities;
- incidents;
- access reviews;
- audit findings;
- supplier risks.

11.25 Senior Management Reporting

Senior Management shall receive periodic updates regarding:

- significant risks;
- major incidents;
- critical vulnerabilities;
- regulatory developments.

Material concerns shall be escalated promptly.

11.26 Board Reporting

The Board shall receive information security reporting at least annually.

Reports shall include:

- ISMS effectiveness;
- major incidents;
- audit results;
- risk profile;
- supplier risks;
- improvement initiatives.

The Board may request additional reporting where necessary.



ANNUAL ISMS REVIEW

11.27 Annual Management Review

The Company shall conduct an annual review of the ISMS.

The review shall evaluate:

- policy effectiveness;
- risk profile;
- incidents;
- vulnerabilities;
- audit findings;
- supplier performance;
- training effectiveness.

Results shall be documented.

11.28 Annual Information Security Report

The Information Security Officer shall prepare an Annual Information Security Report.

The report shall include:

- significant events;
- trends;
- risks;
- performance metrics;
- recommendations.

The report shall be presented to the Board.

POLICY BREACHES AND DISCIPLINARY ACTION

11.29 Policy Violations

Violations of this Manual may include:

- unauthorised access;
- password sharing;
- failure to report incidents;



- unauthorised software installation;
- mishandling information.

Violations shall be investigated.

11.30 Disciplinary Measures

Failure to comply with security requirements may result in:

- additional training;
- access restrictions;
- disciplinary action;
- contract termination.

The severity of the response shall be proportionate to the breach.

11.31 Whistleblowing and Reporting

Personnel shall be encouraged to report:

- security concerns;
- control weaknesses;
- suspected misconduct.

Reports may be made without fear of retaliation.

CONTINUAL IMPROVEMENT

11.32 Continuous Improvement Framework

The Company shall continually improve the ISMS.

Improvement activities shall be driven by:

- incidents;
 - audits;
 - vulnerability assessments;
 - penetration testing;
 - regulatory developments;
 - management reviews.
-



11.33 Improvement Register

Material improvement activities shall be tracked within an Improvement Register.

The register shall include:

- issue identified;
 - source;
 - owner;
 - target date;
 - completion status.
-

11.34 Lessons Learned Process

The Company shall maintain a lessons learned process.

Lessons may arise from:

- incidents;
- audits;
- testing;
- supplier reviews.

Lessons shall be evaluated and incorporated where appropriate.

11.35 ISMS Maturity Assessment

The Information Security Officer may periodically assess the maturity of the ISMS.

Assessments may consider:

- governance;
- technical controls;
- resilience;
- compliance;
- monitoring.

Results shall support strategic planning.

11.36 Documentation Review

Security documentation shall be reviewed:

- annually;



- following significant change;
- following major incidents;
- following regulatory change.

Outdated documentation shall be updated promptly.

11.37 Record Retention

Records generated under this section shall be retained in accordance with the Company's retention requirements.

Records include:

- training records;
- audit reports;
- management reports;
- review records;
- improvement records.