

Goodwin N.V.

Information Security Policy

Jurisdiction: Curaçao

Regulator: Curaçao Gaming Authority (“CGA”)

Version: 1.2

Effective Date: September 29, 2025

Approved by:

Name: Vladyslav Nebrat

Title: Chief Executive Officer

Signature: _____



Morganite Corporate Services B.V.
Managing Director

1. Introduction

1.1 Purpose

This Information Security Policy (the “Policy”) establishes Goodwin’s governance, control framework, and operating procedures to protect the confidentiality, integrity, and availability of information assets owned or managed by Goodwin (the “Company”). The Policy defines standard practices appropriate for B2C gaming operations licensed by the CGA and is designed to be practical, proportionate, and promptly implementable.

1.2 Objectives

The objectives of this Policy are to:

- a) protect Information Assets against unauthorized access, disclosure, alteration, or destruction;
- b) define roles and responsibilities for information security across the Company and its vendors;
- c) promote awareness and training to maintain an appropriate security culture;
- d) ensure timely detection, escalation, and response to Security Incidents; and
- e) support business continuity and regulatory compliance, including CGA requirements and applicable data-protection laws.

2. Scope

2.1 Applicability. This Policy applies to all employees, officers, contractors, agents, and third-party service providers (collectively, “Personnel”) who access Company systems, networks, applications, premises, or data. It covers all forms of information (electronic, physical, and verbal) regardless of location or storage medium, including cloud-hosted solutions used for B2C operations.

2.2 Geographic Scope. The Policy applies to operations in Curaçao and international activities conducted under the Company’s CGA license.

2.3 Exclusions. Publicly released information or data formally declassified by the ISO or a Data Owner is outside the scope of protection controls in Sections 5–15.

3. Definitions

- **Information Assets:** Data, systems, applications, infrastructure, hardware, software, and processes that store, process, or transmit information valuable to the Company, including customer data, financial records, and operational logs.
- **Confidential Information:** Non-public information whose unauthorized disclosure may adversely affect the Company, customers, or partners (e.g., personal data, financials, contracts, KYC documentation).
- **Restricted Information:** The most sensitive subset of Confidential Information, including player personal data, KYC documents, payment tokens or instrument identifiers, authentication secrets, private keys, production database snapshots, and system configuration backups.
- **Security Incident:** Any actual or suspected event that compromises or attempts to compromise the confidentiality, integrity, or availability of Information Assets (e.g., unauthorized access, data breach, malware, or material service outage).
- **Access Control:** Administrative, physical, and logical measures regulating access to Information Assets based on authorization and business need.
- **Risk Assessment:** A documented process to identify threats and vulnerabilities, evaluate likelihood and impact, and determine risk treatment.

4. Governance and Responsibilities

4.1 Executive Management

- a) approve this Policy and ensure alignment with business strategy;
- b) allocate resources to implement and maintain controls;
- c) review annual reports from the ISO regarding security posture, incidents, vendor risk, and remediation.

4.2 Information Security Officer (ISO)

The ISO shall:

- a) maintain this Policy, supporting standards, and procedures;
- b) conduct and coordinate Risk Assessments (Section 5);

- c) oversee Incident Response (Section 12) and Business Continuity/DR (Section 13);
- d) monitor compliance and report material deviations to Executive Management;
- e) coordinate with Compliance/Legal on CGA obligations and data-protection requirements.

4.3 System Owners and Data Owners

For each system and dataset, an Owner shall be designated to:

- a) classify the information (Section 6), approve access rights, and validate control effectiveness;
- b) review user access at least quarterly and after role changes;
- c) ensure timely remediation of audit and risk findings.

4.4 Department Heads

Department Heads shall ensure Personnel compliance within their remit, identify control gaps, and support training and awareness.

4.5 All Personnel

All Personnel shall:

- a) comply with this Policy and related procedures;
- b) use Information Assets for authorized business purposes only;
- c) promptly report suspected Security Incidents to the ISO.

4.6 Third Parties

Third-party providers with access to Company data or systems must contractually agree to security standards equivalent to this Policy. The Company reserves audit/review rights.

5. Risk Management

5.1 Risk Assessment Cadence. Formal Risk Assessments shall be performed at least annually and upon material change (e.g., new platform component, major integration, or new hosting region).

5.2 Method. Risks are evaluated for likelihood and impact, assigned owners, and treated through mitigation, acceptance (with executive sign-off), transfer, or avoidance.

5.3 Evidence. Risk registers, treatment plans, and closure evidence shall be maintained and made available for internal and regulatory review.

6. Information Classification and Handling

6.1 Classification Levels.

- **Public:** Approved for unrestricted distribution.
- **Internal:** Routine business information not intended for public release.
- **Confidential:** Sensitive business information (e.g., contracts, partner terms, operational procedures).

- **Restricted:** Highest sensitivity (e.g., personal data, KYC, payment tokens, secrets/keys).

6.2 Handling Requirements.

- Labeling:** Confidential and Restricted information shall be clearly labeled where practicable.
- Storage:** Restricted information shall be stored only in approved systems or encrypted repositories; avoid local desktop storage except where necessary and encrypted.
- Transmission:** Use TLS 1.2+ or equivalent secure channels (e.g., HTTPS). Do not send Restricted information via unsecured channels.
- Printing and Transport:** Discouraged; if required, keep under lock and key; avoid leaving hardcopies unattended.
- Disposal:** Shred paper; securely erase electronic media using system-provided wipe or decommissioning procedures.
- Data Minimization:** Collect only what is required for regulatory, fraud-prevention, and service purposes; avoid retaining full primary account numbers—use processor tokens where available.

7. Access Control and Identity Management

7.1 Principles. Enforce least privilege and need-to-know for all systems and datasets. Use role-based access where supported.

7.2 Authentication.

- Passwords:** Minimum 12 characters; prohibit commonly breached passwords; account lockout after repeated failures; password manager use is recommended.
- Multi-Factor Authentication (MFA):** Required for privileged/admin accounts, remote access (VPN), cloud consoles, KYC/payment platforms, and production environments.

7.3 Joiners-Movers-Leavers.

- access approved via ticket with Owner authorization;
- adjust permissions promptly when roles change;
- disable accounts on the last working day; retrieve or remotely wipe devices within 24 hours.

7.4 Privileged Access.

Use dedicated admin accounts separate from user accounts; log privileged sessions; store any unavoidable shared credentials in a Company-approved vault with access logging.

7.5 Third-Party Access.

Time-bounded, Owner-approved, monitored, and disabled upon task completion.

8. Asset, Configuration, and Change Management

8.1 Inventory. Maintain inventories of hardware, software, cloud services, and critical vendors, noting Owners, purpose, and data classification.

8.2 Standard Configuration. Servers, workstations, and network devices shall run supported operating systems, enable automatic security updates, activate host firewalls, and disable non-essential services. Default passwords must be changed prior to production use. Laptops shall have full-disk encryption.

8.3 Change Management.

- a) all production changes require a ticket, risk assessment, peer review, testing in non-production, and Owner approval;
- b) emergency changes may be executed to restore service, with retrospective review within one (1) business day.

9. Network and System Security

9.1 **Perimeter Controls.** Internet-facing services must be placed behind managed firewalls; only required ports shall be exposed; use certificates from trusted CAs.

9.2 **Segregation.** Production workloads shall be logically separated from corporate IT. Datastores containing Restricted data shall not be directly accessible from the Internet.

9.3 **Endpoint Security.** Endpoints shall run supported OS versions, have automatic updates enabled, use anti-malware, and enforce screen lock after ten (10) minutes of inactivity. USB storage is restricted to business need.

9.4 **Wireless Security.** Company wireless networks shall use WPA2 or WPA3; guest networks shall be segregated from internal networks.

9.5 **Backups.** Perform daily incremental and weekly full backups for critical systems and databases; retain at least one logically separate copy (e.g., cloud snapshots). Test restorations at least quarterly. Target **RPO $\leq$ 24 hours** and **RTO $\leq$ 24 hours** for critical databases and services.

10. Application Security and SDLC

10.1 **Source Control and Build.** Code shall reside in approved repositories with branch protection and mandatory peer review. Production builds shall be automated; only build-server-signed artifacts may be deployed.

10.2 **Dependencies.** Use repository or pipeline dependency scanning; remediate critical/high findings within fourteen (14) days or document compensating controls with Owner approval.

10.3 **Secrets Management.** Secrets shall not be hardcoded in code or configuration stored in source control. Use environment variables or managed secrets facilities provided by hosting/cloud platforms. Rotate credentials at least annually or upon suspected compromise.

10.4 **Configuration Separation.** Maintain separate configurations for development, test, and production; enforce least-privilege for database and API keys; restrict outbound connections from production to trusted endpoints.

10.5 **Testing.** Conduct functional testing prior to release. For externally exposed applications, arrange annual penetration testing by an independent party and track remediation to closure.

11. Cryptography

11.1 Data in Transit. Enforce HTTPS (TLS 1.2 or higher) for external and internal applications carrying Restricted data. Disable insecure protocols and weak ciphers.

11.2 Data at Rest.

- a) enable full-disk encryption on laptops;
- b) enable platform-provided encryption at rest for production databases and storage containing Restricted data;
- c) restrict access to encryption keys to authorized administrators; store keys using provider key facilities or a secure vault; change keys on role changes or suspected compromise.

12. Logging, Monitoring, and Alerting

12.1 Log Content. At a minimum, log authentication events (success/failure), admin actions, configuration changes, elevation of privileges, access to Restricted datasets, payment/withdrawal actions, and security tool alerts.

12.2 Retention. Retain security-relevant logs for at least six (6) months online and a total of twelve (12) months accessible (online or cold storage).

12.3 Monitoring and Alerts. Use centralized or cloud logging where feasible. Configure alerts for repeated failed logins, disabled security tools, unusual admin activity, and anomalous withdrawal patterns.

13. Vulnerability and Patch Management

13.1 Scanning. Perform weekly external scans of Internet-facing assets and monthly internal scans of production subnets or cloud equivalents.

13.2 Patch Timeframes (Targets).

- Critical: seven (7) calendar days
- High: fourteen (14) calendar days
- Medium: thirty (30) calendar days
- Low: best effort

13.3 Exceptions. Where immediate patching is infeasible, implement compensating controls (e.g., WAF rules, configuration hardening) and document an ISO-approved exception with review dates.

14. Email, Web, and Domain Hygiene

14.1 Email Security. Implement SPF, DKIM, and DMARC (quarantine or stricter) on primary domains. Block executable attachments by default and flag external senders.

14.2 Browser Controls. Keep browsers auto-updated; disable unnecessary plugins; restrict installation rights to administrators.

14.3 User Awareness. Conduct phishing awareness at onboarding and annually. Require brief refresher training after repeated simulation failures.

15. Data Protection and Privacy

15.1 Data Subject Rights. Maintain a documented process and contact channel for access, rectification, and deletion requests where legally permissible. Verify identity and coordinate with Legal/Compliance considering gaming retention obligations.

15.2 Retention and Deletion. Apply documented retention schedules consistent with regulation and contracts. Upon expiry, delete or archive to cold storage; allow backups to expire naturally unless law requires earlier deletion.

16. Third-Party and Cloud Security

16.1 Due Diligence. Prior to onboarding critical vendors (hosting, payments, KYC/AML, CRM): obtain a security questionnaire or summary certifications, data location details, incident notification commitments, and sub-processor lists.

16.2 Contractual Controls. Contracts shall require confidentiality, data-protection, incident notification within seventy-two (72) hours of confirmed incidents affecting Company data, right to audit/review summaries, and secure return or deletion of data upon termination.

16.3 Access Control. Grant vendors only necessary access for the shortest duration; disable access promptly when the engagement ends.

17. Physical and Environmental Security

17.1 Offices. Control entry with keys or electronic badges; escort and log visitors; store Restricted hardcopy in locked cabinets.

17.2 Data Centers / Cloud. Use reputable providers with industry-standard physical protections (access control, CCTV, environmental safeguards). Obtain provider assurances during due diligence.

17.3 Devices. Secure Company laptops; prevent unattended exposure in public areas; enforce automatic screen locks after ten (10) minutes.

18. Security Awareness and Training

18.1 Mandatory Training. Provide role-appropriate security training at onboarding and annually, covering data classification, phishing/social engineering, password/MFA hygiene, secure handling of Confidential/Restricted information, and incident reporting.

18.2 Targeted Training. Provide additional briefings for administrators, developers, customer support, and finance/withdrawals personnel (e.g., social-engineering indicators, handling KYC documents).

19. Acceptable Use

Personnel shall:

- a) use Company systems primarily for business purposes;
- b) not bypass security controls or introduce unapproved software;
- c) refrain from sharing credentials or transferring data through personal accounts;
- d) avoid accessing production systems from public or shared computers.

20. Review and Maintenance

This Policy shall be reviewed at least annually and upon significant changes in business operations, threat landscape, technology, or regulation. Updates require Executive approval and shall be communicated to all Personnel.