

INFORMATION SECURITY CONTROL POLICY

(CGA APRIL 2026 ALIGNED)

1. Purpose

The purpose of this Information Security Control Policy is to ensure the secure, reliable, and compliant operation of NovaPlay's IT systems and services, including business-critical lottery platforms, in accordance with applicable laws and the Curaçao Gaming Authority (CGA) Information Security Control Requirements (April 2026).

This policy establishes the minimum requirements for information security, IT governance, data protection, access control, system security, incident management, and business continuity.

The Company operates exclusively as a business-to-business ("B2B") provider of lottery software and related services.

2. Business Model Statement

The Company operates exclusively as a business-to-business ("B2B") provider of lottery software, lottery management systems, draw management platforms, ticketing solutions, random number generation services, application programming interfaces (APIs), and related technology services.

The Company's customers may include distributors, resellers, aggregators, platform providers, integration partners, licensed operators, and other business customers.

The Company does not offer lottery products directly to players, does not sell lottery tickets, does not process player funds, does not maintain player accounts, and does not establish contractual relationships with end-users.

The Company does not collect, process, or store end-user personal data.

3. Scope

This policy applies to:

- All employees, contractors, consultants, and outsourced IT service providers
- All hardware, software, networks, cloud systems, and databases
- All B2B lottery platforms, APIs, RNG services, and draw management systems
- All customer integrations, reseller platforms, and third-party environments supported by the Company
- All classified, confidential, and operational business information

4. IT Governance

- The IT Department and/or designated outsourced IT providers are responsible for implementing and maintaining this policy
- Compliance with CGA Information Security Control Requirements is mandatory
- The Board of Directors retains ultimate oversight of information security governance
- Regular audits of IT systems, processes, and controls shall be performed to ensure security and compliance

5. Information Classification

All information is classified as follows:

5.1 Classification Levels

- Public – Information approved for public disclosure
- Internal – non-sensitive operational business information
- Restricted – Sensitive internal information where unauthorized disclosure may cause operational or regulatory risk
- Confidential – Highly sensitive information including system architecture, source code, encryption keys, and customer integrations

5.2 Handling Classified Information

- Access is granted strictly on a need-to-know and least privilege basis
- Confidential information must be encrypted in transit and at rest
- Classified information must be securely stored and transmitted using approved systems only

6. Access Control

- All users must have unique accounts
- Multi-Factor Authentication (MFA) is required where technically possible
- Access to sensitive systems (RNG, draw systems, admin panels) is strictly restricted
- Access rights must be approved prior to provisioning
- Privileged access is logged and monitored

6.1 Password Requirements

Passwords must:

- Be at least 8 characters in length
- Not contain username or account name
- Include at least 3 of the following:
 - Uppercase letters (A–Z)
 - Lowercase letters (a–z)
 - Numbers (0–9)
 - Special characters (!, \$, %, etc.)
- Be unique and not reused across systems
- Never be shared or stored in plain text

7. User Management

This section defines the lifecycle management of user accounts to ensure only authorized personnel have access to IT resources.

7.1 Provisioning

- All access must be formally requested and approved
- Access is granted based on least privilege principle

7.2 Review

- User access rights must be reviewed at least quarterly

7.3 Termination

- Access must be revoked immediately upon termination or role change
- All credentials, tokens, and access keys must be disabled

7.4 Service Accounts

- Shared accounts are prohibited except for approved service accounts
- Service accounts must be securely stored and regularly reviewed

8. Asset Management System

The Company maintains a centralized asset inventory covering:

- Hardware (servers, laptops, network devices)
- Software systems (applications, APIs, platforms)
- Cloud infrastructure and virtual environments
- Cryptographic assets and security keys

Requirements:

- All assets must be recorded and updated within 24 hours of change
- Each asset must have an assigned owner
- Assets must be classified according to sensitivity
- Configuration baselines must be documented and enforced
- Secure disposal is required for all retired assets

9. Data Protection

- All sensitive data must be encrypted in transit and at rest
- Daily backups must be performed and stored securely offsite
- Backup restoration tests must be conducted regularly
- Data retention and disposal must comply with legal and contractual requirements
- No end-user personal data is collected or processed by the Company

10. System Security

- Firewalls, antivirus, and intrusion detection systems must be deployed
- Security patches must be applied in a timely manner
- Vulnerability scans and penetration tests must be performed at least annually by independent third parties
- Security configurations must follow approved baseline standards

11. Incident Management

- All IT security incidents must be reported immediately
- A formal Incident Response Plan must be maintained
- Incidents must be investigated, contained, and remediated
- All technical incidents must be reported to the CGA within 24 hours, in line with the applicable incident classification framework and reporting obligations
- Post-incident reviews are mandatory

12. Logging and Monitoring

- All critical systems must generate audit logs
- Logs must include access, system changes, and security events
- Logs must be protected from tampering or deletion
- Continuous monitoring must be implemented
- Logs must be retained according to regulatory requirements

13. Disaster Recovery and Business Continuity

13.1 Objectives

Ensure continuity of critical lottery operations and systems.

13.2 Requirements

- Recovery Time Objective (RTO): 2 hours for critical systems
- Recovery Point Objective (RPO): 15 minutes
- Daily offsite backups required
- Disaster recovery plans must be tested at least twice per year

13.3 Scenarios Covered

- Cyberattacks
- Hardware failure
- System corruption
- Natural disasters

13.4 Roles and responsibilities

- Appoint a DR coordinator and team responsible for executing the plan

13.5 Communication

- Stakeholders and regulators must be notified where legally required
- Vendor and customer contact lists must be maintained

14. Third-Party Management

- All vendors, resellers, and integration partners must comply with security requirements
- Security due diligence must be performed annually
- Contracts must include SLAs covering security, uptime, and disaster recovery
- Access may be suspended in case of security risk

15. Security Awareness and Training

- Mandatory annual security training for all staff
- Training includes phishing awareness, access control, and incident reporting
- Additional training applies to developers and privileged users

16. Compliance, Audit, and Monitoring

- Internal audits of IT controls are performed regularly
- Compliance with CGA requirements is reviewed quarterly
- Findings are reported to the Board
- Corrective actions must be tracked to closure

17. Enforcement

Non-compliance may result in:

- Disciplinary action
- Suspension of access rights
- Contract termination
- Legal action

18. Policy Review

This policy is reviewed at least annually or upon:

- Changes to CGA requirements
- Changes in IT infrastructure
- Changes in business operations

19. CGA Control Mapping Matrix (Embedded Compliance View - B2B Lottery Provider)

CGA Control Area (April 2026)	Policy Reference Section(s)	Policy Coverage / Implementation Summary
Governance	Section 4 (IT Governance), Section 16 (Compliance, Audit & Monitoring)	Board oversight, IT governance structure, outsourced IT accountability, and periodic compliance audits ensure regulatory alignment and control ownership.
Access Control	Section 6 (Access Control)	Role-based access control (RBAC), MFA enforcement, least privilege principle, restricted access to sensitive systems (RNG, draw systems), and controlled administrative privileges.
User Management	Section 7 (User Management)	Formal provisioning, quarterly access reviews, immediate deprovisioning upon termination, and controlled use of service accounts with vault storage and periodic review.
Asset Management	Section 8 (Asset Management System)	Centralized inventory of hardware, software, cloud infrastructure, and cryptographic assets with ownership, classification, lifecycle tracking, and secure disposal requirements.
Data Protection	Section 9 (Data Protection)	Encryption in transit and at rest, secure backups, offsite storage, tested restoration, and strict retention/disposal controls; explicit confirmation of no end-user data processing.
System Security	Section 10 (System Security)	Firewalls, antivirus, intrusion detection systems, patch management, secure configuration baselines, vulnerability assessments, and annual independent penetration testing.

CGA Control Area (April 2026)	Policy Reference Section(s)	Policy Coverage / Implementation Summary
Incident Management	Section 11 (Incident Management)	Formal incident response framework including detection, reporting, containment, remediation, post-incident review, and regulatory escalation to CGA where required.
Logging & Monitoring	Section 12 (Logging and Monitoring)	Comprehensive audit logging of system access, administrative actions, and security events with tamper protection, continuous monitoring, and regulated retention periods.
Disaster Recovery (DR) & Business Continuity (BCP)	Section 13 (DR & Business Continuity)	Defined RTO (2 hours) and RPO (15 minutes), daily backups, offsite storage, biannual DR testing, and structured communication plan for incidents and outages.
Third-Party Controls	Section 14 (Third-Party Management)	Security requirements embedded in contracts, annual vendor due diligence, SLA requirements for uptime and security, and controlled integration access for resellers and platforms.
Security Awareness & Training	Section 15 (Security Awareness and Training)	Mandatory annual training covering phishing, access control, incident reporting, and secure handling of systems; enhanced training for privileged users and developers.
Audit & Compliance	Section 16 (Compliance, Audit and Monitoring)	Regular internal audits, quarterly compliance reporting to Board, corrective action tracking, and continuous monitoring of control effectiveness and regulatory adherence.