

CENTRUM IT Policy Manual



CENTRUM GLOBAL B V

VERSION 2026-01
CENTRUM GLOBAL B V

TABLE OF CONTENTS

1	PURPOSE	3
2	SCOPE	3
3	REGULATORY & LEGAL COMPLIANCE	3
4	IT GOVERNANCE	4
5	INFORMATION SECURITY	4
5.1	Security Objectives	4
5.2	Access Control	4
5.3	Data Protection	4
6	GAMING PLATFORM INTEGRITY	5
7	SYSTEM DEVELOPMENT & CHANGE MANAGEMENT	5
8	INFRASTRUCTURE & NETWORK SECURITY	5
9	LOGGING, MONITORING & AUDITING	5
10	INCIDENT MANAGEMENT	6
11	BUSINESS CONTINUITY & DISASTER RECOVERY	6
12	THIRD-PARTY & VENDOR MANAGEMENT	6
13	ACCEPTABLE USE OF IT RESOURCES	6
14	TRAINING & AWARENESS	7
15	POLICY ENFORCEMENT & DISCIPLINARY ACTION	7
16	POLICY REVIEW & UPDATES	7
17	VERSION CONTROL	8

1 Purpose

The purpose of this IT Policy is to establish a structured framework for the secure, reliable, and compliant use of information technology systems supporting online gaming operations. This policy ensures the protection of player data, integrity of gaming platforms, system availability, and compliance with applicable laws and regulatory requirements.

2 Scope

This policy applies to:

- All IT systems, applications, infrastructure, and networks
This includes any on-premise servers, cloud infrastructure, hosted services, communication systems, and software used for operational or support purposes.
- Gaming platforms (web, mobile, APIs)
This includes all front-end and back-end systems, mobile apps, and APIs handling bets, user activity, or financial transactions.
- Employees, contractors, consultants, and third-party service providers
All individuals accessing CENTRUM's IT systems must follow this policy regardless of employment status.
- Production, staging, and development environments
All environments where code is developed, tested, or deployed are included to ensure consistent controls throughout the lifecycle.

3 Regulatory & Legal Compliance

The company shall comply with all applicable laws and gaming regulations, including but not limited to:

- Data protection laws (e.g., GDPR, local privacy regulations)
These laws govern the collection, processing, storage, and use of player data and must be strictly adhered to.
- Gaming authority technical standards
CENTRUM must comply with technical frameworks and platform requirements established by the Curaçao Gaming Board.
- Anti-Money Laundering (AML) and KYC system requirements
All player accounts must be subject to stringent identity verification and monitoring mechanisms.
- Cybersecurity and information security regulations
System configurations must adhere to recognized cybersecurity best practices and compliance standards.
- IT systems must support auditability, data retention, and regulatory reporting.

4 IT Governance

- The Chief Technology Officer (CTO) or designated IT Head is responsible for IT governance.
- Clear segregation of duties must exist between development, testing, and production environments.
This reduces risk of unauthorized changes and maintains operational integrity.
- All system changes must follow formal change management procedures.
Documented review and approvals are required for all system modifications.
- IT risks shall be identified, assessed, and mitigated on an ongoing basis.
Regular IT risk assessments and controls should be embedded in operational planning.

5 Information Security

5.1 Security Objectives

- Confidentiality of player and business data – Ensuring that sensitive information is accessed only by authorized individuals.
- Integrity of gaming outcomes and transactions – Protecting systems from unauthorized changes that could alter outcomes or records.
- Availability of gaming services – Maintaining consistent uptime and performance of all gaming platforms, including redundancy and failover mechanisms.

5.2 Access Control

- Role-based access control (RBAC) must be enforced – Users are assigned access based on defined roles to minimize unnecessary privileges.
- Multi-factor authentication (MFA) is mandatory for administrative and privileged access – Adds an additional layer of security against credential compromise.
- Access rights must be reviewed periodically and revoked upon termination – Ensures access is limited only to active, authorized users.

5.3 Data Protection

- Player personal data must be encrypted at rest and in transit – Using industry-standard encryption protocols (e.g., AES-256, TLS 1.2/1.3).
- Payment data must comply with PCI-DSS requirements – Applies to any system that stores, processes, or transmits cardholder data.
- Data minimization principles shall be applied – Only necessary data is collected and retained, reducing exposure and compliance burden.

6 Gaming Platform Integrity

Although CENTRUM does not have Random Games or similar and is solely focused on Pari Mutuel connectivity, elements of this policy must still be adhered to when and where applicable:

- Game logic, Random Number Generators (RNGs), and payout mechanisms must be protected against unauthorized modification – Changes must be logged and require dual-authorization.
- Production game configurations shall be immutable except through approved change processes – Changes must go through change control and testing before release.
- All game transactions must be logged and traceable – Each transaction must include timestamp, player ID, game ID, and bet outcome data.

7 System Development & Change Management

- Secure software development lifecycle (SSDLC) practices must be followed – Includes threat modeling, secure coding standards, and regular code reviews.
- All code changes require peer review, testing, and formal approval – Prevents unauthorized or low-quality code from being deployed.
- Emergency changes must be documented and reviewed retrospectively – Post-deployment reviews ensure lessons learned are captured and policy followed.
- Version control systems must be used for all source code – Repositories such as Git must be used to maintain history and enforce approval gates.

8 Infrastructure & Network Security

- Firewalls, intrusion detection/prevention systems, and DDoS protection must be implemented – Ensure continuous protection from external threats and service disruption.
- Hosting environments (cloud or on-premise) must meet industry security standards – Must comply with ISO 27001, SOC2, or similar certifications.
- Regular vulnerability scans and penetration testing must be conducted – At least quarterly or after major changes, and follow-up actions must be tracked.

9 Logging, Monitoring & Auditing

- System logs must capture user activity, transactions, system events, and security incidents – Enable incident response, forensic analysis, and auditability.
- Logs shall be protected from tampering and retained as per regulatory requirements – Store in append-only formats and back up securely.
- Continuous monitoring shall be implemented to detect suspicious activities – Use SIEM tools or custom alerting mechanisms.

10 Incident Management

- An incident response plan must be maintained and tested – Includes defined roles, communication procedures, and response timelines.
- Security incidents must be reported, investigated, and documented promptly – Incident reports must include root cause, impact assessment, and mitigation steps.
- Regulatory authorities and affected users shall be notified as required by law – Depending on breach severity and applicable jurisdictions (e.g., GDPR).

11 Business Continuity & Disaster Recovery

- Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP) must be in place to ensure minimal disruption to operations during unforeseen events such as cyberattacks, natural disasters, or system failures.
- Critical systems must have redundancy and high availability features including failover capabilities, clustering, or replication.
- Backup data shall be encrypted and tested regularly through restoration drills to ensure recovery effectiveness and compliance with data retention policies.

12 Third-Party & Vendor Management

- Third-party vendors must undergo security and compliance due diligence before integration, including checks for cybersecurity practices, financial stability, and prior regulatory compliance.
- Contracts must include provisions on data protection (including handling of personal data), confidentiality, data ownership, service level agreements (SLAs), and rights to audit.
- Vendor access to systems must be strictly limited based on need-to-know, logged, and regularly reviewed to prevent unauthorized or lingering access.

13 Acceptable Use of IT Resources

- IT resources shall be used strictly for authorized business purposes; personal or unapproved use of company systems, software, or data is not permitted.
- Unauthorized software installation, data sharing, or system misuse is prohibited, including attempts to bypass security controls or install unauthorized applications.
- Employees must adhere to company cybersecurity awareness guidelines, including reporting phishing attempts, using secure passwords, and avoiding unsafe websites or downloads.

14 Training & Awareness

- Employees must receive periodic IT security and data protection training to maintain awareness of evolving threats and corporate security expectations.
- Specialized training shall be provided to developers, system administrators, and other high-privilege users to ensure secure coding practices, system hardening, and monitoring techniques are applied.

15 Policy Enforcement & Disciplinary Action

- Violations of this policy may result in disciplinary action, up to and including termination of employment or contracts.
- Serious breaches, such as intentional data breaches or gross negligence, may be reported to regulatory authorities or law enforcement agencies in accordance with legal requirements.

16 Policy Review & Updates

- This policy shall be reviewed at least annually or upon significant regulatory or operational changes, such as updates from the Curaçao Gaming Board or adoption of new technologies.
- Updates must be approved by senior management to ensure alignment with corporate strategy, risk management practices, and applicable legal requirements.

17 Version Control

Name	Description
Document Name	IT POLICY
Version	1.0_26
Author	Kevin Bowd
Authorised By	Dennis Verrios
Distribution Date	22/01/2026
Review Date	01/02/2027



e-Management N.V.

Intro

Final Audit Report

2026-05-15

Created:	2026-05-15
By:	Bryon Finies (bryon.finies@hbmgroup.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA2wtCsjop8e-qi9pZZIIHnVOiUpLjhsmn

"Intro" History



Document created by Bryon Finies (bryon.finies@hbmgroup.com)

2026-05-15 - 7:07:54 PM GMT



Document emailed to Herman Oosten (herman.oosten@hbmgroup.com) for signature

2026-05-15 - 7:08:00 PM GMT



Email viewed by Herman Oosten (herman.oosten@hbmgroup.com)

2026-05-15 - 9:42:21 PM GMT



Document e-signed by Herman Oosten (herman.oosten@hbmgroup.com)

Signature Date: 2026-05-15 - 9:42:37 PM GMT - Time Source: server - Signature Appearance Selected: MOBILE_IMAGE



Agreement completed.

2026-05-15 - 9:42:37 PM GMT



Adobe Acrobat Sign