

Information Security Policy

Entity: Eastpoint Operations N.V.

Version: Revised (Compliance Update)

Purpose: This document incorporates mandatory remediation actions identified in the compliance review (GCB/CGA regulatory requirements, AML/CFT framework).

1. Purpose

This Information Security Policy forms part of the Company's overall compliance framework and supports the AML/CFT Policy, Responsible Gaming Policy, and Operations Manual.

It establishes operational, auditable controls to protect information assets and ensure compliance with regulatory obligations.

2. Scope

This policy applies to:

- All employees, contractors, and third parties
 - All internal systems and third-party hosted systems
 - Cloud infrastructure, payment providers, and external platforms used by the Company
-

3. Governance & Responsibilities

3.1 Roles

- IT & Security Team (Owner): System monitoring, log review, vulnerability management, incident response
- Compliance Officer (Reviewer): Regulatory assessment, incident reporting, oversight
- Management (Escalation): Approval and risk acceptance decisions

3.2 Control Ownership Framework

Each control must include:

- Owner
- Reviewer
- Escalation path

3.3 Incident Escalation

All security incidents must be escalated to the Compliance Officer for regulatory assessment and reporting.

4. Access Control

4.1 Access Provisioning Process

1. Access request submitted and approved by manager
2. Access granted by IT
3. Access logged and recorded
4. Quarterly access review conducted
5. Access revoked upon role change or termination

4.2 Monitoring

- All login attempts and privilege changes are logged
 - Logs are reviewed weekly
-

5. Data Protection

5.1 Data Retention

Customer and transaction data shall be retained for a minimum of 5 years in accordance with AML/CFT requirements.

5.2 Data Classification

- Data Owner: Responsible for classification
- IT & Security: Oversight and enforcement

5.3 Secure Deletion

Sensitive data must be deleted using documented procedures ensuring irrecoverability.

6. System & Network Security

6.1 Responsibilities

The IT Department is responsible for firewalls, IDS/IPS, and system configurations.

6.2 Patch Management

- Critical patches applied within 7 days
- Medium-risk patches within 30 days

6.3 Vulnerability Management Process

1. Perform regular system scans
 2. Identify vulnerabilities
 3. Assess risk levels
 4. Prioritize remediation
 5. Document actions
-

7. Monitoring & Logging

7.1 Logging Requirements

- All systems must generate logs for access and activity
- Logs retained for minimum 5 years

7.2 Log Review

- Daily review for critical alerts
- Weekly review for general monitoring

7.3 Tools

Centralized logging and monitoring systems (e.g., SIEM) must be used.

8. Incident Management

8.1 Response Timeline

- Incidents assessed within 24 hours

8.2 Regulatory Reporting

- Material incidents reported to GCB within 24 hours

8.3 Incident Response Process

1. Detection
 2. Containment
 3. Investigation
 4. Escalation
 5. Reporting
 6. Remediation
 7. Post-incident review
-

9. Business Continuity & Disaster Recovery

9.1 Objectives

- Define RTO and RPO for all critical systems

9.2 Testing

- DR and BCP testing conducted annually
-

10. Third-Party Security

10.1 Onboarding

- Security due diligence
- Risk assessment
- Compliance approval

10.2 Monitoring

- Annual security review of providers
-

11. Change Management

- All changes must be documented and approved by IT management
 - High-risk changes require Compliance review
-

12. Training & Awareness

- Annual security awareness training mandatory
 - Includes AML-related risks and fraud indicators
-

13. Compliance & Audit

- Internal audits conducted annually
 - Findings documented and tracked
-

14. Continuous Improvement

- All incidents and audit findings logged in a remediation register
- Each item assigned an owner and deadline

15. SLA Framework

Defined timelines:

- Incident response: 24 hours
 - Log review: daily/weekly
 - Access reviews: quarterly
 - Patch management: 7–30 days
-

16. System Identification

The Company must maintain an inventory of:

- Logging systems
 - Monitoring tools
 - Access control systems
 - Security tools (IDS/IPS, SIEM)
-

17. AML Integration

Information security controls must support AML/CFT compliance, including protection of:

- Customer data
 - Transaction records
 - Regulatory reporting processes
-

18. Final Compliance Statement

This policy is aligned with:

- GCB AML regulations (2025)
- Data protection obligations

- Operational risk management requirements

All controls defined herein are operational, measurable, and subject to audit validation.
