

Information Security Policy

Company: F3 markets N.V.

Jurisdiction: Curaçao

Document owner: Compliance Officer (Information Security Officer)

Version: 1.0

Effective date: 03.03.2026

Review cycle: At least annually and upon any material regulatory, operational, or technological change

1. Purpose

This Information Security Policy establishes the governance, principles, and minimum control requirements for protecting the confidentiality, integrity, availability, authenticity, and traceability of information processed by F3 markets N.V.

The Policy is designed to support the secure and lawful operation of a Curaçao-licensed gambling business, including gaming operations, player accounts, payment processing, compliance monitoring, responsible gaming controls, and regulatory reporting.

2. Scope

This Policy applies to:

- F3 markets N.V.
- All directors, officers, employees, temporary staff, contractors, consultants, and outsourced service providers with access to Company information or systems.
- All information assets owned, controlled, processed, or hosted by the Company.
- All business processes supporting gambling operations, customer onboarding, KYC/CDD, AML/CFT controls, responsible gaming controls, payments, dispute handling, customer support, marketing operations, and regulatory communications.
- All technology environments, including cloud services, on-premise assets, software-as-a-service platforms, gaming platforms, back-office systems, payment integrations, logging infrastructure, development environments, and end-user devices.

3. Policy Objectives

The objectives of this Policy are to:

- Protect player, business, and regulatory information against unauthorized access, disclosure, alteration, destruction, or loss.
- Ensure resilient and secure delivery of gambling services.
- Maintain records and logs necessary for supervision, investigations, audits, and legal proceedings.
- Support compliance with applicable legal, regulatory, contractual, privacy, AML/CFT, and licensing obligations.
- Promote a risk-based security culture across the Company and its critical service providers.

- Ensure the Company can detect, respond to, contain, and recover from security incidents in a timely manner.

4. Regulatory Alignment

F3 markets N.V. shall maintain an information security framework that supports regulatory oversight in Curaçao and is appropriate for a licensed online gambling operator.

This Policy shall be interpreted and applied in a manner consistent with the Company's licensing obligations, supervisory expectations, portal submission obligations, and any applicable laws, regulations, standards, or official guidance relevant to the Company's operations.

5. Governance and Accountability

5.1 Board and Executive Management

The Board of Directors and executive management are accountable for establishing and maintaining an effective information security framework.

Management shall ensure that adequate financial, technical, and human resources are allocated to implement this Policy.

Executive management shall review information security risks, significant incidents, remediation status, and material control deficiencies on a periodic basis, and no less than annually.

5.2 Compliance Officer and Security Function

The Compliance Officer shall coordinate alignment of this Policy with licensing, AML/CFT, responsible gaming, privacy, and reporting obligations.

The Company may designate an Information Security Officer or equivalent responsible person to manage day-to-day implementation, control monitoring, and incident coordination.

The security governance structure shall be formally documented, current, and available for supervisory review when required.

5.3 Employees and Users

All personnel are responsible for protecting Company information, following approved security procedures, completing mandatory training, promptly reporting incidents or suspicious activity, and using Company assets only for authorized business purposes.

5.4 Third Parties

Third-party processors, gaming suppliers, payment providers, cloud providers, identity verification vendors, and other outsourced service providers shall be subject to appropriate due diligence, contractual security obligations, confidentiality obligations, and ongoing oversight proportionate to the risk and criticality of the services provided.

6. Information Classification

Information shall be classified at minimum into the following categories:

- **Public** — information approved for public disclosure.

- **Internal** — routine business information intended for internal use.
- **Confidential** — sensitive operational, financial, commercial, technical, or compliance information.
- **Restricted** — highly sensitive information requiring enhanced protection, including player personal data, identity documents, payment-related data, AML/CFT investigation data, regulator submissions, security credentials, cryptographic secrets, and incident investigation records.

Classification shall determine access restrictions, storage rules, transmission safeguards, encryption requirements, retention periods, and disposal requirements.

7. Asset Management

The Company shall maintain and periodically review an inventory of critical information assets, including:

- Gaming platforms and player account systems;
- KYC/CDD and AML/CFT systems;
- Payment and wallet integrations;
- Databases, storage repositories, and backups;
- Logging, monitoring, and alerting systems;
- End-user devices and administrator workstations;
- Vendor-managed and cloud-hosted systems.

Each critical asset shall have an identified owner responsible for classification, acceptable use, access approval, and risk treatment.

8. Access Control

Access to information and systems shall be granted on the principles of least privilege, need-to-know, segregation of duties, and role-based access.

At a minimum, the Company shall:

- Identify users.
- Require strong authentication for all users and multi-factor authentication for privileged access, remote access, administrative consoles, production environments, payment systems, and security tooling.
- Implement formal user provisioning, access change, and deprovisioning procedures.
- Periodically recertify user access, especially for privileged, technical, finance, AML/CFT, customer data, and regulatory portal access.
- Restrict shared accounts except where technically unavoidable, and in such case ensure compensating controls and traceability.
- Log and monitor privileged activities.

9. Cryptography and Data Protection

The Company shall use appropriate cryptographic controls to protect Restricted and Confidential information in transit and at rest.

Encryption standards, key management procedures, certificate lifecycle management, and secret storage practices shall be documented and periodically reviewed.

Transmission of sensitive data to regulators, banks, payment providers, or other authorized third parties shall occur only through approved secure channels.

10. Secure Operations

The Company shall implement operational controls appropriate to a licensed online gambling operator, including:

- Secure configuration baselines for servers, endpoints, cloud services, and network components;
- Patch and vulnerability management based on asset criticality and exploitability;
- Malware protection and endpoint detection measures;
- Centralized logging and time synchronization;
- Monitoring for suspicious activity, fraud indicators, abuse of privileged accounts, and anomalous access patterns;
- Capacity management and availability monitoring for customer-facing services;
- Backup controls with periodic restoration testing;
- Change management for infrastructure, code, integrations, games, payment functionality, and security tools.

Production changes that may impact player protection, payment integrity, responsible gaming controls, regulatory reporting, or AML/CFT controls shall be risk-assessed, approved, tested, and traceable.

11. Network and Infrastructure Security

The Company shall protect internal and external network boundaries through layered technical controls, including segmentation, firewalls, secure remote access, denial-of-service protection where appropriate, secure administration channels, and continuous monitoring of exposed services.

12. Secure Development

Where the Company develops or customizes software, it shall maintain a secure software development lifecycle, including:

- Security requirements during design;
- Segregation of development, test, and production environments;
- Code review and change approval;
- Dependency and vulnerability management;
- Secure handling of secrets;
- Pre-release testing, including security testing proportionate to risk.

High-risk changes affecting player balances, gaming fairness controls, identity verification, payment controls, self-exclusion, limits, or reporting shall receive enhanced review before release.

13. Logging, Monitoring, and Evidence

The Company shall generate, retain, protect, and review logs necessary to support security operations, fraud prevention, AML/CFT monitoring, internal investigations, complaints handling, and regulatory cooperation.

Logs should, at a minimum where relevant, record:

- User authentication events;
- Administrative actions;
- Access to Restricted data;
- Payment events and exceptions;
- KYC/CDD workflow actions;
- Account changes;
- Security alerts and incident actions;
- System configuration changes;
- Relevant communications or submissions to regulators.

Logs shall be protected from unauthorized alteration and retained for periods defined by law, regulation, litigation hold, investigative need, or internal retention schedules.

14. Data Privacy and Personal Data

The Company shall process personal data lawfully, fairly, and securely, applying privacy-by-design and need-to-know principles.

Personal data shall be collected, used, stored, shared, retained, and deleted according to applicable law, internal privacy standards, and regulator-facing obligations.

The Company shall ensure documented legal bases, access restrictions, secure disclosure procedures, processor oversight, and incident escalation for regulated data-sharing activities.

15. Third-Party Risk Management

Before onboarding a critical supplier or processor, the Company shall perform due diligence appropriate to the service, including assessment of security posture, data protection capability, business continuity, incident notification arrangements, sub-processing, and legal/regulatory fit.

Contracts with critical providers shall, where appropriate, include:

- Confidentiality and data protection obligations;
- Minimum security standards;
- Audit and information rights;
- Incident notification obligations;
- Business continuity and disaster recovery commitments;

- Data return or secure deletion on termination;
- Cooperation requirements for regulatory inquiries and investigations.

Where a provider supports critical compliance or supervisory functions, the Company shall ensure that the relationship does not impair its ability to demonstrate control to the regulator.

16. Human Resources Security

The Company shall implement personnel security measures proportionate to role sensitivity.

These shall include contractual confidentiality obligations, acceptable use rules, screening where legally permissible and appropriate, role-based training, and prompt revocation of access upon termination or role change.

Personnel performing critical activities, especially those involving compliance, AML/CFT, payments, privileged access, player funds, or regulator interaction, shall receive enhanced security and confidentiality training.

17. Security Awareness and Training

All personnel shall complete information security and data protection training at onboarding and periodically thereafter.

Training shall be tailored to role and cover, as relevant, phishing, credential hygiene, secure handling of player information, incident reporting, AML/CFT data sensitivity, fraud red flags, secure remote work, and regulatory confidentiality.

Additional training shall be assigned to administrators, developers, compliance staff, finance personnel, customer support teams, and responsible gaming personnel.

18. Incident Management

The Company shall maintain an incident response framework for identifying, escalating, assessing, containing, eradicating, recovering from, and documenting information security incidents.

Security incidents shall be categorized by severity and business impact, with escalation criteria covering at least:

- Personal data breaches;
- Unauthorized access to player accounts or funds;
- Fraud affecting gameplay, balances, or withdrawals;
- Loss or compromise of regulatory submission data;
- Material outages affecting critical gambling controls.

Incident records shall be complete, time-stamped, preserved, and available for internal review and external reporting where required by law, contract, or regulator instruction.

19. Business Continuity and Disaster Recovery

The Company shall maintain business continuity and disaster recovery arrangements proportionate to the criticality of its gambling operations and compliance obligations.

This shall include identification of critical services, recovery priorities, alternate processing capabilities where appropriate, tested backups, and periodic scenario exercises.

Recovery planning shall prioritize services supporting player authentication, gameplay integrity, deposits, withdrawals, self-exclusion and limit controls, AML/CFT monitoring, customer support, and regulator communications.

20. Responsible Gaming and Security Interfaces

Security controls shall support responsible gaming controls by protecting the integrity and availability of tools such as age verification, self-exclusion, cool-off periods, deposit limits, behavior tracking, and related customer information.

Where responsible gaming mechanisms are implemented in platform logic or third-party systems, the Company shall treat related configurations, override rights, and event logs as Restricted information requiring enhanced change control and monitoring.

21. AML/CFT and Investigation Support

The Company shall ensure that security controls support effective customer due diligence, screening, transaction monitoring, record retention, internal investigation, suspicious activity handling, and regulatory cooperation.

Access to AML/CFT cases, source-of-funds information, sanctions screening outputs, unusual transaction reviews, and investigation records shall be tightly restricted, logged, and reviewed.

22. Physical and Environmental Security

Where the Company uses office premises, equipment rooms, or secure storage locations, physical access shall be controlled in accordance with business need and asset sensitivity.

Physical media containing Restricted information shall be securely stored, transported, and destroyed.

If infrastructure is hosted by third parties, the Company shall obtain reasonable assurance that physical and environmental protections are implemented by those providers.

23. Retention and Secure Disposal

Information shall be retained in accordance with legal, regulatory, contractual, accounting, AML/CFT, dispute, and operational requirements.

Once retention periods expire and no legal hold or legitimate business need remains, data and media shall be securely deleted, destroyed, or anonymized using methods appropriate to the medium and sensitivity.

24. Policy Exceptions

Any exception to this Policy shall be documented, justified by business need, risk-assessed, approved by appropriate management, and time-limited.

Compensating controls shall be implemented where feasible.

Exceptions affecting regulatory reporting, personal data protection, AML/CFT controls, player balances, or responsible gaming tools shall require review by Compliance and executive management.

25. Monitoring, Review, and Assurance

Compliance with this Policy shall be monitored through control testing, access reviews, vulnerability assessments, incident reviews, vendor oversight, audit activity, and management reporting.

This Policy shall be reviewed at least annually and whenever there is a material change in the Company's business model, licensing status, systems architecture, outsourcing model, legal obligations, or regulatory requirements.

26. Enforcement

Violation of this Policy may result in disciplinary action, contractual remedies, removal of access, escalation to management, notification to competent authorities where required, and other legal or operational measures appropriate to the circumstances.

27. Approval

This Policy shall be approved by the Board of Directors or authorized executive management of F3 markets N.V. and communicated to all relevant personnel and applicable third parties.

Annex 1 — Minimum Control Baseline

F3 markets N.V. shall maintain, at minimum, the following baseline controls:

- Asset inventory for critical systems and data stores.
- Formal information classification and handling rules.
- Role-based access control and periodic access reviews.
- Multi-factor authentication for privileged and remote access.
- Encryption for sensitive data in transit and at rest.
- Secure backups and restoration testing.
- Centralized logging and security monitoring.
- Incident response procedures and contact matrix.
- Vendor due diligence and contractual security clauses.
- Employee awareness training.
- Change management and secure release practices.
- Data retention and secure disposal procedures.
- Business continuity and disaster recovery planning.

Annex 2 — Incident Response Plan

1. Purpose

This Incident Response Plan establishes the operational process by which F3 markets N.V. identifies, triages, contains, investigates, remediates, recovers from, documents, and reports information security incidents affecting its gambling operations, player data, payment flows, AML/CFT controls, or regulatory obligations.

2. Scope of Incidents

This Plan applies to actual or suspected incidents involving:

- Unauthorized access to systems, accounts, or data;
- Compromise of player accounts, wallets, or balances;
- Personal data breaches;
- Payment fraud or payment system compromise;
- AML/CFT monitoring disruption or compromise of investigation data;
- Malware, ransomware, phishing, or business email compromise;
- Denial-of-service or other attacks affecting service availability;
- Integrity issues affecting games, odds, limits, responsible gaming controls, or reporting;
- Insider misuse or abuse of privileged access;
- Loss, alteration, or unauthorized disclosure of data submitted or to be submitted to the regulator;
- Third-party or cloud incidents with impact on regulated operations.

3. Incident Response Principles

All incidents shall be handled according to the following principles:

- Immediate escalation on a need-to-know basis;
- Preservation of evidence;
- Rapid containment proportionate to business and regulatory risk;
- Accurate and time-stamped documentation;
- Clear ownership and decision-making;
- Timely internal and external reporting;
- Restoration of services in a controlled manner;
- Post-incident remediation and lessons learned.

4. Roles and Responsibilities

4.1 Incident Response Team

The Company shall maintain an Incident Response Team, which may include:

- Compliance Officer;
- Chief Technology Officer or senior IT lead;

- Operations representative;
- AML/CFT representative where relevant;
- Data protection/privacy representative where relevant;
- Legal counsel, internal or external;
- Communications representative;
- Third-party forensic, infrastructure, or platform specialists as required.

4.2 Core Responsibilities

- **Compliance Officer and Incident Manager:** assesses reporting obligations to the regulator and coordinates portal submissions, coordinates the response, assigns actions, maintains timeline, and lead
- **Legal/Privacy Function:** assesses breach-notification, privilege, contractual, and data-sharing issues.
- **Business Owner:** decides on business continuity measures for the affected service.
- **Communications Lead:** manages internal and external messaging where needed.

5. Severity Classification

Severity	Description	Examples
Critical	Incident causes or is likely to cause major regulatory, financial, customer, or operational impact	Mass player account takeover; ransomware in production; compromise of withdrawal controls; outage of critical gambling systems
High	Serious incident affecting sensitive data, regulated functions, or major internal systems	Breach of KYC database; compromise of privileged admin account; significant DDoS with customer impact
Medium	Contained incident with limited scope but requiring formal handling	Malware on staff endpoint; unauthorized access attempt with limited impact
Low	Minor event or security anomaly with no confirmed material impact	Blocked phishing attempt; isolated policy violation

Any incident potentially reportable to the regulator, or affecting regulated operations, shall be treated at least as High until assessed otherwise.

6. Detection and Reporting Channels

Incidents may be detected through:

- Security monitoring tools and alerts;
- Application and infrastructure logs;
- Fraud monitoring or AML/CFT alerts;
- Customer complaints or player support channels;

- Vendor notifications;
- Employee reports;
- Threat intelligence or law enforcement communication.

All personnel shall immediately report suspected incidents to the designated internal escalation channel. Reports should include, where known, the time of detection, affected system, affected users or customers, observed indicators, and actions already taken.

7. Response Workflow

7.1 Identification

Upon receipt of an alert or report, the Incident Manager or delegate shall:

1. Open an incident record.
2. Assign a unique incident identifier.
3. Record the time of detection and reporting.
4. Perform an initial impact assessment.
5. Determine provisional severity.
6. Trigger escalation to the Incident Response Team where required.

7.2 Initial assessment

Initial assessment shall determine:

- Whether the event is a true security incident;
- Which systems, data, jurisdictions, customers, funds, or controls are affected;
- Whether player funds, player data, responsible gaming controls, AML/CFT controls, or regulatory reporting integrity may be affected;
- Whether a third party is involved;
- Whether the incident may qualify for regulator notification.

7.3 Containment

Containment actions may include:

- Disabling compromised accounts;
- Blocking malicious IP addresses or sessions;
- Isolating hosts or containers;
- Suspending affected integrations;
- Pausing withdrawals or sensitive transactions where necessary;
- Revoking keys, tokens, or certificates;
- Applying temporary rules in WAF, firewall, or fraud systems.

Containment decisions shall balance evidence preservation, customer protection, operational continuity, and legal/regulatory duties.

7.4 Evidence Preservation

For incidents of Medium severity or above, and for any incident with potential legal, regulatory, or financial significance, the Company shall preserve:

- Relevant logs and alerts;
- Screenshots and system state information;
- Copies of malicious files or indicators, where safe;
- Access records and administrator activity logs;
- Communications with vendors, processors, or customers;
- Timeline of response decisions and actions.

Evidence handling shall maintain integrity, access restriction, and chain-of-custody records where appropriate.

7.5 Eradication

Eradication may include malware removal, credential reset, vulnerability remediation, patching, code rollback, infrastructure rebuild, access revocation, secret rotation, or removal of unauthorized persistence.

7.6 Recovery

Recovery shall occur only after the Incident Manager, technical owner, and business owner confirm that residual risk is acceptable. Recovery actions may include staged service restoration, enhanced monitoring, reconciliation of transactions, user communication, and validation of critical controls.

8. Regulatory Reporting

The Company shall assess without delay whether an incident qualifies for reporting to the regulator through the regulatory portal.

The Compliance Officer shall be responsible for coordinating regulator-facing submissions. In the event of any qualifying adverse incident, the Operator shall immediately complete and submit an Incident Report through its personal account in the regulatory portal in order to notify the regulator without delay.

Where facts are incomplete, an initial report shall be submitted based on verified information available at the time, followed by supplemental updates as material facts become known.

At minimum, incident records prepared for potential regulator reporting should include:

- Date and time of detection;
- Date and time of occurrence, if known;
- Affected systems, domains, services, or business functions;
- Description of the incident;
- Impact on players, funds, regulated controls, or operations;
- Immediate containment actions taken;
- Current status and recovery steps;

- Contact details for the responsible Company representative;
- Any third-party involvement.

9. Notification Matrix

Trigger	Internal Notification	External Consideration
Player data breach	Security Lead, Compliance, Legal/Privacy, Management	Regulator portal assessment; privacy/legal assessment; processor/customer notices as applicable
Player fund or withdrawal compromise	Security Lead, Finance, Compliance, Management	Regulator portal assessment; payment provider notice; law enforcement/legal assessment
AML/CFT system failure or investigation data compromise	Compliance, Security Lead, Management	Regulator portal assessment; AML reporting implications
Major outage of gambling operations	IT Lead, Operations, Compliance, Management	Regulator portal assessment; supplier notices
Third-party critical incident	Vendor Owner, Security Lead, Compliance, Management	Regulator portal assessment; contractual notices

10. Communication Controls

No employee other than authorized personnel may communicate externally about an incident. External communications to regulators, banks, payment processors, suppliers, customers, media, or law enforcement shall be coordinated through Compliance, Legal, and authorized management.

Where customer communication is necessary, messages shall be accurate, approved, and consistent with known facts. Communications shall avoid speculation and shall not compromise investigations or evidence preservation.

11. Special Scenarios for Gambling Operations

The following scenarios require immediate escalation to executive management and Compliance:

- Unauthorized manipulation or suspected manipulation of game logic, RNG-connected systems, payout tables, or bonus mechanics;
- Mass account takeover or credential-stuffing affecting players;
- Compromise or bypass of self-exclusion, limit, affordability, or responsible gaming controls;
- Suspicious change to withdrawal rules, wallets, or banking destinations;
- Breach affecting KYC/CDD repositories, sanctions screening, or source-of-funds records;
- Domain hijacking, DNS compromise, or impersonation of licensed domains;

- Incident affecting data submitted through or required for the regulatory portal.

12. Service Providers and Supply Chain Incidents

Where a third party experiences an incident affecting the Company, the vendor owner and Security Lead shall immediately obtain:

- Nature and scope of the incident;
- Systems and data affected;
- Timing and duration;
- Containment measures;
- Impact on confidentiality, integrity, availability, and compliance;
- Expected restoration timeline;
- Copies of relevant notices or reports.

Contracts with critical suppliers should require prompt incident notification and cooperation with investigations and regulator-facing reporting.

13. Recordkeeping

For each incident, the Company shall maintain a complete case file containing:

- Initial report and classification;
- Timeline of decisions and actions;
- Evidence inventory;
- Affected systems and data types;
- Notifications made;
- Business impact assessment;
- Root cause analysis;
- Corrective and preventive actions;
- Closure approval.

Incident records must be sufficiently complete and retrievable to support supervisory review