

Farup Entertainment N.V. Information Security Policy

Last updated 23rd April 2026

1. Purpose

This Information Security Policy defines the principles, controls, and responsibilities applied by Farup Entertainment NV 'The Company' to protect systems, player data, and operational infrastructure.

The Company operates a **cloud-based, vendor-supported platform model**. Core platform components (including PAM, database infrastructure, and certain security controls) are provided and managed by contracted third-party providers.

Security responsibilities are shared between the Company and its providers in accordance with:

- contractual arrangements
- regulatory obligations
- operational responsibilities

This policy reflects the Company's:

- size and organisational structure
 - outsourcing model
 - risk profile
-

2. Scope

This policy applies to:

- all employees and contractors
- all company-issued devices
- production, staging, and development environments
- third-party access to Company-managed systems

This policy does not override internal security controls operated by third-party providers within their managed environments.

3. Governance & Responsibilities

The Company operates a **lean security model embedded within Engineering and Operations**.

3.1 Accountability

- Executive Management retains overall accountability for information security
- Engineering / Technology functions are responsible for implementation and maintenance of controls
- Operational security activities are handled within Engineering and Operations

3.2 Roles

- **System Owners:** approve and review access, ensure correct configuration
- **Engineering Team:** manages infrastructure, deployments, and technical controls
- **Operations / Management:** oversees incident response and risk review
- **Employees & Contractors:** comply with security requirements and report issues

All development, infrastructure configuration, and system access management are centrally controlled by the Company as the group's technology provider.

The Company does not operate a dedicated Security Operations Centre (SOC). Controls are proportionate to scale and risk.

4. Risk Management

The Company maintains a **proportionate risk management approach** aligned with its operational model.

- Information security risks are reviewed periodically (at least annually or following material changes)
- Risk areas considered include:
 - cyber threats (e.g. unauthorised access, DDoS, phishing)
 - data loss or leakage
 - third-party service failure
 - operational disruption
- Risk reviews are conducted by Engineering and Management
- Identified risks are mitigated through:
 - technical controls
 - vendor-managed controls
 - operational procedures

Material risks and mitigation actions are documented internally where appropriate.

5. Access Control & Identity Management

5.1 Access Principles

- Access is granted on a **least privilege** and role-based basis
- Access requires approval from a system owner or responsible manager
- Access is limited strictly to business need

5.2 Access Lifecycle

- Access is granted during onboarding
- Access is updated upon role change
- Access is removed promptly upon offboarding
- Access rights are reviewed periodically

5.3 Authentication

- MFA is enforced where supported (e.g. AWS, administrative systems, key third-party tools)
 - Passwords are securely stored using password managers
 - Strong password practices are applied where systems support them
-

6. Infrastructure, Hosting & System Security

6.1 Cloud Infrastructure

- Infrastructure is hosted in AWS
- Production, staging, and development environments are logically separated
- Access to production systems is restricted and logged

6.2 System & Network Security

Systems are protected using a layered security model combining:

- cloud-native security controls within AWS
- network-level protections and access restrictions
- logical separation between environments

Infrastructure is designed to isolate backend systems from front-end application layers, reducing risk exposure and improving resilience.

6.3 Third-Party Platform Providers

Core platform components (e.g. PAM, database infrastructure) are managed by third-party providers.

Providers are responsible for:

- infrastructure-level security
- hosting-layer controls
- database backup and restoration

The Company is responsible for:

- configuration of its own systems
 - access control within its environments
 - validation of system functionality after recovery
-

7. Data Protection

The Company acts as **Data Controller** for player and employee data.

Controls include:

- role-based access restrictions
- encryption in transit (HTTPS/TLS)
- encryption at rest where supported
- contractual data processing agreements with third-party providers
- controlled onboarding and offboarding processes

Data is retained and securely deleted in accordance with legal, regulatory, and operational requirements.

8. Device & Endpoint Security

- All company-issued devices are managed via MDM
 - Devices are encrypted (e.g. BitLocker / FileVault)
 - Devices can be remotely restricted or wiped if compromised
 - Access to production systems requires approved devices and authentication
-

9. Backup & Business Continuity

- Core database backups are managed by platform providers using AWS infrastructure
- Backups are performed on a scheduled basis (typically multiple times per day) in line with recovery objectives
- Backup storage, retention, and access controls are managed within provider environments

Restoration procedures include:

- selection of the most recent valid backup
- restoration into a controlled environment
- validation of database integrity and configuration
- application-level verification

The Company coordinates with providers during restoration events and validates system functionality following recovery.

Business continuity measures are proportionate to system criticality and scale.

10. Logging, Monitoring & Alerting

- Logging is enabled across infrastructure and application layers where supported
- Logs are used for:
 - troubleshooting
 - monitoring
 - incident investigation

Monitoring and alerting are supported through a combination of:

- infrastructure-level logging
- application logs
- event-based alerting systems

Alerts are used to notify relevant personnel of system issues or anomalies in real time.

Logs and alerts are reviewed periodically by Engineering and Operations personnel as part of system monitoring and incident response.

Log retention is aligned with system capabilities and provider configurations.

11. Vulnerability Management & Security Testing

Security testing is performed proportionate to business scale and exposure.

This includes:

- external vulnerability scanning of internet-facing infrastructure
- secure development practices and code review
- remediation of identified issues based on risk

External vulnerability scanning is conducted using a third-party provider, and findings are reviewed and addressed accordingly.

Where appropriate, additional third-party assessments may be commissioned.

12. Incident Management

12.1 Definition

A security incident includes:

- unauthorised access
- data loss or exposure
- loss of player funds
- material operational disruption

12.2 Response Model

The Company operates a structured **on-call incident response model**:

- A dedicated on-call contact is maintained and shared with key providers
- Calls are routed to the responsible on-call engineer
- Incidents are acknowledged within defined response time targets (typically within 15 minutes)

12.3 Incident Handling

Incidents are:

- triaged and prioritised
- escalated internally and to relevant third-party providers
- managed through to resolution by the assigned incident owner

Handling includes:

- coordination with providers via service desks and communication channels
- provision of logs, user data, and technical details
- escalation to senior management where required

12.4 Resolution & Review

- System functionality is validated after resolution
- Stakeholders are informed of outcomes
- Material incidents are documented and may be subject to post-incident review

13. Third-Party Risk Management

The Company relies on third-party providers for:

- platform infrastructure (PAM)
- database hosting
- cloud services (AWS)
- payment processing
- sportsbook and integrations

Risk is managed through:

- contractual agreements
- reliance on provider security frameworks
- operational oversight and monitoring

Providers are expected to maintain appropriate security standards.

14. Change Management

- System and configuration changes are managed within Engineering processes
- Changes are reviewed and tested prior to deployment where applicable
- Production deployments are restricted to authorised personnel

Security considerations are incorporated into development and deployment processes.

15. Employee Security & Awareness

- Employees and contractors must follow security practices
- Security responsibilities are communicated during onboarding
- Personnel are expected to:
 - protect company data
 - use systems appropriately
 - report incidents or suspicious activity

Security awareness is reinforced periodically as part of operational practices.

16. Policy Review

This policy is reviewed by management:

- at least annually
- following material system or business changes
- in response to regulatory developments

Updates are approved by management and communicated internally.