

Information Security Policy

99 Services B.V.

Document Control

Version	Date	Description of Changes	Author
1.0	26.01.2026	Initial draft	IGA Trust B.V.

1. Purpose

The purpose of this policy is to establish a comprehensive framework for protecting information assets against internal and external threats. This policy defines principles, responsibilities, and security controls necessary to safeguard digital and physical assets across the organization to support operational resilience, regulatory compliance, and the confidentiality, integrity, and availability of information systems.

2. Scope

This policy applies to all employees, contractors, consultants, vendors, and third-party service providers who access, process, manage, or store the organization's information or information systems. It applies to all information formats (digital, physical, verbal) and all systems, whether on-premises, cloud-based, or mobile.

3. Governance and Responsibility

Information security is governed at the highest levels of the organization and embedded in all operational, technical, and administrative functions.

- Executive Leadership is responsible for setting a strategic direction for information security and ensuring sufficient resources are allocated.
- Chief Information Security Officer (CISO) is accountable for implementing this policy, conducting risk assessments, and coordinating internal and external audits.
- Department Heads must ensure their teams comply with security policies and controls.
- All Users are responsible for protecting information assets in accordance with this policy and must report any suspected security incident or policy breach immediately.

4. Risk Management

The organization maintains a documented information security risk management process that includes:

- Regular risk assessments to identify, assess, and prioritize information security risks
- Evaluation of likelihood and impact of risks on operational, legal, and reputational objectives
- Implementation of risk treatment plans to mitigate or accept risks based on defined criteria

- Periodic review and updates to the risk register and risk controls

5. Information Classification and Handling

Information assets must be classified based on their sensitivity and business value, and handled according to their classification level:

- **Public:** May be freely distributed without harm.
- **Internal Use:** Access limited to authorized internal personnel.
- **Confidential:** Requires restricted access due to operational sensitivity.
- **Highly Confidential / Restricted:** Critical data requiring strict access control and encryption (e.g., personal data, financial records, system architecture, customer data).

All information must be labeled and protected throughout its lifecycle—from creation and storage to transmission and destruction.

6. Access Control

Access to information is governed by the following key principles:

- **Least Privilege:** Users shall only be granted the minimum level of access required to perform their job responsibilities.
- **Need-to-Know:** Access to sensitive information shall only be granted to authorized personnel with a justified business need.
- **Separation of Duties:** Critical tasks must be divided between individuals to reduce the risk of misuse or fraud.

Access Authorization

- All access must be approved by the designated data or system owner through a documented access request and approval process.
- Access to production environments, databases, and administrative functions requires additional levels of approval and logging.
- Temporary access must be time-bound and revoked automatically upon expiry.

User Access Management

- **Onboarding:** Access rights shall be assigned during onboarding based on the employee's job function and department.
- **Changes in Role:** Access must be reviewed and updated promptly when users change roles.
- **Termination:** All access rights shall be revoked immediately upon termination or resignation. This includes access to email, VPN, physical premises, cloud services, and applications.
- **Access Reviews:** Periodic reviews (at least quarterly) of user access shall be performed to validate the appropriateness of access rights and identify excessive privileges.

Authentication and Password Policy

- All systems must enforce secure authentication methods, including:
 - Unique usernames and strong passwords
 - Multi-factor authentication (MFA) for remote access, administrative accounts, and access to sensitive systems
- Passwords must:
 - Be at least 12 characters in length
 - Include complexity requirements (uppercase, lowercase, numbers, special characters)
 - Be changed at least every 90 days or as dictated by risk
 - Not be reused for a defined number of previous versions

Privileged Access Management (PAM)

- Privileged accounts (e.g., system admins, DBAs, security officers) must be:
 - Created separately from normal user accounts
 - Monitored continuously using audit logs and alerts
 - Logged out of systems when not actively in use
- Privileged access must be assigned only to individuals with a legitimate business requirement and must be reviewed monthly.

System and Application Access Control

- All systems must enforce session timeouts and automatic lockouts after inactivity.
- Access must be logged and auditable.
- Remote access must be via secure encrypted channels (e.g., VPN, SSH with MFA).
- Access to critical systems must be segregated from development and test environments.

Physical Access Control

- Physical access to data centers, server rooms, and restricted office zones must be controlled by electronic access systems (e.g., key cards, biometrics).
- Access is granted on a need-to-enter basis, logged, and regularly reviewed.
- Visitors must be escorted at all times and recorded in visitor logs.

7. Asset Management

All information assets—hardware, software, systems, and data—must be inventoried, owned, and tracked.

- Each asset has a designated owner responsible for its classification, protection, and appropriate use.
- Mobile devices and portable media must be encrypted and physically secured.
- Data stored on third-party systems (e.g., cloud providers) must comply with equivalent controls and oversight.

8. Cryptographic Controls

- Sensitive data must be encrypted at rest and in transit using approved cryptographic algorithms and key lengths.
- Encryption keys must be managed securely, with key rotation and revocation processes in place.
- Digital certificates and secure communications protocols (e.g., TLS) must be used for system interfaces and transactions.

9. Secure System Development and Maintenance

- All system development activities must follow secure coding practices.
- Security requirements must be embedded in the software development lifecycle (SDLC).
- Regular security testing (e.g., code review, static analysis, penetration testing) must be conducted.
- Changes to production systems must go through a documented change control process including security review.

10. Supplier and Third-Party Security

All third-party service providers must:

- Undergo security due diligence prior to onboarding.
- Sign agreements outlining security, confidentiality, and compliance obligations.
- Be subject to ongoing performance and compliance monitoring, including periodic audits.

Cloud and hosting providers must meet equivalent security standards and ensure data is stored in jurisdictions acceptable to applicable regulatory bodies.

11. Logging, Monitoring, and Audit

- System and user activity logs must be maintained for key systems and protected against tampering.
- Logs must be regularly reviewed for anomalous behavior, unauthorized access attempts, and operational issues.
- Automated alerting and Security Information and Event Management (SIEM) tools must be used for real-time threat detection.

Audit trails shall support forensic investigation and compliance verification.

12. Physical and Environmental Security

- Access to facilities and server rooms must be controlled and monitored using badge systems, biometrics, or equivalent controls.
- Environmental controls (e.g., fire suppression, temperature monitoring) must be in place in critical infrastructure areas.
- Visitors must be logged, supervised, and restricted from sensitive areas.

13. Business Continuity and Disaster Recovery

- The organization must maintain business continuity and disaster recovery plans to ensure resilience of critical functions.
- Recovery objectives (RTO/RPO) must be defined and tested at least annually or as stipulated in the Business Continuity and Disaster Recovery document.
- Backups must be performed regularly, encrypted, tested for integrity, and stored securely offsite or in resilient cloud services.

14. Human Resource Security

- Background checks must be conducted where permitted by law, especially for roles with access to sensitive data.
- Security obligations must be communicated during onboarding and reinforced through periodic training.
- Upon termination or role change, access rights must be immediately revoked and assets returned.

15. Information Security Awareness and Training

- All users must complete security awareness training annually.
- Specialized training must be provided for staff in technical, compliance, and operational risk roles.
- Simulated phishing campaigns or incident response drills should be conducted periodically to assess user readiness.

16. Incident Management

- All security incidents must be reported promptly using the designated incident response process.
- An incident response team is responsible for investigation, containment, communication, and recovery.
- Post-incident reviews must be conducted to assess root causes and implement corrective actions.
- Certain incidents may require notification to external authorities or affected stakeholders in line with legal requirements.

17. Compliance

The organization is committed to complying with all applicable data protection laws, gaming regulations, financial service rules, cybersecurity directives, and industry best practices. This includes:

- Ensuring the protection of player data and transaction integrity
- Maintaining system logs and audit trails as required
- Adhering to technical security requirements as mandated by relevant supervisory bodies

Failure to comply with this policy may lead to disciplinary action, contract termination, or legal proceedings.

18. Roles and Responsibilities

<i>Role</i>	<i>Responsibilities</i>
Information Security Officer	Oversees the development, implementation, and maintenance of the information security program.
Management	Ensures that employees understand and comply with the information security policy and procedures.
Employees	Adhere to all information security policies and report any suspected security incidents.

19. Policy Review and Maintenance

This policy shall be reviewed at least annually or upon significant changes to:

- Business operations
- Legal or regulatory requirements
- Security threats or vulnerabilities

The owner of this document is the Chief Information Security Officer. All changes will be documented, approved, and communicated to relevant stakeholders.