

Information Security Policy

Cyber Labs B.V.

Document Control

Version	Date	Description of Changes	Author
1.0	01.09.2025	Initial draft	IGA Trust B.V.

1. Objective

This policy sets forth a structured and unified approach to safeguarding the organization's information assets from both internal vulnerabilities and external threats. It establishes guiding principles, assigns responsibilities, and outlines essential security measures required to protect both digital and physical resources. The overarching aim is to ensure operational continuity, regulatory adherence, and the confidentiality, integrity, and availability of all information systems.

2. Applicability

This policy governs all individuals and entities interacting with the organization's information systems. It includes employees, contractors, consultants, vendors, and any third parties involved in accessing, processing, managing, or storing organizational data. Its reach extends to all forms of information—whether digital, physical, or spoken—and applies across all platforms, including on-premises infrastructure, cloud environments, and mobile technologies.

3. Information Security Governance

Information security is managed at the highest levels and integrated throughout the organization's functions—operational, technical, and administrative. Executive leadership determines the strategic direction and allocates appropriate resources. The Chief Information Security Officer (CISO) holds the authority to implement this policy, conduct risk analyses, and coordinate audits. Departmental managers are expected to enforce compliance within their respective teams. Every individual within the organization is accountable for protecting information and must promptly report suspected incidents or breaches.

4. Risk Governance

The organization follows a formal, documented process for identifying and managing information security risks. This includes:

- Performing risk assessments at regular intervals to identify potential threats and prioritize them based on likelihood and impact.
- Evaluating how risks may influence operational effectiveness, legal obligations, and public trust.
- Applying appropriate mitigation or acceptance strategies depending on established risk thresholds.
- Keeping the risk register and associated controls up to date to reflect emerging threats and organizational changes.

5. Classification and Handling of Information

All information must be categorized based on its level of sensitivity and value to the organization. Handling procedures are dictated by this classification:

- **Public:** Accessible to anyone with no risk of harm.
- **Internal Use:** Limited to authorized staff within the organization.
- **Confidential:** Sensitive data that requires restricted internal access.
- **Highly Confidential / Restricted:** Information of critical importance, such as personal identifiers, financial records, or architectural blueprints, which must be tightly controlled and encrypted.

Information should be labeled accordingly and protected through all stages of its lifecycle—from creation and storage to transmission and destruction.

6. Access Governance

Access to information is tightly controlled and based on core security principles:

Fundamental Principles

- **Least Privilege:** Users receive only the access necessary to perform their duties.
- **Need-to-Know:** Access is limited to those with a justifiable business purpose.
- **Separation of Duties:** Responsibilities are distributed to prevent abuse or fraud.

Authorization Process

Access must be granted through a formal request process, with approvals documented by the data or system owner. Higher-risk areas such as production systems and databases require additional authorization and activity logging. Temporary access is time-limited and revoked automatically once expired.

User Access Lifecycle

- **Onboarding:** New users are assigned access based on their role and department.
- **Role Transitions:** Access permissions are adjusted when roles change.
- **Termination:** Upon departure, all access—including email, systems, and physical premises—is immediately revoked.
- **Periodic Review:** At least once every quarter, user access is audited to verify appropriateness and detect over-permissioned accounts.

Authentication Standards

Systems must enforce secure authentication through:

- Unique identifiers and strong passwords
- Multi-factor authentication (MFA) for sensitive or remote access

Passwords must be at least 12 characters long, complex, rotated every 90 days, and restricted from reuse within a defined range of prior versions.

Privileged Access Controls

Accounts with elevated privileges (e.g., system administrators, DBAs) must be distinct from general user accounts, continuously monitored, and automatically logged out when inactive. Access must be justified, limited to essential personnel, and reviewed monthly.

System-Level Controls

- Session timeouts and automatic lockouts must be enforced.
- All access must be logged and auditable.
- Remote access must occur via encrypted, secure methods.
- Segregation must be maintained between live, development, and test environments.

Physical Entry Controls

Access to high-security areas like server rooms must be regulated through mechanisms such as key cards or biometric authentication. Entry is granted only when necessary, recorded in logs, and reviewed regularly. Visitors must be accompanied at all times.

7. Asset Oversight

Every piece of hardware, software, data, or system is recorded and assigned an owner responsible for its classification and safeguarding. Mobile devices and removable media must be secured both physically and cryptographically. Data handled by third-party providers must adhere to equivalent security controls.

8. Data Encryption Standards

Confidential data must be encrypted both when stored and during transmission, using approved algorithms and key lengths. Key management processes must include secure storage, regular rotation, and revocation mechanisms. Secure protocols such as TLS and valid digital certificates must be used for all interfaces and data exchanges.

9. Secure Development Practices

Security must be embedded into the software development lifecycle (SDLC). Developers must follow secure coding standards, and all changes to production systems must be approved through a change control process that includes security reviews. Security testing—such as code reviews, vulnerability scans, and penetration testing—must be routinely conducted.

10. Third-Party Risk Management

Any external provider must undergo a formal vetting process prior to engagement. Contracts must explicitly define security and confidentiality expectations. Performance and compliance are continuously monitored and audited. Cloud vendors must adhere to similar standards and ensure data remains within acceptable jurisdictions.

11. Logging and Monitoring

Critical systems must log user and system activity, and logs must be protected against unauthorized modification. These logs must be routinely reviewed to identify anomalies or unauthorized access attempts. Real-time detection systems such as SIEM tools should generate alerts to support rapid response. Audit trails must be detailed enough to support forensic analysis and compliance obligations.

12. Facility and Environmental Controls

Physical access to sensitive infrastructure must be regulated through electronic controls like badges and biometrics. Environmental safeguards—such as fire suppression and climate regulation—are essential in critical areas. Visitor access must be controlled, supervised, and documented.

13. Business Continuity and Disaster Preparedness

The organization maintains and tests comprehensive business continuity and disaster recovery plans. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) must be clearly defined. Backups are encrypted, regularly tested for integrity, and stored securely offsite or on resilient cloud platforms.

14. Personnel Security Measures

Where permitted by law, background screening is conducted—particularly for roles involving sensitive data access. Security responsibilities are communicated during onboarding and reinforced through periodic

training. Upon exit or role change, access is immediately terminated and all organizational property must be returned.

15. Security Training and Awareness

All personnel must complete annual security awareness training. Employees in specialized roles (e.g., technical or compliance teams) receive additional, tailored instruction. Simulated cyberattacks or incident response exercises may be run periodically to assess preparedness.

16. Incident Response Management

All suspected security breaches must be reported through official channels. The designated incident response team handles containment, investigation, communication, and recovery. Following an incident, a review is performed to determine root causes and introduce necessary safeguards. Where required by law, regulatory authorities or affected parties must be notified.

17. Legal and Regulatory Compliance

The organization commits to full compliance with relevant data protection regulations, industry cybersecurity standards, and licensing authority rules, including those specific to gaming and financial services. This encompasses:

- Protection of player and customer data
- Maintenance of logs and system auditability
- Conformance to mandated technical security requirements

Non-compliance may result in disciplinary action, termination of contracts, or legal consequences.

18. Defined Roles

Role	Responsibility
Chief Information Security Officer	Oversees the entire information security framework and ensures ongoing alignment with business objectives.
Management	Promotes adherence to security procedures within their teams.
Employees	Follow security guidelines and report suspicious activities.

19. Policy Maintenance

This policy will be reviewed annually or whenever significant changes occur in operations, legal frameworks, or threat environments. The CISO holds responsibility for maintaining this document. Any revisions must be documented, approved, and distributed to all relevant stakeholders.