

INFORMATION SECURITY POLICY

Table of Contents

INFORMATION SECURITY POLICY	1
VERSION CONTROL	3
1. Purpose and Scope	4
2. Objectives of Information Security	4
3. Core Areas of Security Implementation	4
4. Protection of Personal Data	5
5. Identification of Threats	5
Threat Sources (Where the risk comes from)	5
Threat Vectors (How the threats happen)	5
6. Core Technical Principles	6
7. Information Security Risk Management	6
8. Access Rights Management	6
9. Secure Software Development Practices	7
10. Technical Security Testing	7
11. Handling Security Incidents	8
12. Collaboration with Third Parties	8
13. Policy Review and Governance	8

VERSION CONTROL

VERSION NUMBER	DATE	APPROVED BY
1.0	22.06.2026	Director

1. Purpose and Scope

1.1. The Company recognizes the operational value of information shared by its business clients, personnel, founders, counterparties, and stakeholders, and implements reasonable protections to safeguard it. Information security and cybersecurity are core components of daily operations and are critical to maintaining the trust of clients and partners. Information Security focuses on protecting the confidentiality, integrity, and availability of data.

1.2. This Policy defines the formal security goals of the Company and serves as the governing framework for all internal processes, technical procedures, and operational rules.

1.3. Kahuna B.V. (hereinafter also the “Company”) operates strictly as a Business-to-Business (B2B) gaming software provider. Direct B2C operational functions - are managed by the Company’s B2C operator clients and fall outside the direct operational scope of Kahuna B.V.

1.4. This Policy is the primary directive establishing the framework used to secure the operational workflows and information assets of **Kahuna B.V.** (the "Company"). It serves as a formal declaration of Management's commitment to supporting security principles across the organization.

Adherence to these mandates is mandatory for all internal employees and any external individuals handling Company information under contract.

2. Objectives of Information Security

2.1. The Company treats the protection of information assets used across its business divisions as a key strategic objective. This includes securing the data and personal information of business clients, partners, staff, and any entities interacting legally with the Company. Safely delivering B2B services and platforms while protecting client data is a fundamental principle.

2.2. This objective is maintained through:

- Managerial oversight and governance of security processes;
- Conducting regular security risk assessments and managing identified threats;
- Allocating necessary budgets and human resources;
- Performing periodic internal security assessments;
- Implementing applicable statutory requirements for data protection, etc.

3. Core Areas of Security Implementation

The Company maintains an active, ongoing security program to meet legal requirements and industry benchmarks through the following core activities:

- **Security Planning:** Regular planning and implementing security measures.
- **Rule Enforcement:** Setting clear organizational security rules and checking that everyone follows them.
- **Access Control:** Managing user accounts and blocking unauthorized people from logging in.
- **Threat Defense:** Using software defenses to stop hacker attacks and block malware or viruses.
- **Data Encryption:** Using cryptographic tools to encrypt sensitive information whenever necessary.
- **System Reliability:** Ensuring corporate networks and systems are resilient and remain up and running without unexpected downtime.
- **Technical Certification:** Maintaining direct regulatory responsibility for obtaining and renewing technical certifications for all the software components subject to certification requirements.

4. Protection of Personal Data

4.1. The Company prioritizes the protection of personal data and privacy-related information belonging to employees, client representatives, partners, and counterparties.

4.2. Security considerations must be factored into the design, deployment, and modification of any corporate system or workflow that processes personal data.

5. Identification of Threats

5.1. Information assets are protected through synchronized legal, organizational, and technical controls designed to prevent security incidents and manage risk.

The Company maintains appropriate processes and inventory records to identify and track corporate hardware and software assets supporting its operations.

Operational assets are monitored and updated periodically to ensure systems remain supported, secure, and aligned with operational needs.

Threat Sources (Where the risk comes from)

Potential security risks to the Company originate from three main areas:

- **Human Errors:** Internal mistakes made by employees due to a lack of training or accidentally failing to follow security procedures.

- **Adversarial Actions:** Intentional attacks from external parties, such as hackers, fraudsters, and malicious software developers.
- **Environmental Factors:** Uncontrollable events, including physical hardware breakages, system utility failures, or natural disasters.

Threat Vectors (How the threats happen)

The Company actively monitors and defends against the specific ways an environment can be compromised, including:

- **Data Leaks:** Sensitive corporate or customer information being exposed or stolen.
- **Unauthorized Entry:** Unapproved individuals gaining access to corporate accounts, networks, or systems.
- **Malicious Software:** Structural infections from malware, viruses, ransomware, or spyware.
- **Deceptive Scams:** Targeted phishing emails or spam meant to trick employees into giving away credentials.
- **Network Interruption:** Cyber-attacks like Denial of Service (DoS) that purposefully slow down or crash company platforms.
- **System Tampering:** Technical vulnerabilities such as remote exploits, false network routing, or unauthorized code changes.

Management acknowledges that materialized threats can cause financial and reputational harm. Minimizing these risks requires continuous vulnerability identification and remediation.

6. Core Technical Principles

All corporate architectures and user behaviors must align with these nine core concepts:

- **Identification:** Unique distinction of an individual or system asset.
- **Authorization:** Allocation of rights to perform specific operations.
- **Authentication:** Verification of a claimed identity.
- **Accountability:** Linking individual responsibility to specific system actions.
- **Business Necessity:** Restricting access permissions to verified business requirements.
- **Least Privilege:** Limiting active user rights to the minimum required for a role.
- **Separation of Duties:** Requiring multiple individuals for critical operations to prevent unilateral control.
- **Security Compliance:** Meeting all applicable legal and administrative security expectations.
- **Event Logging:** Maintaining clear records of user activity and system events.

7. Information Security Risk Management

7.1. The risk management framework consists of compiling asset inventories, mapping asset classifications, analyzing threats, and executing risk mitigation plans.

7.2. The technical asset scope covers:

- Physical assets, including facilities, corporate offices, and physical equipment.
- Software applications and proprietary systems.
- Operational network systems and technical services.
- Information assets and digital databases.
- Corporate personnel and contractors.

8. Access Rights Management

8.1. System credentials and permissions are granted strictly on the basis of business necessity and the principle of least privilege.

8.2. Access to corporate networks, applications, and endpoints must be managed in accordance with business and security requirements.

8.3. Provisioning access permissions requires the approval of the immediate supervisor and the asset owner, following verification that the requested rights match the user's role and policy mandates.

8.4. Users are responsible for assets accessed under their credentials and must use them solely for intended business operations.

8.5. Network access granted to external vendors must be strictly controlled and immediately revoked upon contract termination or expiration.

9. Secure Software Development Practices

9.1. Software engineering must follow secure development practices to prevent system component manipulation. Applications must be designed to protect core databases from malicious user inputs.

9.2. Production troubleshooting and maintenance are restricted to authorized technical staff. Servers must be configured to prevent the unauthorized execution of external or untrusted code.

9.3. Engineering teams must enforce strict environment separation across the application life cycle:

- Production, development, and testing environments must be logically segregated.
- Access to live production environments by development personnel must be controlled and require formal peer code reviews before deployment.

- Deployment controls must prevent unverified test code from entering production environments.
- The use of live production data or real personal data in testing or non-production environments is strictly prohibited.

10. Technical Security Testing

10.1. The Application Security Team is authorized to perform routine technical security evaluations and vulnerability scans within production environments.

10.2. Vulnerability assessments must utilize a combination of automated scanning tools and manual penetration testing techniques to locate system flaws.

10.3. Testing parameters must include all corporate network infrastructure layers, internal applications, and operating systems.

10.4. Assessments must include both authenticated (internal threat profile) and unauthenticated (external threat profile) testing to simulate diverse attack methods.

10.5. Vulnerability reports must be delivered directly to the technical service owners and development leads for immediate prioritization and remediation.

10.6. Technical testing frameworks and remediation timelines must align with relevant industry standard benchmarks and compliance regulations.

10.7. If a technical incident or service interruption impacts B2C partner operations, the Company will notify the affected B2C operators without delay to ensure operational transparency and compliance.

11. Handling Security Incidents

11.1. Confirmed policy violations and security anomalies must be documented, investigated, and contained using formal response procedures.

11.2. System incidents may be identified via employee escalation paths or flagged automatically by corporate security monitoring tools.

11.3. Executive management establishes clear operational rules for reporting, registering, and tracking security incidents.

11.4. Every verified security incident must be investigated, and the formal root-cause findings must be recorded to prevent reoccurrence.

12. Collaboration with Third Parties

12.1. All agreements and contracts with third-party service providers that require access to, processing, or management of the Company's data or systems must include formal provisions for confidential information and data protection. These contractual requirements ensure that vendors implement necessary safeguards and comply with applicable security regulations.

12.2. To maintain a consistent level of security, the Company periodically monitors and reviews the services provided by third-party partners to check compliance with agreed security protocols and identify potential risks.

12.3. Any changes involving third-party service providers must be managed systematically to maintain and improve existing security policies and controls against evolving threats.

13. Policy Review and Governance

13.1. To ensure this Policy remains effective, up to date, and aligned with evolving operational and legal requirements, Management will formally review and, if necessary, update this document at least once per calendar year, or sooner if significant technical or organizational changes occur.

13.2. Management commits to allocating the necessary tools, budgets, and personnel required to maintain these security standards and meet the objectives outlined in this Policy.