

Information Security Policy

Galaktika N.V.

Version Control

V. 1.0 – 2026.23.06 - Galaktika N.V. - Policy creation

Version Control	2
1. General Provisions	4
2. Purpose and Objectives	4
3. Goals and Objectives of the Information Security	4
4. Main Directions of Information Security Provision	5
5. Use of Information Protection Measures	6
6. Personal Data Protection	6
7. Information Security Threats	6
8. Principles of Information Security Provision	7
9. Information Security Risk Management	8
10. Personnel Management Processes	8
11. Access Management	9
12. Secure Software Development	9
13. Security Testing and Vulnerability Assessments	10
14. Information Security Incidents	11
15. Information classification	11
16. Collaboration with Third Parties	12
17. Responsibility	12

1. General Provisions

1.1. The Company acknowledges the critical importance of the information entrusted to it by its clients, employees, founders, and business partners. Protecting such information is a fundamental business responsibility, and the Company is committed to implementing appropriate safeguards to prevent unauthorized access, disclosure, alteration, or loss. Effective information security and cybersecurity practices form an essential part of the Company's operations and contribute to maintaining the confidence and trust of its stakeholders.

Information security is focused on preserving the confidentiality, integrity, and availability of information assets. Cybersecurity constitutes a key element of information security and encompasses the measures, controls, and technologies established to protect systems, networks, applications, and services from cyber threats and malicious activities.

1.2. This Policy establishes the Company's overarching information security objectives and principles. It serves as the governing framework for the development, implementation, and maintenance of all information security-related processes, procedures, standards, controls, and internal documentation adopted by the Company.

2. Purpose and Objectives

2.1. This Policy serves as the primary framework document governing information security within Galaktika N.V. (hereinafter referred to as the "Company"). It establishes the core principles and methodologies applied to protect the Company's information assets and business operations. Furthermore, this Policy reflects the commitment of the Company's Management to actively support, maintain, and promote information security initiatives and related governance processes across the organization.

2.2. All employees of the Company, as well as individuals handling the Company's information pursuant to contractual obligations, are required to comply with this Policy.

3. Goals and Objectives of the Information Security

3.1. The Company regards the protection of information assets utilized within its business operations as a strategic priority. This includes safeguarding information and/or personal data relating to customers, partners, employees, and any natural or legal persons engaged in contractual, business, or other forms of interaction with the Company. The security of players' data and the reliable provision of Platform services constitute fundamental principles of the Company's operations.

3.2. The Company pursues this objective through the following measures:

- Active participation of top management in the oversight and governance of information security activities.
- Performance of information security risk assessments.
- Identification, evaluation, and management of information security risks.
- Allocation of appropriate resources to support information security processes.
- Regular internal reviews and assessments of information security controls and practices.
- Implementation of applicable legal and regulatory requirements relating to information protection.
- Adherence to relevant national and international standards and requirements.

4. Main Directions of Information Security Provision

The Company ensures information security in accordance with applicable information protection laws, regulatory requirements, and relevant national and international standards. To achieve and maintain an appropriate level of protection, the Company focuses on the following key areas:

- Planning and implementing information security controls and protective measures.
- Establishing organizational security requirements and monitoring compliance with such requirements.
- Applying functional security controls within business processes and information systems.
- Managing access rights and preventing unauthorized access to information and systems.
- Protecting information assets against attacks, malicious activities, and malware.
- Utilizing cryptographic protection measures where appropriate and necessary.
- Maintaining the resilience, stability, and reliability of information systems.

5. Use of Information Protection Measures

5.1. The Company applies information protection measures that are appropriate to the nature of the information being protected and are implemented in accordance with applicable legal and regulatory requirements.

5.2. All information protection measures adopted by the Company shall possess the parameters and characteristics necessary to satisfy the applicable information security requirements.

6. Personal Data Protection

6.1. The Company attaches particular importance to safeguarding the personal data and privacy-related information of its players and employees.

6.2. Information security requirements shall be taken into account throughout the design, implementation, and modification of systems and services that process personal data to ensure that the required level of security is maintained.

7. Information Security Threats

7.1. To protect its information assets, the Company employs measures intended to:

- Maintain the confidentiality, integrity, and availability of information through legal, organizational, and technical safeguards.
- Detect potential threats and vulnerabilities, perform risk analysis and assessment activities, and prevent the occurrence of information security incidents.

7.2. Information security threats may originate from the following sources:

- Mistakes or omissions by employees resulting from inadequate awareness or failure to comply with established procedures.
- Technical and social factors of a harmful nature, including malware, cyber-attacks, and fraudulent actions.
- Natural and human-induced events capable of adversely affecting information systems and information assets.

7.3. The most common information security threats include:

Unauthorized access to information or systems.

- Hacker activity and cyber-attacks.
- Phishing attempts.
- Malicious software.
- Spyware.

- Targeted attacks.
- Denial of Service (DoS) attacks.
- Leakage of information.
- Failures affecting supporting infrastructure.
- Spam-related threats.

7.4. Threats directed at information systems may include:

- Remote unauthorized access to systems.
- Impacts caused by software or mathematical manipulation.
- Unauthorized access to operational environments.
- Transmission of false routing data.
- Abnormal system operation.
- Impersonation or substitution of trusted network objects.

7.5. The occurrence of information security threats may adversely affect the Company and result in financial losses, reputational damage, or other negative consequences. Risk exposure may be reduced through the identification of vulnerabilities and the implementation of measures to eliminate or mitigate them.

8. Principles of Information Security Provision

The Company's information security framework is based on the following principles:

- **Business Necessity** – granting access to information solely where justified by legitimate business requirements.
- **Identification** – ensuring the unique identification of individuals, users, or systems.
- **Authentication** – confirming the identity and authenticity of users seeking access to information resources.
- **Least Privilege** – restricting access rights to the minimum level required for the performance of assigned duties.
- **Authorization** – assigning permissions and access rights necessary to perform specific actions.
- **Accountability** – establishing individual responsibility for the use, access, and handling of information and information systems.

- **Security Obligations** – ensuring adherence to established information security requirements and controls.
- **Segregation of Duties** – distributing critical functions and responsibilities among multiple individuals to reduce risk.
- **Event Logging** – maintaining records of user activities and information security events for monitoring and audit purposes.

9. Information Security Risk Management

9.1. The Company's information security risk management process includes the identification and classification of assets, as well as the identification, analysis, evaluation, and treatment of information security risks.

9.2. Assets subject to risk management may be categorized as follows:

- Information assets.
- Physical assets, including premises and equipment.
- Software assets.
- Personnel.
- Service and system assets.

9.3. The Company may apply one or more of the following risk treatment strategies:

- Reducing the risk.
- Accepting the risk.
- Transferring the risk.
- Avoiding the risk.

10. Personnel Management Processes

10.1. In the course of personnel management activities, the Company pursues the following key objectives:

- Recruiting personnel with the qualifications and competencies necessary to perform their assigned responsibilities.

- Assessing the reliability and suitability of employees.
- Ensuring that personnel are informed of applicable information security requirements and obligations.
- Promoting and maintaining information security awareness among personnel.

11. Access Management

11.1. Access rights shall be granted in accordance with the principles of business necessity and least privilege.

11.2. Access to the Company's information, systems, services, and networks shall be managed and controlled with due regard to operational requirements and information security considerations.

11.3. The granting of access constitutes authorization to use the Company's information, systems, services, and/or network resources. Access approval shall include authorization by the requestor's immediate supervisor and the relevant asset owner, together with verification that the requested level of access is appropriate for business purposes and consistent with the requirements of this Policy.

11.4. Users granted access to a specific asset shall use such access solely for its authorized and intended purpose.

11.5. Access rights assigned to third-party service providers shall be subject to strict control measures and shall be revoked without undue delay upon the expiration or termination of the relevant contractual relationship.

12. Secure Software Development

12.1. Software development activities shall follow secure coding principles intended to reduce the risk of unauthorized modification, misuse, or compromise of system components. Applications shall be designed and implemented in a manner that protects databases and other critical assets from unintended actions or malicious programming attempts initiated by users.

12.2. System maintenance and application troubleshooting may only be performed by personnel who have been granted the appropriate authorization and access rights. Appropriate safeguards shall be implemented to protect servers from the unauthorized execution of mobile or externally introduced code and to maintain the integrity and reliability of systems.

12.3. To support the security and integrity of software development throughout its lifecycle, the Company shall implement measures including, but not limited to, the following:

- Prohibition of the use of raw production data within testing environments.
- Verification and validation procedures for software releases to prevent test code or unauthorized changes from being introduced into production environments.
- Controlled and authorized access to production environments for development personnel, ensuring that software changes are subject to appropriate review and approval prior to deployment.
- Separation of development, testing, and production environments, where technically feasible, to prevent unauthorized interactions between environments.

13. Security Testing and Vulnerability Assessments

13.1. The Company conducts periodic technical security testing and vulnerability assessments within production environments to identify, evaluate, and remediate potential security weaknesses. Such activities are carried out by the Application Security Team.

13.2. Security testing and vulnerability assessment activities utilize various techniques, including vulnerability analysis and simulated attack scenarios, to identify existing threats and potential weaknesses within the Company's infrastructure.

13.3. Assessments are performed across all relevant components of the environment, including applications, operating systems, and network infrastructure.

13.4. The Company applies both authenticated and unauthenticated testing approaches to simulate different attack scenarios, including attempts to gain access to systems under varying levels of privilege.

13.5. Findings identified during testing activities shall be reviewed and analyzed by technical service owners and developers and used to strengthen existing security controls and protective measures.

13.6. Testing activities are conducted in accordance with applicable industry standards and regulatory requirements to support compliance with established security expectations and benchmarks.

14. Information Security Incidents

14.1. Information security violations shall be subject to investigation, documentation, and the implementation of appropriate response measures.

14.2. Information security incidents may be identified through employee observations or by automated monitoring and detection systems.

14.3. The Company maintains established procedures governing the reporting, monitoring, and recording of information security incidents.

14.4. Each information security incident shall be investigated, and the outcome of the investigation shall be documented and retained.

15. Information classification

15.1. Some types of information are more sensitive than others. The classification of the information determines how it shall be handled. There are four levels of information:

- **Restricted** – Information of the highest sensitivity level that may result in significant harm to the Company or affected individuals if disclosed without authorization. Examples include financial information such as profit and loss statements, revenue and expenditure records, budget information, and sensitive customer information, including payment card data.
- **Confidential** – Information intended for access by a limited group of authorized individuals. Unauthorized disclosure may adversely affect the Company, its employees, customers, or other stakeholders. Examples include employee records, internal project documentation, operational information, player activity and behavioural data, game-related information, and compliance or regulatory records.
- **Internal** – Information intended solely for internal business purposes and not for public disclosure. Unauthorized access would generally not result in significant harm. Examples include internal policies, procedures, aggregated business information, and similar internal-use materials.
- **Public** – Information approved for public distribution and disclosure, the release of which presents no material risk to the Company. Examples include press releases, marketing materials, and publicly available communications.

15.2. Information classification decisions shall take into consideration the following factors:

- Applicable legal and regulatory obligations, including relevant requirements under GDPR, PCI DSS, and other applicable frameworks.
- The potential business impact arising from unauthorized disclosure, alteration, misuse, or loss of information.
- Input and guidance provided by the designated information owner or other individuals responsible for the information

16. Collaboration with Third Parties

16.1. Agreements with third-party service providers that involve access to, processing of, communication with, or management of the Company's systems or system components shall include applicable information security requirements. Such agreements shall address compliance with the Company's security policies, the implementation of appropriate security measures, and adherence to relevant legal and regulatory obligations.

16.2. To ensure that an appropriate level of security is maintained, the Company may periodically monitor and review services provided by third-party partners. Such reviews may include assessments of performance against agreed requirements, verification of compliance with security obligations, and evaluation of potential risks and vulnerabilities.

16.3. Changes affecting the supply chain and third-party service providers shall be managed in a structured manner. The Company shall maintain and, where necessary, enhance its security policies, procedures, and controls to address emerging threats, risks, and vulnerabilities.

16.4. Requirements relating to the management of third-party access are further addressed within the Company's Access Management Policy.

17. Responsibility

17.1. The Company's Management is responsible for the implementation, maintenance, and periodic review of this Policy.

17.2. The Company's Management is committed to undertaking all relevant actions and measures necessary to achieve the Company's information security objectives.