

Gareton B.V.
Information Security Policy

Version Control

V. 1.0 – 2025.13.11 – Gareton B.V. - Policy creation

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

1. General Provisions

1.1. The Company recognizes the importance of information entrusted to it by clients, employees, founders, and counterparties, and takes all possible measures to protect it. Information security and cybersecurity are integral components of the Company's business and essential for maintaining client trust.

Information security ensures the confidentiality, integrity, and availability of information. Cybersecurity is a component of information security aimed at creating and implementing measures to protect systems, services, networks, and applications from cyber-attacks.

1.2. This Policy defines the Company's goals and objectives in ensuring information security and serves as the foundation for all related processes, procedures, rules, and documents within the Company.

2. Purpose and Objectives

2.1. This policy is the main document defining the principles and approaches to ensure the security of the business processes and information assets of the Alfa Entretenimento (hereinafter – the Company) as well as declaring the willingness of the Company's Management to support the principles and processes of information security.

2.2. Compliance with this Policy is mandatory for all employees and individuals working with the Company's information under contractual obligations.

3. Goals and Objectives of the Information Security

3.1. The Company considers one of its strategic tasks to ensure the protection of information assets involved in any business processes of the Company's divisions, as well as information and / or personal data of customers, partners, and employees, any legal and physical persons who are in legal relations or other types of interaction with the Company. Players' data safety and secure Platform services provision are the Company's primary principles.

3.2. This goal is achieved by:

- Involving top management in managing information security processes.
- Conducting risk assessments.
- Managing information security risks.
- Providing necessary resources for information security processes.
- Conducting internal evaluations of information security.
- Implementing legal requirements in information protection.

- Ensuring compliance with applicable national and international standards.

4. Main Directions of Information Security Provision

The Company implements information security based on legal norms for information protection following national and international applicable standards as well as by:

- Planning and implementing information security measures.
- Enforcing organizational security requirements and monitoring compliance.
- Implementing functional security requirements.
- Managing access and controlling unauthorized access.
- Preventing attacks and malware infiltration.
- Using cryptographic protection when necessary.
- Ensuring the resilience and reliability of information systems.

5. Use of Information Protection Measures

5.1. The Company uses appropriate measures in line with legal and regulatory requirements when protecting information.

5.2. The parameters and characteristics of protection measures must meet the necessary security requirements.

6. Personal Data Protection

6.1. The Company places special emphasis on protecting the personal data and privacy information of players and employees.

6.2. Information Security must be considered in designing, implementing, or changing systems and services that process personal data to ensure compliance with security requirements.

7. Information Security Threats

7.1. The Company protects information by:

- Implementing legal, organizational, and technical measures to ensure confidentiality, integrity, and availability.
- Identifying potential threats and vulnerabilities, analyzing and assessing risks, and preventing incidents.

7.2. **Threat Sources:**

- Employee errors due to lack of knowledge or failure to follow procedures.

- Technical and social negative factors (e.g., malware, hacking, fraud).
- Natural and man-made negative factors.

7.3. Common Threats:

- Information leaks.
- Unauthorized access.
- Malware.
- Hacker attacks.
- Denial of Service (DoS) attacks.
- Targeted attacks.
- Spam.
- Phishing.
- Spyware.
- Infrastructure failures.

7.4. Specific Threats to Systems:

- Abnormal operating modes.
- Unauthorized access to operating environments.
- Remote unauthorized access.
- Substitution of trusted network objects.
- Routing false information.
- Software and mathematical impacts.

7.5. Threat realization can cause damage to the Company, including financial losses and reputational harm. Reducing risk likelihood involves identifying and addressing vulnerabilities.

8. Principles of Information Security Provision

- **Identification:** Uniquely distinguishing individuals or systems.
- **Authorization:** Granting rights to perform specific actions.
- **Authentication:** Verifying user authenticity.
- **Accountability:** Individual responsibility for access and handling of information.
- **Business Necessity:** Access based on business needs.
- **Least Privilege:** Limiting access rights to the minimum necessary.
- **Segregation of Duties:** Requiring multiple people for critical tasks.
- **Security Obligations:** Compliance with security requirements.
- **Event Logging:** Recording user actions and security events.

9. Information Security Risk Management

9.1. The Risk Management process includes inventorying and classifying assets, identifying, analyzing, assessing, and treating risks.

9.2. Asset Categories:

- Physical assets (premises, equipment).
- Software assets.
- Service/system assets.
- Information assets.
- Personnel.

9.3. Risk Treatment Strategies:

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

10. Personnel Management Processes

10.1. The main objectives of the Company in the process of working with personnel are:

- Hiring qualified personnel.
- Verifying employee reliability.
- Informing personnel about security requirements.
- Enhancing awareness.

11. Access Management

11.1. Access is granted based on business necessity and least privilege.

11.2. Access to the Company's information, systems, services, and/or network must be controlled, taking into account business and security requirements.

11.3. Obtaining access serves as authorization to use the Company's information, systems, services, and/or network and includes coordination with the initiator's immediate supervisor and the asset owner, as well as verification that the level of access provided aligns with business needs and the requirements of this Policy.

11.4. When a user is given access to a particular asset the user is only allowed to use the asset for the intended purpose.

11.5. Access rights granted to third-party service providers must be strictly controlled and removed promptly upon termination of contracts or agreements.

12. Secure Software Development

12.1. All software development must adhere to secure coding practices designed to prevent unauthorized manipulation of system components. Applications must

be structured to safeguard the database and other critical assets from any unintended or malicious programming activities initiated by users.

12.2. Only authorized personnel with appropriate access rights are permitted to perform system maintenance or application troubleshooting. Measures must be implemented to ensure that servers are adequately safeguarded against unauthorized execution of mobile or external code, preserving the integrity and reliability of the system.

12.3. To ensure the security and integrity of software development processes throughout the entire lifecycle the following measures should be implemented, but not be limited to:

- Separation of production, development, and testing environments where technically possible to prevent unauthorized connections.
- Controlled access mechanisms to production systems for development teams, ensuring that code changes are properly vetted before deployment.
- Rigorous verification processes for software deployment to prevent test code from entering production environments.
- The use of raw production data in testing environments is strictly prohibited.

13. Security Testing

13.1. Regular technical security tests / vulnerability assessments should be conducted in a production environment to identify and address potential vulnerabilities. These assessments are performed by the Application Security Team.

13.2. Security tests / vulnerability assessments employ a variety of methods, including simulated attacks and vulnerability analyses to identify both active threats and potential weaknesses in its infrastructure.

13.3. Security assessments cover all aspects of the system, including network infrastructure, applications, and operating systems.

13.4. The Company employs both authenticated and unauthenticated testing methodologies to simulate different types of potential attacks including attempts to access systems at various privilege levels.

13.5. Results from these tests should be carefully analyzed and used to enhance security measures by technical service owners and developers.

13.6. Testing procedures are aligned with industry standards and regulatory requirements, ensuring that the Company meets the necessary security benchmarks and approaches.

14. Information Security Incidents

14.1. Violations are investigated and documented with appropriate responses.

14.2. Incidents can be detected by employees or automated systems.

14.3. Procedures for incident reporting, monitoring, and registration are established.

14.4. Investigations are conducted for each incident, with results recorded.

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:

- **Public:** Information that can be freely shared with the public

/or/ Information that is intended for public disclosure and poses no risk if accessed by anyone.

Examples: press releases, marketing materials, etc.

- **Internal:** Information intended for internal use only

/or/ Information that is not intended for public release but whose unauthorized disclosure would not cause significant harm.

Examples: company policies and procedures, aggregated data, etc.

- **Confidential:** Sensitive information that requires limited access.

/or/ Information that is sensitive and intended for a specific group of individuals within the company. Unauthorized access could cause harm to the company or individuals.

Examples: Employee records, internal project documentation, operational data, player activity and behaviour, game data, compliance and regulatory data, etc.

- **Restricted:** Highly sensitive information that could cause severe damage if disclosed.

/or/ Highly sensitive information that, if disclosed without authorization, could have severe consequences for the company or individuals.

Examples: Financial data (profit and loss, revenue and expenses, budget statements), sensitive customer information (e.g., credit card data), etc.

15.2. Classification Criteria:

- **Legal and regulatory requirements:** Compliance with laws and regulations (GDPR, PCI DSS, etc.).
- **Business impact:** Potential impact on the business if the data is exposed or misused.
- **Data owner input:** Input from those responsible for the data.

16. Collaboration with Third Parties

16.1. All contracts with third-party service providers that involve access, processing, communication, or management of the Company's systems and their components must encompass all relevant security requirements. This includes stipulations that mandate adherence to our security policies, the implementation of necessary safeguards, and compliance with applicable regulations.

16.2. To maintain the appropriate level of security, a periodic monitoring and review process for services by third-party partners should be conducted. This process may involve evaluating their performance against agreed-upon metrics, assessing compliance with security protocols, and identifying any potential risks or vulnerabilities.

16.3. Changes in the supply chain related to third-party service providers must be managed systematically. This includes maintaining and enhancing existing security policies, procedures, and controls in response to evolving threats and vulnerabilities.

16.4. The access management approach for third parties is described in the Access Management Policy.

17. Responsibility

17.1. The Company's management is responsible for implementing and updating this Policy.

17.2. Management commits to taking all relevant measures to achieve the objectives of information security.