



games for business
the learning experience

Information Security Policy

Version: 1.0

Release date: 10/13/2025

Approved by: Miklós Szalai

Games for Business Kft.

INFORMATION SECURITY POLICY

Effective from: 13.10.2025

VERSION CONTROL

Version	Date	Chapter(s)	Reason and essence of modification
1.0	2025.10.13.	Full	Approval



INFORMATION SECURITY POLICY

The aim of the Information Security Policy is to fully formulate the managerial intention of Games for Business Kft., which is aimed at preserving the security of the data and information managed by the organization and the organization's IT systems.

Games for Business Kft. enforces the following security principles in the field of IT security:

- Confidentiality: information must be protected from unauthorized access or publication. It must be prevented from the acquisition of business secrets by competitors and the violation of the confidentiality of business information.
- Integrity: ensure that information is accurate, complete, and valid at all times in accordance with business values and expectations.
- Availability: ensure that the information needed for business processes is available now and in the future. The necessary resources must also be protected.
- Safety risk: in most cases, the risk must be reduced to a tolerable level by means of protective measures for threats representing a significant damage value.
- Completeness of protection: physical, logical and administrative protection must be enforced in the following three dimensions:
 - all system components,
 - all layers of system architecture, both at the level of IT infrastructure and applications,
 - the central and endpoint IT devices and their environment.
- Closedness of protection: above the risk value determined by the Company, all preventive protection measures against probable threats are implemented, and they form a regulated and organic whole as a whole.
- Risk-proportionality of protection: in order to meet the security objectives and IT security requirements, it must be ensured that adequate, reasonable, cost-effective, risk-proportionate protective measures and controls are applied, in accordance with the resources available at all times.
- Continuity of protection: the established security measures must be maintained without interruption even in the face of the constantly changing security environment and conditions.

The Company has designed, developed, operates and develops its information security management system taking into account the principles in order to ensure the closed, comprehensive and continuous protection of the data assets under its management, covering the entire life cycle of the systems in a closed, complete and continuous manner proportionate to the risks of threats endangering the confidentiality and availability of the elements of electronic information systems. logical, physical and administrative safeguards.



The management of the Company is committed to the protection of the organization's electronic information systems and the data stored therein as a priority task, and is committed to continuously providing the resources necessary for the implementation of IT security protection measures that are appropriate to the technological level of the age. Our company improves the level of security by developing control processes, regular control activities and integrating information security into processes.

The management of the Company is committed to the determination of the expectations regarding data management in accordance with the principles of information security, and to the implementation of modern and secure data management in accordance with the expectations. The organization takes into account the expectations regarding the quality and confidentiality of data, the regularity of data transfers and data security to a large extent, introduces protective measures to meet the expectations, and provides the necessary resources.

The Company's management, all its employees and contractual partners are responsible for complying with the information security principles and expectations regarding the data entrusted to their management, regularly educates on the principles and expectations, and protects the processed data in accordance with the expectations and principles.

Dated, 13.10.2025

Managing Director