



Information Security Policy

Information in all its forms (written, verbal, printed, stored on electrical mediums) represents main asset for work and therefore it has to be protected. Information and the assets that process/store/transfer the information (people, systems, equipment, premises) represent the information system of Net-Bit.

The General manager of Net-Bit is establishing this Information Security Policy for the management system that provides protection of the information system of Net-Bit from different threats (unauthorized access, computer fraud, espionage, hackers attack, viruses, and natural disasters – fire, flood, earthquakes etc).

The information security management system provides:

- Minimization of the impact of the threats
- Maximization of return on investments
- Business continuity
- Improved image of the company

The General manager of Net-Bit is directly responsible to provide clear and concrete support in the implementation of the Information Security Policy and to follow its implementation in the daily activities of the company, by appointing responsibilities, authorizations and appropriate organizational structure. For this purpose, the manager has appointed Information Security Officer and members for the security board. Their responsibilities and authorizations are defined in a separate document.

All the activities, measures and controls of the Net-Bit information security management system, are to provide the three aspects of the protection of the information:

- **Confidentiality** - protection from unauthorized access to information,
- **Integrity** - accuracy and completeness and
- **Availability** - authorized users will have access when needed.

In order to fulfill all those requirements, the information security management system of Net-Bit provides the following functions and activities:

- Compliance with ALL relevant regulatory and legal requirements, contractual requirements and those from the international standards. Special care is taken for compliance in regards to the local Law for Personal Data Protection and EU General Data Protection Regulation (GDPR).
- Education and awareness programs to all users of the information systems of Net-Bit, regarding the threats to the day to day working, the need for information protection, and how they contribute to the effectiveness of the management system.
- Performing regular checks on the access controls, after the status of an employee changes, according to the procedure for human resources
- Identifying and recording of all information assets and equipment, regular update of each change, in order to prevent unauthorized use, theft and damage of information assets.

- Risk analysis of the information assets and implementing risk treatment plan(s).
- Setting Classification Policy, to define the level of confidentiality, and rules for labeling, storing and use of the classified information in order to prevent misuse.
- Prevention of use of unauthorized and illegal equipment in the premises of the company and its systems. Special protection care is taken for the clients whose information assets are under control of Net-Bit, including the systems and assets that are accessed by the employees of Net-Bit.
- Implementing physical perimeter with additional access controls to protect information assets from unauthorized access
- Designed and implemented business continuity for the critical processes in case when the information systems are not available. Development and testing of continuity plans to assure the processes are back in operations in reasonable and accepted time period.
- Regular monitoring, notification and reporting of all events (human errors, defects, damages, security incidents or unauthorized activities) in order to identify areas for continual learning and improvements, and thus decreasing the consequences from the detected threats to the security of the information systems. The IS management system will be continually improved.
- Continual improvement of the management system.

In order to support this Policy, Net-Bit has defined additional policies and documents, procedures, manuals that are part of the information security management system. It is responsibility of all the employees to be informed, to respect and follow the instructions from the IS management system of Net-Bit. Every breach of those guidance represents direct threat to the security of the information, employees, clients, and company's reputation and those incidents will be further investigated and discipline actions will be implemented.

With the regular, and additionally requested internal and external audits, the company will check the compliance of the implemented controls against the local laws, international standards (ISO 27001, ISO27701, ISO 22301, ISO 20000) and provide continual improvement of the management system

Skopje, 28.05.2021

Net-Bit General manager