Framework Information Protection Policy within the Company Panteon Group®

Version 3.41

Koper, June 20th, 2018
FRAMEWORK INFORMATION PROTECTION POLICY WITHIN THE COMPANY Panteon Group® D.O.O.

1. PURPOSE

Company Panteon Group® d.o.o. is fully aware of the value of information and of information system. For the successful business operation of the company, secure and reliable information and information related assets are of utmost importance. For this purpose, the company is managing the information protection system, which is defining, by means of its applicable policies, by means of corresponding organization related regulations and by means of operation related instructions, how the information related assets have to be protected appropriately. By means of the Framework Information Protection Policy, the management is emphasizing its responsibility and commitment to the appropriate information related assets protection, while employees, contracted workers and all users of information and of information related systems are emphasizing their responsibility regarding the implementation of information protection policy of the Company Panteon Group®.

Objective of the information protection policy is to prevent or to mitigate the consequences of the security related incidents to the minimum possible extent and to ensure the uninterrupted business operation. Purpose of the information protection related policy is to determine the importance of information assets for the business operation of the Company and to protect them accordingly, in the sense of ensuring their confidentiality, integrity and availability.

- **Confidentiality**: to ensure the access to information to authorized persons only
- **Integrity**: protection of accurateness and of completeness of information by means of prevention of unauthorized modifications
- **Availability**: provision of access to the information and to related information assets to the authorized persons when they need these information and related information assets.

Information protection policy is defining protective measures and in accordance with security related sensitivity, with business value and with criticality of information, irrespective of the form in which information are making their appearance: in computers, on the paper or on the portable storage media and during their transmission through the network or at their oral transmission, respectively.

Due to increasingly emphasized dependency of the business operations on the information technology, the vulnerability regarding various external and internal threats is becoming more and more widespread, refined and effective at causing the business related damage to the company. Security related policy, in the form of security controls, is establishing the integral framework for the assurance of information and information system protection against threats, for instance errors, failures, disturbances, falsifications, sabotages, violations of confidentiality, interruptions of business operations, thefts and natural disasters.
2. Extent of information protection policy

Information protection related policies, instructions and procedures on the lower level are covering all business operation related processes for the assurance of information services provided by the Company Panteon Group®.

Information and information system protection related policy implemented by the Company Panteon Group® is encompassing all of 14 (fourteen) areas, as defined within the Standard ISO/IEC 27001:2013, containing 114 security related controls, i.e.:

1. **Information protection policy**
   Document regarding information protection policy, overview/verification of information protection policy

2. **Organization of information protection**
   Information protection management within the organization and management of the third parties access to the information technology related devices

3. **Protection in connection with the personnel**
   Appropriate verification of candidates for employment, Confidentiality Declaration, education/training of users regarding security related procedures and regarding correct use of information technology related equipment, termination of employment relationship management and responsibility related changes management, education concerning information security

4. **Information assets management**
   Identification of information systems owners, responsibilities regarding protection related measures, security related classification of information

5. **Control of access to information sources**
   Definition of ownership of rights and restrictions on access to information sources, network and IT sources. Ensuring the abolition of access rights, the use of user names, and rules for changing and selecting passwords, restrict access to servers, and use special controls to access source code

6. **Use of cryptography**
   Use of cryptography for data transfer and use of certificates for access to documents and applications

7. **Physical and environmental protection**
   Physical protection of secured areas against the unauthorized access, damage and disturbances, physical protection of the information technology, protection of the electrical installations and of cable network against security related risks and threats resulting from the environment

8. **Safety of operation**
   Establishment of responsibility and of procedures for operation and management of all computers and networks, planning and preparation for assurance of appropriate capabilities of the system, protection against harmful software, policy of production of backup data copies, protection within computer networks, data media protection management, data and software exchange management between organizations, control of information systems and recording of security related incidents

9. **Security of communications**
   Policy of access to systems, control of the allocation of the right of access to information systems and services, user responsibilities, control of access to the operating system, control of access to applications and information, management of the use of portable computer equipment and remote work, interconnection policy, data exchange policy with suppliers and customers.

10. **Purchasing, developing and maintaining the system**
Defining the security requirements of information systems, security controls in applications, the policy of using data encryption, handling access to system files and source programs, protecting the development and maintenance environment, managing vulnerabilities

11. Relationship with partners and customers.
Signing of a contract on information security with clients and partners, recording access to information resources

12. Security incidents management
Procedures regarding security related incidents reporting, management of security incidents related responsibilities and procedures

13. Uninterrupted business operations management
Development and maintenance of appropriate plans for fast recovery of important vital business processes in case of serious interruptions of business operations.

14. Compliance
Compliance with legal requirements, compliance with security related policies and technical compliance, consideration of systems audits.

3. General responsibility and responsibility for individual areas of information protection

Management of company is responsible for implementation of information protection system management, for follow-up and for monitoring of efficiency regarding protection related measures and procedures.

For consideration and implementation of individual security related measures and procedures all employees are responsible, however management of the company is responsible for the implementation of information protection related policy as the whole and for the assurance of required financial and human resources.

Management of the company defines and appoints the responsible person for the establishment, implementation and maintenance of processes that are required for the information protection system management in accordance with the Standard ISO/IEC 27001:2013. The tasks of a security manager are as follows:

- Monitoring of protection policy related documents at changes, as for instance security incidents, new vulnerabilities, changes in organizational and technical infrastructure
- At least once a year evaluate the security risks that threaten the company
- Preparation of plans concerning measures for improvement of information security status, based on the assessed security related risks, results of evaluations, reviews and tests
- Preparation of annual plan and program of internal security related evaluations
- Assurance of independent evaluation of elements of information protection system management
- Continuous improvement of information protection system management
- Follow up and evaluation of efficiency of information protection system management and reporting to the management regarding its performance and requirements for the improvement process
- Assurance of awareness of employees regarding information protection system management and regarding appropriate qualifications, enabling the employees to understand the information protection policy and protection related measures
- Communication with external customers regarding issues, referring to the information protection system management.

4. Responsibilities of employees at reporting security related incidents and security related deficiencies

All employees should be included into the process of improvement of information and of information assets security. Task of the security manager, is to acquaint appropriately all employees with security related requirements and controls and to enable them for the secure use of information technology assets.

Employees have to report observed security related incidents, for instance:

- Observed security related deficiencies
- Intentional and unintentional security related violations
- Incorrect or suspicious performance of systems or software respectively
- Malfunctions of systems
- Viruses
- Errors and failures
- Threats and vulnerabilities of systems and services
- All unplanned activities on systems that are not the part of the regular maintenance,

to the person being responsible for the information protection. Security related incidents have to be reported as soon as possible, orally, by phone (+386 40 435 058) or by e-mail to the address varnost@panteongroup.com, thus enabling the security manager to act appropriately as soon as possible.

The security manager has to collect, review, evaluate and analyze reports on security related incidents, to inform immediately the management, if needed, to react in time by appropriate measures or to coordinate required activities. The security manager is reporting in regular meetings of the security forum, and based on this report, security forum is deciding on required measures, in order to prevent recurrence of security related incidents. In case of suspicion of the violation of law, the employee which perceived the incident, has to inform the manager, being responsible for all subsequent procedures, including reporting to appropriate legal bodies.

Users of computer services are under no any condition allowed, to substantiate suspicions regarding deficiencies of information protection and on vulnerability of systems.
5. Explication of special security related measures

Information system related protection policies are available to employees in the whole in electronic form. Security related provisions that in continuance of this document, are representing key elements for security assurance:

- Clean desk and clean display policy
- Passwords management
- Policy of access to the system management
- Policy of software management
- Management of mobile computing equipment
- Use of Internet and of electronic mail on company's systems

6. Maintenance of security related policy

At changes of legislation, at occurrence of new threats, new security related incidents, changes of organizational or technical infrastructure, that may impact the protection of information and of information systems, the information protection system will be continuously adapted accordingly by means of implementation of new security related measures and procedures and by means of improvements of already existing security related measures and procedures. Dynamic adaptation of the security related policy, in accordance with business requirements and changes that influence the initial risk assessment, is the commitment of the security manager.

7. Management of information protection related documents

Information protection related documents are being published in electronic form, thus being available for the insight to all employees and to third parties, having the access to the company's information and information system. Each information protection related document must have the appointed custodian, being responsible for its timely updating and change and the person, being responsible and entitled for the approval of document. Names of both persons are to be written in the lower left hand corner of the document. In each document, also the effective date of this document has to be indicated.

Amendment or improvement of the document may be suggested by each employee in such a way that the proposal is being addressed to the custodian or to the security forum. As soon as documents have been changed and approved, they have to be published immediately and all employees of the company and those third parties which have to consider these changes at their work, have to be informed on all changes immediately.

8. Sanctions

Each failure to comply with rules of information protection related policy and with corresponding documents is being considered as the violation of the employment agreement and is being sanctified as such violation.