General Security Policy

Table of Content

1 Mission and objectives

XLAB d.o.o. is one of the leading providers of IT solutions in the region. Our focus is software development and research in the field of cloud computing and distributed systems.

Our goals are to create an environment for the development of high-quality and innovative technological products, to offer these products in the international market and to provide exceptional support to our customers.

2 Vision

The vision of XLAB is to bridge top academic knowledge with high-tech industry and, in turn, provide solutions for our most demanding customers. Our slogan is "Get IT done".

3 Information security policy

Confidentiality, integrity and availability of the data that XLAB manages are essential to the overall functioning of the company. Information security policy was thus adopted by the CEO together with other executive structures in our company to provide a framework which establishes appropriate levels of information security for all data and information technology systems.

The company's Information security policy includes a commitment to meet the demands regarding data management and provides the basis for a management review of the progress of set objectives. Information security policy is constantly reviewed according to current market trends and trends in the field of information security.

4 Purpose / Objective

The objective of the security policy is to ensure data confidentiality, availability and integrity, while being managed by the company. The information security policy is ISO / IEC 27001: 2013 standard compliant.

The goals of the security policy are:

- Improving the protection of all information in the company
- Increasing the information security awareness of all employees and other parties (including but not limited to students and third-party contractors) that have any contact with data managed by XLAB
- Ensuring continuous operation in case of a major incident or extraordinary event
- Establishing good practices of personal information protection

5 Responsibilities

All employees, contractors and students, who have any contact with information resources that are owned by the company, are responsible for the application of the security policy.

XLAB has the responsibility to provide all current and new employees, students and contractors with appropriate education and training ensuring accordance with information security standards. After training each person has to sign the **Confidentiality Statement**, which confirms that they have been acquainted with the security and other policies of XLAB and agree to adhere to them.

Depending on the sensitivity and confidentiality of the data involved in their work an employee or a contractor might be required to sign additional documents to ensure information security.

6 Leadership commitment

The leadership of the company commits to the Information Security Management System (hereinafter: ISMS) by:

- their own attitude towards clients, employees and the social environment
- emphasizing the importance of meeting the requirements of legislation
- defining and implementing the vision, strategic direction, strategies and company policies
- providing conditions and resources to meet ISMS requirements
- continuously raising awareness and education of all employees and outsourced contractors
- monitoring the effectiveness of ISMS implementation based on the results from risk assessments, internal audits and management reviews

7 Security engineer

The management of the company authorized a security engineer, who will take care of the ISMS documentation. The CEO appoints the security engineer for a five-year period, which may be extended.

The tasks of the security engineer are:

- to prepare and review the information security policy
- to forward the security policy to management for confirmation
- to monitor for important changes during the implementation of information resources
- to avoid major hazards
- to review and monitor security events
- to validate major initiatives for increasing information security

- to ensure active commitment of employees to the process of information security
- to conduct investigations into all alleged incidents, offenses and extraordinary events related to information security

In addition, the security engineer is responsible for the implementation, execution, administration, and the interpretation of policies, standards, guidelines and procedures related to information security in the company.

8 Objectives and their evaluation

To monitor the implementation of the information security policy, we have established the following objectives:

- Improving the information security of the company - We monitor this by decreasing the number of similar security incidents on the yearly basis. Security engineer is responsible for presenting the report and possible solutions to the management.
- Integrating information security as one of the objectives of each project - Each project must have at least one check in the field of information security, even if the client does not require it. Reports and actions that were taken as the result of security checks are used to document and monitor the progress and success of information security on per-project basis.
- Improving the information security awareness of all employees - We monitor this trough a short test taken by an employee during their information security training. Results are used to project the level of the information security awareness.

9 Legal basis and compliance with regulations

During creation of security policies, rules, instructions, declarations and procedures, the following is taken into account:

- currently valid legislation of the Republic of Slovenia
- relevant European Union directives
- ISO / IEC 27001: 2013 standard and
- Established security practices in the area of information security that are in line with the law

10 Security policy

The security policy and other ISMS documentation includes the requirements and recommendations of the ISO / IEC standard 27001: 2013. Individual security policy chapters describe the topics defined by the standard. Security Policy Chapters are intertwined and complement each other.

The chapters defined by the security policy are:

- information security policy
- organization of information security
- human resources' security
- asset management
- access control
- cryptography
- physical and environmental security
- operations security
- communication security
- system acquisition, development and maintenance of information
- supplier relationships
- information security incidents management
- information security aspects of continuity business management
- compliance

Additional sections may be written for individual fields of application, where required.

11 Action plan in the event of deviations or exceptional circumstances

All employees, contractors and students are required to report any extraordinary events (deviations from normal state) to the security engineer. An extraordinary event is reported orally, by telephone, through an electronic message or by completing the prescribed form, paper or electronic. The security engineer is responsible for recording the incident and, if necessary, taking appropriate action.

Reports shall be made in the case of:

- extraordinary events in information security
- deficiencies or any suspicion of deficiencies in the information security as well as any threat that threatens systems or services
- improper operation of software or hardware

Each reported suspicion of a security policy violation is dealt with separately. During the investigation, the allocated access rights, authorizations or powers may be revoked. The incident is investigated by a person or group of people operating within the company, appointed by the management.

In the event of a breach of security policies, personnel shall act in accordance with the legislation and the rules defined in the security policies. Regarding subcontractors, the company shall act in accordance with the signed contract.

12 Reference documents

- ISO / IEC 27001: 2013 Information technology - Security techniques - Information security management systems - Requirements
- ISO / IEC 27002: 20013 Information technology - Security techniques - Code of conduct in information security controls
- http://data.europa.eu/eli/reg/2016/679/oj
- Confidentiality statement of XLAB coworkers

13 Document owner

The owner of the document is Chief Security Engineer who is responsible for maintaining the document.

Dr. Gregor Pipan, CEO

Ljubljana, 18.4.2018