Information Security Policy Framework

Index

1. Introduction

The document entitled "Security Policy Framework" contains public information and does not require a specific label in accordance with the relevant document classification. All users of the information system of the University of Maribor (UM) must be made familiar with the information contained herein.

The primary task of the Computer Centre of the University of Maribor (CCUM) is to provide comprehensive, flexible and efficient information support at the University of Maribor (UM). CCUM is in charge of a geographically widespread and heterogeneous infrastructure facilitating the implementation of computer, information, communication and other services and providing access to sources required for the smooth running of the teaching process, research work and operating activities.

The most important services provided by CCUM:

- basic IT infrastructure planning and management (UM's central information and communication network ad central servers of UM's information system);
- provision of access to the network and its services (access, IP addresses, e-mail, web servers);
- maintenance and development of application of UM's information system;
- administration of computer and communication equipment for the Rector's Office and university members without own personnel;
- helpdesk (providing help to employees of individual departments at university members);
- software distribution;
- security and protection of information;
- training of users.

Being aware of the importance of business continuity of the information system operation for the efficient provision of services, the University of Maribor adopted the information security policy (ISP).

A consistent implementation of the information security policy ensures an effective management of security issues in the following sense:

- **Confidentiality:**
    - Protection of sensitive business information from unauthorised access and illegal interception. Confidentiality ensures that information is available to authorized persons only. In the event of failure of other security mechanisms (e.g. stolen laptops, data stolen from servers), confidentiality ensures that these data are unusable/non-recoverable – written in an incomprehensible/unusable form.

- **Integrity:**
    - Ensuring correct and comprehensive information and software. Integrity control is used for the protection of data and systems from unauthorized change. Integrity facilitates the identification of changes and prevents that the modified copy would be treated as an original.

- **Availability:**
    - Ensuring that information and important services, applications and processes are available to authorized users when they require them.

The Rector of the University of Maribor supports the information security policy and demands that it is observed, regularly reviewed and supplemented by CCUM (at least once a year).

All employees and users of UM's services have been informed of the information security policy and are obliged to understand and respect it.

Any violation of the provisions of the information security policy represents a breach of professional, contractual or academic duties and will be sanctioned in accordance with the internal rules for employees of the University of Maribor. With regard to other users of UM's services, CCUM and university members reserve the right to restrict or deny access to the information system.

The document shall be reviewed on an annual basis. If changes to the document are proposed, the security engineer shall examine all proposed changes and prepare a final proposal

2. Information Security Policy Framework

2.1 Information Security Objectives

The primary objective of information security is to ensure business continuity and sound administration and minimize damage by preventing and alleviating the negative impacts of undesirable security events.

2.2 Information Security Policy

The aim of the security policy is the protection of UM's information means and sources against different risks, internal and external, intentional or accidental, in accordance with ISO/IEC 27001.
The security policy contains instructions and standards for information security assurance and management for all users of the information system.

The information security policy comprises the following:

- confidentiality, integrity and availability of information;
- protection of information from unauthorised access, disclosure, change or destruction;
- provision of training on information security for all employees;
- observation of rules for secure use on the part of users of UM's information infrastructure;
- management of security incidents and adoption of relevant measures;
- compliance with the laws and regulations in force.

Anyone with access to UM's information system must comply with the requirements of the information security policy.

The person responsible for coordinating the work of outsourcers is obliged to inform them of the security policy and make sure that its provisions are observed. Before starting work, outsourcers must sign a statement stipulating that they are familiar with the security policy and will respect its provisions.

2.3 Organisation of Information Security Management

Information security management includes:

- understanding UM's strategic objectives and technology development guidelines in order to formulate a long-term information security strategy;
- defining, establishing, maintaining and implementing UM's information security policy;
- obtaining support for information security;
- establishing and maintaining a high level of information security;
- monitoring and observing legislation on information security;
- ensuring security consultations;

- ensuring relevant training and informing all users of UM's information media of information security;
- informing the university management of security issues and related risks.

2.3.1 Management

The management must ensure that employees comply with the requirements of the information security policy. The management shall be responsible for the rejection of unjustified or unnecessary requests for access to information sources and termination of access to information sources if no longer required.

The management shall be responsible for the effective management of information security. For this reason, it shall implement efficiency screenings of the security management system, including:

- results of system reviews and inspections;
- reports on risk assessment and identified threats;
- reports on changes that may impact information security;
- suggestions for improvement.

The management also has the following obligations:

- approving strategic guidelines for information security;
- approving documents on information security policy;
- providing support for information security projects;
- overseeing larger changes with regard to the exposure of information sources to security threats;
- monitoring and assessing security efficiency and capacity.

2.3.2 Person responsible for information security at UM

The person responsible for information security is in charge of the efficient implementation of information security at UM.
Tasks of the person responsible for information security:

- reporting to the management with regard to all matters related to information security;
- advising on all areas related to information security;
- reviewing and updating the risk catalogue;
- reviewing and updating the catalogue of changes to IT infrastructure as well as the security incidents catalogue;
- developing the security policy and supervisions;
- overseeing the implementation of the security policy and supervisions.

2.3.3 Persons responsible for information security at faculties

At university members, persons responsible for information security are chief secretaries who may allocate the responsibility to another person, in which case the head of the

Computer Centre must be informed. The list of persons responsible for information security is published on UM's website. The appointed person is also responsible for the implementation of rules defining security policy at university members.

2.3.4 Owner of information resource

The owner of information resource is responsible for the control, development, maintenance and protection of UM's information resource.
Tasks of the owner of information resource:

- confirming eligibility for access;
- reviewing security events in logs and taking action in the event of identified irregularities;
- reviewing the list of users with access rights (once a year)
- reviewing the list of users with special (administrative) rights on a regular basis (every 6 months).

2.3.5 Administrator of information sources and communication infrastructure

The administrator is responsible for the establishment of operation, settings and maintenance of information sources and communication infrastructure at UM:
Administrator's tasks:

- checking the functioning of information sources and communication infrastructure;
- introducing and maintaining information solutions in order to ensure the smooth functioning of information sources and communication infrastructure;
- adjusting security settings of information sources and communication infrastructure;
- trouble shooting and identifying causes of malfunction;
- ongoing training in order to refresh relevant skills.

2.3.6 Information system users

All employees, students and other users of the information system including outsourcers must observe UM's information security policy (Information Security Policy for Users). UM's information security policy for employees is laid down in the document entitled "Information Security Policy for Employees". The information security policy for outsourcers is laid down in the document entitled "Information Security Policy for Outsourcers".

2.4 Management of Information Sources

Information sources and resources must be developed, introduced and maintained in accordance with the security requirements laid down in the document "ICT Security Policy Information".

3. Transitional and Final Provisions

IT administrators at university members are obliged to ensure the observance of the rules contained in this document within 18 months from its adoption at the latest.

The information security policy for employees shall apply to all users of UM's information system.

Any violation of the instructions contained in this document shall be considered a breach of professional, contractual or academic duties.

The document shall enter into force on the eight day following its publication in the Announcements of the University of Maribor.

Rector of the University of Maribor

Prof. Dr. Danijel Rebolj