ICT Security Policy

Index

1 Introduction

The document entitled "ICT Security Policy" contains information considered internal in accordance with the relevant document classification and is not intended for the general public.

The security of the information system is an integral part of UM's operation. The information security policy is based on three security elements: confidentiality, integrity and availability. All employees at UM and users of UM's information system must be familiar with these elements, which are integrally related to the security of the information system supporting and implementing business activities.

The protection of confidentiality, integrity and availability are three main goals than must be achieved in order to reduce security risks.

Confidentiality means the protection of sensitive business information from unauthorized 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 laptop, stolen data from servers), confidentiality ensures that data are useless – written in an incomprehensible/useless format.

Integrity focuses on ensuring the correctness and integrity of 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 ensures that information and important services, applications and processes are available to authorized users when required.

The Information Security Policy has been formulated In order to support the protection of confidentiality, integrity and availability of UM's information sources.

This document describes the information security policy for the field of ICT. The document is composed of various levels defined and described in the following chapters.

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 Elements of Security Control

2.1 Information resource management

The aim of information resource management is to achieve and maintain relevant protection of UM's resources.

Control 1: Every year, CCUM and university members shall review and harmonize the list of software and hardware used at UM.
Control 2: Every information resource has an owner.
Control 3: Every information resourced has an administrator.
Control 4: All information are tagged and classified.

Harmonization criterion

Consideration of controls described under "Exact description" is **obligatory**.

- Deviations from this criterion must be documented and approved by the responsible person at CCUM or university members.

Implementation

Establishing a register of servers, network devices and other production systems
Establishing a register of business and information production applications
Compiling a table entitled "Relations between business processes and information resources"

Exact description

Control 1: Every year, CCUM and university members shall review and harmonize the list of software and hardware used at UM

The list of systems (servers – physical and virtual, important workstations, network communication equipment, other production equipment) shall be designed in form of a table, for which system administrators shall be responsible. All important elements of UM's information system must be recorded in the table entitled "Relations between business processes and information media". The table contains processes listed by priority, which are important in order to establish priorities for the modernisation of the information system. A detailed list with a brief description of software developed in the context of UM shall be kept by CCUM and individual university members. All lists shall be regularly supplemented and reviewed and updated at least once a year.

Control 2: Every information resource listed in the register has an owner.

The owners of information resource shall be responsible for control, development, maintenance and protection of UM's information resource.
Tasks of owners:

- confirming access eligibility for different users;
- reviewing security events in long entries and taking action in the event of detected irregularities;
- reviewing the list of users with access rights for a certain information source (once a year);

- reviewing the list of users with specific access rights on a regular basis (every 6 months).

Control 3: Every information resource listed in the register has an administrator.

Administrators must ensure the functioning, settings and maintenance of information resource and network communication infrastructure at UM:
Tasks of administrators:

- operational checks for information resource or network communication infrastructure;
- introduction and maintenance of information solutions to ensure business continuity of information resource or network communication infrastructure;
- implementation of security settings for information resource or network communication infrastructure;
- troubleshooting and root-cause analysis;
- ongoing education and training in order to acquire knowledge and skills in the relevant area of work.

Control 4: Information are tagged and classified.

The organization of information is laid down in the rules on the protection of personal data and confidential information, which are in compliance with ZVOP-1 (Rules on Personal Data and Confidential Information Protection No. A11/2006-524 JR).

2.2 Physical protection

The aim of physical protection is the prevention of unauthorized physical access, damage and disturbances on premises as well as loss, damage, theft or compromise of information media.

Control 5: Critical capabilities for information processes have been installed in protected areas.
Control 6: Control of entry in areas where UM's information resources (servers, communication equipment) are located has been established
Control 7: Media used for archiving and restoring data are physically protected from unauthorized access, theft or damage.
Control 8: Prior to the removal of equipment, data carriers shall be checked and data and licence software shall be removed.

Harmonization criterion

Consideration of controls described under "Exact description" is **obligatory**.

- Deviations from this criterion must be documented and approved by the responsible person at CCUM or university members.

Implementation

Establishing the required controls for the protection of UM's data centre

Exact description

Control 5: Critical capabilities for information processes have been installed in protected areas.

Protected areas are equipped with uninterruptible power supply, fire and breakage detection and protection as well as air conditioning.

Control 6: Established control of entry in areas where UM's information resources (servers, communication equipment) are located – controlled area.

The following controls or security elements shall apply to protected areas:

1. The area must be locked even when under surveillance
2. CCUM or responsible persons at university members shall establish business needs for access to this area.
3. Each access to the controlled area shall be logged.
4. Persons whose access rights have been revoked must be removed from the list immediately.
5. Report on access to the protected area must be reviewed every three months in order to detect unauthorized access attempts.
6. The eligibility for access of persons from the list of accesses must be review annually.
7. Alarms must operate via emergency power supply.
8. If the alarm sets off, an investigation shall be conducted. Based on findings, corrective measures must be adopted and, where appropriate, the entry mode must be changed in order to prevent another alarm.

Note:

Troubleshooting procedures must be conducted on a regular basis, after the conducted quarterly or annual reviews.

Control 7: Media used for archiving and restoring data are physically protected against unauthorized access, theft or damage

The following instructions must be observed:

- Media must be stored in the protected area in a locked cupboard.
- The area where the media are stored must be fireproof.
- Authorized persons only have access to media.

Control 8: Prior to the removal of equipment, data carriers shall be checked and data and licence software shall be removed.

All devices containing sensitive information (esp. confidential and personal data) must be physically destroyed or deleted in such a manner as to prevent the recovery of original information (the use of "delete" or "format" commands is not allowed).

2.3 Communication and production management

The aim of communication and production management is to ensure the correct functioning of the information system, minimization of system failures, protection of software and information, preservation of the integrity and availability of information, protection of networks and support infrastructure and detection of unauthorized processing of information.

Control 9: All working procedures shall be documented and available to all persons requiring them.
Control 10: Backup copies of data must be kept in two separate locations. Recorded data shall be reviewed on a regular basis in accordance with the prescribed recovery procedures.
Control 11: Technical controls for prevention of distribution and implementation of malware have been established.
Control 12: During exchange, information must be suitably protected.
Control 13: Prior to the publication of publicly available data, information must be verified in order to ensure the correctness of published data.
Control 14: With regard to the preparation of the final product version, software developers must also perform an antivirus scan.
Control 15: Patch installation must be performed in the context of the approved change management process.
Control 16: Where technically feasible, control records must be created for systems, programmes and network equipment.
Control 17: Control records must be created for all successful and unsuccessful attempts to access UM's information media from external locations.
Control 18: Data on activities must include at least the following parameters: date, time, type of access attempt, user identification.
Control 19: Clocks on all information systems are synchronized to network time servers.

Harmonization criterion

Consideration of controls described under "Exact description" is **obligatory**.

- Deviations from this criterion must be documented and approved by the responsible person at CCUM or university members.

Implementation

A record of settings of the communication equipment – configuration for individual elements of the communication equipment

Exact description

Control 9: All working procedures shall be documented and available to all persons requiring them.

Procedures for system activities are documented in operating instructions for individual activities, such as:

- server startup and shutdown,
- data archiving and recovery,
- technical maintenance of the equipment,
- handling of data carriers,

- activities related to communication infrastructure,
- maintenance of security infrastructure.

Control 10: Backup copies of data must be kept in two separate locations. Recorded data shall be reviewed on a regular basis in accordance with the prescribed recovery procedures.

In order to ensure business continuity and the protection of data during unexpected events, backup and archiving procedures described in the following chapters shall be implemented on information sources.
Magnetic tapes and other media for data storage shall be kept in a fireproof cupboard.

Servers

Persons responsible for archiving shall also be in charge of the data archive. Data archiving shall be conducted for each server in accordance with the predefined plan.
Archiving is conducted automatically by means of automatic rules every day at a certain hour. Every morning, the person responsible for archiving shall check the success of the archive/s and, where appropriate, replace the media and facilitate their transport to a secure location.
At the central location, archiving shall be conducted as follows:

- everyday incremental archiving (from Monday to Saturday),
- archiving of the entire system (Sunday).

Workstations

For key users, a central data and document storage system has been set up. Users shall save all business data and documents in a file on the network-attached storage connected into the central storage system. Security is ensured through archiving in the central archive system.
Users must take care of locally stored documents and data themselves by archiving on data carriers (CDs, DVDs, USB, etc.), which must be protected from unauthorized access. Users are solely responsible for these archives.

Network infrastructure

Configurations of communication devices are stored in a central place. Upon each change of parameters on the communication device, a new version of the back-up copy of configuration parameter is created, which are required for the recovery of the communication network.

Control 11: Technical controls for prevention of distribution and implementation of malware have been established

Malware dissemination and implementation shall be prevented by adopting the following measures:

- Only the use of approved antivirus protection is allowed.
- The antivirus programme must be updated regularly.
- Configuration of the antivirus programme for auto recovery of security definitions must be conducted at least once a day. If auto recovery via the network is not possible, the procedure for manual recovery of security definitions must be conducted at least once a week.
- Configuration of the antivirus programme – scans must be conducted at least once a day after the recovery of security definitions and full scans at least once per week.

Note:

- *If it is suspected that malware is installed on any part of the information system, the security engineer or administrator must be informed immediately in order to minimize damage.*

Control 12: During exchange, information must be suitably protected.

The internal network has controls preventing interception and manipulation of data on the communication route. During the exchange of data with third parties, it is obligatory to use protected communication routes (encryption, digital signature ...).

Control 13: Prior to the publication of publicly available data, information must be verified in order to ensure the correctness of published data.

Prior to publication on UM's website, information need to be verified. In the context of regular network vulnerability scans, the vulnerability of publicly available servers shall also be checked.

Control 14: With regard to the preparation of the final product version, software developers must also perform an antivirus scan.

The following must be included in the implementation:

- The application must undergo a security scan before being transferred to the production environment.
- Security scans must also be implemented for patches and new versions of existing applications.

Control 15: Patch installation must be performed in the context of the approved change management process.

It is not allowed to modify data and programmes without a pre-planned change in accordance with the change management process except in the event of a procedure of exceptional character requested by the responsible person.

Control 16: Where technically feasible, control records must be created for systems, programmes and network equipment

Control records shall include the following activities:

- Successful and unsuccessful login attempts.
- Successful and unsuccessful attempts to access settings of the operating system (modification and/or reading) deviating from generally permitted ones.
- Activities conducted by the administrator (e.g. changing security configurations). These records must also be collected.
- Successful IP address assignment and releasing on network services (DHCP).

Control 17: Control records must be created for all successful and unsuccessful attempts to access UM's information media from external locations

All records must be stored in a separate system in UM's network.
Exceptions with regard to the collection of control records are not allowed.
Records must be reviewed once per week (automatically or manually) in order to detect systematic attacks.

Control 18: Data on activities must include at least the following parameters: date, time, type of access attempt, user identification

Different information sources store information in different formats and with different parameters. All information systems store at least the above mentioned parameters.

Control 19: Clocks on all information systems are synchronized to network time servers.

Clocks of information sources inside UM must be synchronised with the centrally determined time source on servers of CCUM or university members, which are synchronised with external servers.

2.4 Access to information resources

The aim of controls for access to information media is to provide access to information and capacities for the processing of information and business processes based on business and security requirements and needs.

Control 20: Each user of UM's information technology (employees, students, outworkers, outsourcers) shall be assigned a unique identifier.
Control 21: The process for assigning, changing and deleting user identification has been established.
Control 22: Authorization for admin access to information is based on business needs and shall be determined by the owner of the information resource or system.
Control 23: The process for annual eligibility verification of users and other persons with an assigned identification for access to production systems has been established.
Control 24: User identity shall be authenticated before users start to use the information system or application.
Control 25: Passwords for privileged access shall be available only to persons requiring it for the execution of their tasks. Where appropriate, the password shall be linked to the person.
Control 26: Where appropriate, reusable passwords for identity verification shall take into account the defined instructions.
Control 27: Reusable passwords for identity verification are protected.
Control 28: Systems or applications using passwords for direct communication with other systems and applications may use non-expiring passwords.
Control 29: Idle sessions shall be aborted after a certain period of time.
Control 30: The access of outsourcers and business partners to UM's internal information resources must be approved by the responsible person and technically limited to the lowest extent possible for the execution of agreed tasks.
Control 31: The supplier or the relevant support service shall adjust security settings of user sources enabling access only to authorized users approved by the owner of the information medium.
Control 32: Technical control for the prevention of unauthorized access to UM's confidential data and personal data of UM's employees has been established.

Harmonization criterion

Consideration of controls described under "Exact description" is **obligatory**.

- Deviations from this criterion must be documented and approved by the responsible person at CCUM or university members.

Implementation

Setting up a user identification register
Implementing annual verification of user identification

Exact description

Control 20: Each user of UM's information technology (employees, students, outworkers, outsourcers) shall be assigned a unique identifier.

Authentication systems at UM are managed separately. Users may have different unique identification at different sources. The allocation of rights shall be based on the request of responsible persons.

Control 21: The process for assigning, changing and deleting user identification has been established

User identifications may be allocated, changed or deleted in accordance with the procedure prescribed for individual systems or sources. Owners of information resource shall decide on identification assignment, change and deletion.

Procedures for UM employees:
Assigning user accounts:

- The human resources department shall enter basic data of new employees into the human resources information system
- Based on proposed business needs and their powers, responsible persons at university members shall compile information requirements with regard to the post, duties, functions and terms of office and communicate them to the system administrator.
- The system administrator shall allocate access rights for user accounts and inform the human resources department and the employee's superior of the implemented action.

Deleting user accounts:

- The employee's superior shall forward data on deletion of the user account to the system administrator.
- In addition to requests of superiors, the system administrator may check employees' activities in the human resources information system and disable access rights to the information system upon termination of the employment or contractual relationship.
- The system administrator shall disable access to the user account and initiate the termination procedure.

Changing user accounts:

- The employee's superior shall communicate the request to the system administrator.
- The system administrator shall modify access rights and inform the employee's superior of the implemented action.

Control 22: Authorization for admin access to information is based on business needs and shall be determined by the owner of the information resource or system.

Admin authorization shall be assigned in accordance with a predefined procedure, which includes:

- verification of a business need,

- impunity verification,
- verification of the required level of education and work experience.

Authorization must be approved by the personal responsible for information security.
Business needs for the preservation of authorization shall be reviewed at least once a year. Authorization revocation shall be conducted within three working days after establishing that the business need no longer exists or after receiving relevant notification.

Control 23: The process for annual eligibility verification of users and other persons with an assigned identification for access to production systems has been established.

Verification of eligibility for access to information sources shall be conducted separately for each information source. The owners of information resource are responsible for reviewing data.

Control 24: User identity shall be authenticated before users start to use the information system or application.

Authentication methods at UM:

- LDAP (Lightweight Directory Access Protocol) for all users of the information system.
- Authentication implemented in individual information solutions (e.g. EDUROAM etc.).
- Authentication for access to external applications, such as ZZZV, online banking, etc.

User authentication represents only the initial verification step. At the information source, access authorization to individual parts or sections of the source is implemented after basic authentication in LDAP.
Access to certain information resources may also be provided by means of additional authentication and authorization. In the event of unauthorized access, the administrator may disable access to the information source or change authorization rights on the information source.
When using external applications, security approaches, authentication and settings of user profiles must be adjusted in accordance with the application provider/administrator.

Control 25: Passwords for privileged access shall be available only to persons requiring it for the execution of their tasks. Where appropriate, the password shall be linked to the person

Passwords for privileged access to the information system are available only to persons requiring it for the execution of their duties. They shall be stored in a safe place (sealed envelope). Each password access shall be recorded.

Control 26: Where appropriate, reusable passwords used for identity verification, shall take into account the defined instructions

- Recommendations for password selection are published on CCUM's website.

Control 27: Reusable passwords for identity verification are protected

Instructions for password identity verification:

- The password is encrypted. If encryption is not possible, access to passwords is limited to authorized system administrators only.
- Passwords must not be used for multiple users except if control and audit of use by individual user has been established.

- In order to reset passwords, a security procedure involving request verification has been established.
- Default passwords selected upon installation of the operating system or application must be changed during or immediately after installation.
- The transfer of passwords via internet, public networks or wireless networks is allowed only in safe mode in encrypted form.

Control 28: Systems or applications using passwords for direct communication with other systems and applications may use non-expiring passwords.

Direct communication with other systems and application is enabled via approved communication routes. New communication pathways between information systems must be approved by the security engineer or administrators of connected information systems.

Control 29: Idle sessions shall be aborted after a certain period of time.

Idle sessions shall be aborted after a certain period of time, which depends on system criticality and is determined by the owner of the information resource.

Control 30: Access of outsourcers and business partners to UM's internal information resource must be approved by the responsible person and technically limited to the lowest extent possible for the execution of agreed tasks

Rights and accesses shall be reviewed at least once a year.

Unnecessary accesses to UM's information resource shall be disabled or permanently deleted. The review shall be conducted by the owner of the information resource, who must forward the results to the person responsible for information security.

Control 31: The supplier or the relevant support service shall adjust security settings of user sources enabling access only to authorized users approved by the owner of the information medium

Prior to the transfer to the production environment, default user names must be disabled and passwords on all systems changed.

Access to the information system is provided only for users requiring it for the execution of their duties.

Control 32: Technical control for the prevention of unauthorized access to UM's confidential data and personal data of UM's employees has been established

Access to UM's confidential information is provided only to those persons requiring it. Access must be specifically approved by the management. Group access may be granted only if all group members require it. However, if possible, access shall be enabled for one user individually.

If no technical control can be established, procedure control shall be set up (including change and access logging).

2.5 Security incident management

The aim of incident management is to ensure that events and vulnerabilities of information systems are communicated to the central place. Based on the events recorded, different activities for a fast, efficient and regulated response to security incidents shall be adopted.

Control 33: All incidents must be notified to both the person responsible for information security and the administrator in accordance with the prescribed procedure.

Control 34: In the event of a serious security incident (e.g. unauthorized access to confidential or sensitive data, change or risk to the system/server integrity, denial of service (DOS/DDOS), change or damage to websites or servers, system intrusion and intrusion attempts, destruction of data, fraud, etc.), the prescribed activities must be conducted.

Control 35: If the security scan detects a violation of authorization, the person responsible for information security and the owner of the information medium must be informed.

Harmonization criterion

Consideration of controls described under "Exact description" is **obligatory**.

- Deviations from this criterion must be documented and approved by the responsible person at CCUM or university members.

Implementation

An updated, detailed and authentic record of incidents available to authorized persons only

Exact description

Sources of security incidents may be either internal or external. Security incidents vary in scope, goals and impacts on UM's operation.

Control 33: All incidents must be notified to both the person responsible for information security and the administrator in accordance with the prescribed procedure

Users must report security incidents to the administrator, who shall correct the error and record the intervention into the activity log. After completion of the activity, users must confirm the elimination of the incident. Security incidents must be recorded in the central register kept by the information security engineer.

Control 34: In the event of a serious security incident (e.g. unauthorized access to confidential or sensitive data, change or risk to the system/server integrity, denial of service (DOS/DDOS), change or damage to websites or servers, system intrusion and intrusion attempts, destruction of data, fraud, etc.), the prescribed activities must be conducted

In the event of security incidents, the following activities shall be conducted:

- Informing the security engineer who conducts an investigation into the incident and implements the procedure for the elimination of consequences of the incident.

- When a security incident occurs, a log with relevant information and actions related to the incident must be created. For each entry, the date, time and source of information must be recorded.
- If the envisaged duration of failure cannot be estimated and a high risk for UM is suspected, the staff of CCUM or university members must immediately adopt control measures in order to manage and decrease damage to UM's business information system.
- Security incidents related to physical security must be reported to the relevant security service.

If a security incident is suspected, the following actions are **prohibited**:

- Unauthorized conduct of investigation since this might lead to the destruction of traces or put the real investigation at risk.
- Informing individuals who might be the source of the security incident. All activities must be discussed with the security engineer.
- Counter-attack attempt against the attacker. Such procedures are dangerous and may contradict the law.
- Attempt to remove the threat without the prior approval of the security engineer since this might lead to the destruction of traces or put the investigation at risk.

Information on security incident investigations shall be available only to eligible persons. Therefore, information concerning the investigation or its aims, details and results shall not be disclosed to no one except if the security engineer or responsible person decides otherwise. It is also prohibited to disclose information to anyone outside UM without the approval of the management.

Control 35: If a violation of authorization is detected during a security review, the person responsible for information security and the owner of the information medium must be informed

2.6 Business continuity management

The aim of business continuity management is the protection of critical business processes against consequences of system failures or accidents and assurance of timely disaster recovery.

Control 36: On the basis of risks, probability and significance of information resources, owners of information resources and the management determine priorities establishing disaster recovery time for individual parts of the information system.

Control 37: Detailed procedures for disaster recovery are laid down in the document "Recovery Plan", which is available to person authorized for control and implementation.

Control 38: The prescribed procedures of the recovery plan shall be tested upon each larger change of the information system or at least once a year.

Harmonization criterion

Consideration of controls described under "Exact description" is **obligatory**.

- Deviations from this criterion must be documented and approved by the responsible person at CCUM or university members.

Implementation

Formulating and testing the recovery plan

Exact description

Control 36: On the basis of risks, probability and significance of information resources, owners of information resources and the management determine priorities establishing disaster recovery time for individual parts of the information system.

Priorities of key applications with regard to processes are determined in the table "Relations between business processes and information sources". Priorities are indicated by colour – red indicating highest priority and green indicating the lowest. The table shall be updated in accordance with the the information system development.

Control 37: Detailed procedures for disaster recovery are laid down in the document "Recovery Plan", which is available to person authorized for control and implementation.

The recovery plan comprises technical detail required for system recovery, including contact information of all people involved in the implementation of recovery activities.

The recovery plan shall be updated upon each change of the environment at UM or university members. Examples of change, where the recovery plan must be updated, include: purchase of new equipment, system upgrades, introduction of new functions to systems and changed risks.

Control 38: The prescribed procedures of the recovery plan shall be tested upon each larger change of the information system or at least once a year.

Testing shall be conducted by means of the test environment for individual parts and sections or the entire system if permitted by the available sources.

2.7 Compatibility

The aim of compatibility is to prevent violations of law, contractual obligations and security requirements.

Control 39: All personal data shall be handled as provided by the Personal Data Protection Act (ZVOP-1).
Control 40: Access to UM's capacities shall be equipped with a warning on permitted use and prohibited access for unauthorized persons.
Control 41: A security review of the information system must be conducted at regular intervals.
Control 42: Security processes must be reviewed on an annual basis on a representative sample.

Harmonization criterion

Consideration of controls described under "Exact description" is **obligatory**.

- Deviations from this criterion must be documented and approved by the responsible person at CCUM or university members

Implementation

Implementing independent security testing

Exact description

Control 39: All personal data shall be handled as provided by the Personal Data Protection Act (ZVOP-1).

All personal data filing systems at UM are recorded in the relevant register kept by the information commissioner of the Republic of Slovenia. Prescribed controls with regard to the protection of personal data must be taken into account. The personal data protection system is laid down in detail in the relevant rules (Rules on the Protection of Personal Data and Confidential Information No. A11/2006-524 JR).

Control 40: Access to UM's capacities shall be equipped with a warning on permitted use and prohibited access for unauthorized persons

Unauthorized use of UM's capacities for non-business needs is prohibited without the explicit approval of management. Any unauthorized activity must be reported to the superior in charge of the implementation of further procedures.

Control 41: A security review of the information system must be conducted at regular intervals.

Security scans must be conducted at regular intervals depending on the type of server:

Server	Security scan
Web servers, generally available servers	every 3 months
Internal production servers	every 6 months
Other internal servers and	once a year

equipment	

Security review shall include at least the following elements:

- All required controls must be set and implemented in accordance with technical instructions.
- Only approved users have administrator rights.
- Only approved users have access to sources of the operating system.
- Programmes for malware and code protection must be installed and must function properly.
- Control records are being collected.

Established deviations/irregularities shall be managed by the security engineer or data owner. The management must be informed of all irregularities at regular sessions. In the event of significant irregularities, the management must be informed immediately.

Note:
If vulnerabilities of internet servers have been detected and cannot be fixed in the defined period, the servers shall not be used until vulnerabilities have been fixed.
Unauthorized persons are not allowed to use vulnerability scanner tools.

Control 42: Security processes must be reviewed on an annual basis on a representative sample.

The review of security processes must include the following:

- Management of user resources
- Physical access control
- Access to information resources:
  - Administration of user identification and passwords (granting, revoking, regular reviews, resetting passwords)
  - Authorization for administrator access to information and systems
- Compiling and reviewing control records:
  - Storing required control records
- Integrity and availability of information services:
  - management of administrator and security authorization
  - vulnerability testing
  - management of patch installations
  - control and detection of incorrect logging to the system and systematic attacks
  - activation of unauthorized systems and services.

Transitional and Final Provisions

The ICT Security Policy shall apply to all employees in charge of information infrastructure.

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

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 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