Information Security Policy for Users

Index

1. Introduction

The document entitled "Information Security Policy for Users" contains public information and does not require a special 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 document describes basic security mechanisms that must be understood and observed by all employees at UM, business partners and other users of UM's information system.

The document explains the responsibilities of all employees and other users with regard to the protection of information and UM's infrastructure as well as the most important procedures for workstation and malware protection.

Detailed instructions for the implementation of the requirements laid down in this document are described in relevant organisational regulations.

Failure to comply with the requirements contained herein represents a breach of professional, contractual or academic obligations.

With regard to other users of UM's services, who did not conclude an agreement with UM, the Computer Centre of the University of Maribor (CCUM) may restrict or deny access.

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. General Security and Requirements for Use

2.1 *Permitted use of computer equipment*

2.1.1 Workstation set-up and configuration

Users and unauthorized persons are not allowed to set up or move desktop computer equipment.

The changing of workstation configuration (e.g. changing internet access parameters, turning off firewall, antivirus protection ...) on the part of users or other unauthorized persons is laid down in the regulations for individual university members.

2.1.2 Use of UM's computer equipment and infrastructure for private purposes and use of private computer equipment

UM's computer equipment and information infrastructure may be used only for non-commercial purposes (teaching, scientific research) and projects implemented by UM.:

The use of private computer equipment is permitted in accordance with CCUM's rules of use.

2.1.3 Internet and e-mail use

E-mail and internet use is allowed and restricted in accordance with UM's policy and regulated in order to increase security and minimize information incidents. All user activities are recorded in order to ensure an uninterrupted operation of the information system. The content of user activities, i.e. user packages (email content, attachment content and the content of website visits) shall be neither recorded nor otherwise monitored.

Any kind of SSL encrypted traffic inspection for known target addresses with the purpose of detecting misuse is permitted only with prior notice to users. In this case, users must receive an email establishing the duration and scope of the inspection, which must also be published on the website of the University and CCUM.

In the event of unusual behaviour of the information system, users are obliged to inform the person responsible for information security at UM and follow his/her directions. CCUM shall keep a record of information incidents, which must be regularly reviewed by the person responsible for information security implementing relevant security measures.

2.2 *Legislation*

2.2.1 Software licences

Special attention must be paid to the use of copyrighted software (intellectual property). Prior to software installation, users may consult system administrators.

If users require non-standard software, they must discuss the purchase and set-up with their supervisors. However, users shall be solely responsible for this equipment.

The use of pirated software is prohibited.

2.2.2 Copyright and intellectual property

The majority of information and software (music, video, programmes, films, documents ...) available in the public domain (including internet) are protected by copyright or another form of intellectual property. In case of copyright and intellectual property infringement, individuals shall assume full material and criminal liability. In the event of doubts concerning the use of materials, the relevant support service must be consulted.

2.2.3 Protection of privacy

UM collects and maintains personal information from databases published in the personal data register kept by the information commissioner.

Personal files, information and data must always be stored on prescribed information media, which are protected. Protection procedures are laid down in detail in the relevant rules – Rules on the Protection of Personal and Confidential Information No. A11/2006-524 JR.

Employees are not allowed to access information media of other employees (e.g. files, records, other content on different devices and in physical form) without the prior consent of the owner or administrators (in the event of personal data, the consent of the individual in question is required).

2.3 Protection of information

2.3.1 Password

The password and user name for computer access is the primary method of identification facilitating access to UM's information sources. For personal protection and the protection of UM's information media and sources, the password must not be shared with others.

With regard to UM's systems and applications, password setup and handling is subject to rules published by CCUM on its website.

Passwords are considered confidential information. Users are obliged to protect their password by:

- not sharing it or disclosing it to other users;
- not communicating it over the phone;
- not disclosing it (e.g. to the head of office or system administrator);
- disabling password saving in applications;
- not writing it down;
- not saving it on information media (computer, PDA, mobile phone, etc.);
- using passwords different from those for private and other use.

Encrypted passwords for information resources are used for protection from unauthorized access, not identification. Therefore, these passwords must be communicated to the superior, who shall keep them in a sealed envelope in a safe place. With regard to access to information sources not under the control of UM (home computers, private e-mail ...), it is not allowed to choose the same passwords as those for access to UM's information sources.

2.3.2 Protection of confidential information

Information at UM are defined as stipulated by the Rules on the Protection of Personal and Confidential Information No. A11/2006-524 JR.

Confidential information must be protected from unauthorized access, inspection and change:

- Confidential information must normally be encrypted when sent outside UM's network.
- Confidential information on data carriers (discs, CDs, USB sticks ...) must be appropriately labelled and stored in suitable rooms or cabinets.
- Confidential information must not be stored on computers not owned by UM.
- When printing confidential information, only in-house printers may be used. The printed material must be picked up immediately and stored safely.
- Employees must observe the clean desk policy stipulating that material containing confidential information must not be left on the table during absence. Confidential material must be kept in locked drawers, cabinets or rooms.
- After printed documents or other media containing confidential information are no longer required, the media must be physically destroyed and data deleted in such a manner as to prevent the recovery of original information (paper shredding; physical destruction of media, such as CDs or DVDs; multiple rewriting of disks with random values)

2.3.3 Protection of confidential information of business partners

In the course of its operating activities, UM also collects information on other organizations and business partners. This information are intended for business use only and are considered confidential.

2.4 *Local computer network*

When connecting to UM's local computer network, the following requirements must be taken into account:

- Users are not allowed to pose as others (masquerade).
- Intercepting network traffic is prohibited.
- Running system or security applications is prohibited except for authorized persons.
- Adding network devices expanding UM's infrastructure (switch, router, hub, modem, wireless access point ...) is not allowed except for authorized persons. Users adding devices to UM's network shall be liable for their use and the activities of other users connected to the device.

If other networks are used on UM's premises, users must consult with and follow the instructions of the security engineer and CCUM, which shall determine conditions for the use of other equipment (applies especially to equipment enabling wireless access).

2.5 *External connections and remote access*

2.5.1 External connections

Connecting systems or networks to other system or networks (including internet) as well as direct connections represent a security threat for UM. Therefore, the following must be observed:

- Access to other networks is permitted only with prior approval and prohibited if UM's security mechanisms are not taken into account.

- Before connecting to UM's information systems and network from external networks, users must be registered and use the permitted *entry points*. Access is granted at the written request and only with the prior approval of the responsible person.

2.5.2 Remote access to UM's information sources

Employees may gain remote access to UM's information sources via the generally available communication routes and encrypted connection to UM's network.

With regard to telecommuting, where information resources owned or managed by UM are not used, the following must be taken into account:

- Users shall not transfer confidential information to the information device.
- If a web browser is used for remote access, it should be closed and all work processes (applications) should be deleted after finishing work.
- Working documents created on a remote information medium must be deleted and the applications closed.

2.6 E-mail and internet

2.6.1 E-mail use

All employees, professors emeriti and those with standstill employment contracts are entitled to their own email account. For these groups, an email address in the following format name.surname@um.si shall be created on the university email sever. Exceptions are permitted if multiple people have the same name or surname, if the total length of name and surname exceeds 20 characters and for other valid reasons. UM's human resources information system represents the source of data on users.

When the employment relationship is terminated, the right to use information resources, including e-mail address, shall be suspended and access to information sources shall be revoked. It is not allowed to reuse an abandoned identity (e-mail) for another user.

At their request, retired employees (former teachers, other members of teaching staff and administrative personnel) are assigned an email address in the following format name.surname@guest.um.si (limitations from the previous paragraph shall apply) on the university email server to which emails from their account used prior to retirement are forwarded. UM's information system represents the source of data on users.

An email address in the format name.surname@guest.um.si can also be assigned to other persons cooperating with UM provided there is a legal basis with financial effect. In this event, the request formulated by the proposer must be approved by the dean or rector. The proposer must make sure that the email address has been revoked after he/she stopped cooperating with UM. Failure to comply with this requirement shall be considered a breach of professional obligations.

Students are typically assigned an e-mail address in the following format name.surname@student.um.si (limitations from the first paragraph of this article shall apply). UM's academic information system represents the source of data on users. Students' right to use UM's information resources is related to their status. It is not allowed to reuse an abandoned identity (e-mail) for another user.

To persons without student status wishing to complete their remaining study obligations, access to UM's information media shall be granted no longer than to the end of the academic year and with the prior the approval of the office for student affairs approving requests on a case-by-case basis. In these cases, the University may charge a fee for access approval and use of UM's information resources. The University's Management Board determines the amount of the fee for access to UM's information services.

For other purposes, such as organisational units, projects, helpdesk, etc., institutional e-mail addresses in the following format institution@um.si may be created. Emails arriving in these mailboxes are used and managed by authorized users. A responsible person must be appointed.

The following rules shall also apply:

- Email addresses for natural persons are created in the following format *name.surname@[guest,student].um.si*. The name can also be shortened (e.g. Nikolaj – Niko, Aleksander - Sašo).
- There are no anonymous email addresses at UM.
- The assigned e-mail account shall be used for communication inside UM. The use of other e-mail accounts for communication within and on behalf of UM is undesirable.
- UM's email system administrator is CCUM, which may allocate individual administrative tasks to administrators at university members.
- The administrator sets up and manages e-mail accounts at the request of competent persons who shall forward the required data.
- In the event of cessation of use or termination of email account, the email address, and consequently access to domain services are terminated. The content shall be deleted after three months from closure. Until the account has been closed, users may ensure the transfer/protection of content themselves. After the account has been closed, the administrator facilitates the protection of content.
- It is prohibited to forward emails to an account outside UM's information system in order to guarantee the availability.

Use of e-mail account

All email users have their own account. For other purposes (e.g. organisational units, projects, helpdesk, etc.), institutional accounts may be created. Emails arriving in these mailboxes are used and managed by authorized users.

Users are not allowed to use their account for reasons other than the requirements of the service, such as gainful activities, non-service activities (questionnaires and surveys, stores, etc.) or political activities. Spamming is prohibited.

Recommendations:

E-mails should be short with few attachments. There is limited space for outgoing and incoming mail. If the limit is exceeded, the email is automatically discarded and the user receives a notification. The limit serves as a measure preventing system overload.

If users receive an email by mistake, which has not been intended for them, the content must be neither saved nor used for any other purpose. In this case, users are obliged to immediately inform the sender and delete the email.

Incoming and outgoing mail

With regard to outgoing mail, users must adhere to the principle of rationality and security. Large attachments should not be sent. However, if they need to be sent, they should be converted into a suitable format using file compression. For security reasons, files with extensions enabling automatic execution should not be sent via email.

Users are not allowed to use their office email address to sign up for mailing lists that are not directly related to their professional obligations or to fill out electronic forms provided there are not directly related to their obligations.

Users are not allowed to redirect mail.

Deleting mail

Due to limited capacities and other limitations, users must manage their e-mail account by archiving or deleting personal or office mail, which is no longer required.

The administrator may take action if users:

- use their account for sending chain letters;
- use their account for spamming.

In the event of prohibited use of the email system, the administrator may temporarily disable access.

2.6.2 Internet use

Users have internet access in order to perform their duties or receive training. Users must act rationally and use the internet only as a working instrument. Internet connection to UM is provided by ARNES. Therefore, the regulations laid down by ARNES[1] must be observed.

With regard to cloud services for data and network storage enabling peer-to-peer communication, the rules published by CCUM must be taken into account. File transmission traffic should be limited to a reasonable extent in order not to hinder the work of other users.

Code of conduct for internet users

For each internet access, a record may be kept in accordance with the information security policy aimed at monitoring internet use for statistical purposes, the planning of server capacities and potential misuse detection. This information is confidential and does not contain personal data of users.

The internet may be used only by users of UM's information systems connected to UM's network.

When connecting to the network or using services, false or misleading personal information must not be used.

It is prohibited to send contributions for nonprofessional or personal polemics, chain letters or any other behaviour distracting other users.

It is prohibited to transfer data with offensive or pornographic content, confidential data, copyrighted data or data owned by other users.

It is prohibited to destroy or modify data owned by other users and to use programmes or processes distracting the normal functioning of information devices forming the network.

The administrator may take action if users:

[1] http://www.arnes.si/pomoc-uporabnikom/pravila-uporabe-omrezja-arnes.html

- use public conference systems for commercial advertising;
- insult, mock or offend other internet users ("flaming");
- preach religious, racial, sexual, national, political or other type of intolerance;
- conduct activities that may cause the sending of large amounts of data and lead to denial of service (DoS in DDoS attack);
- conduct activities that may cause a large number of SYN requests in an attempt to make the system unresponsive to legitimate traffic (SYN attack).

In the event of prohibited internet usage, the administrators may temporarily disable access.

3. Workstation Security Requirements

3.1 Workstation security

Employees are responsible for the security and inalienability of entrusted information resources owned by the University. Users must handle the workstation in such a manner as to prevent unauthorized use. The following rules shall apply to all workstations:

- During breaks or absence, both the keyboard and monitor must be locked.
- Documents containing confidential information must be encrypted. The encryption method shall be prescribed and introduced by CCUM:

If travelling with confidential information on data carriers (paper, CDs, tablets ...), information must be protected in the same manner as mobile devices.

Note:
Passwords not connected to user accounts (e.g. password for startup or disk encryption) do not have to be changed periodically,
If a mobile device or confidential document is stolen, the person in charge of ICT must be informed immediately.

3.2 Security of mobile devices

Mobile devices (PDA, tablets, mobile phones with access to data ...) and data carriers (USB sticks, portable disks ...) containing confidential information or enabling access to confidential information require physical and logical protection. The following measures shall be adopted:

- Users must handle the mobile device in such a manner as to prevent unauthorized use.
- A power-on and timed shutdown password or lock must be activated.

Mobile devices and data carriers must be treated in a sound and prudent manner. They must not be left unattended in unprotected or public places where they are exposed to inspection and theft.

3.3 Malware

Antivirus protection must be installed on each workstation. The relevant antivirus programme is determined by the person responsible for information security. Administrators can help to install antivirus protection.

Users shall take into account the following requirements:

- They are not allowed to intentionally download and spread malware.
- In case of suspected malware, the person responsible for information security must be contacted immediately and his/her instructions followed.
- Users are not allowed to open or run unfamiliar files if they do not know the source.
- If users suspect or discover that antivirus protection is not working properly or is not updated, they must immediately inform the owner or the person responsible for information security.
- Users are not allowed to forward messages concerning real or false new viruses to other users, friends and acquaintances. Suspicious mail must be forwarded to the administrator or security engineer.

3.4 Firewall

If technically possible, a firewall with relevant security settings must be installed on every workstation or mobile device. Firewall prevents both unauthorized access to data and prohibited use of the workstation.

3.5 Workstation access

Unauthorized or non-agreed access to files on the workstation on the part of other users via UM's computer network is prohibited and normally also technically disabled.

Unauthorized or non-agreed remote access between workstations is prohibited. Rules for limited and controlled use of remote access are formulated by the owner of the information resource.

4. Reporting Security Incidents

In case of suspected information security incidents, users must immediately inform the person responsible for information security and follow his/her instructions.

Employees are not allowed to explore security incidents or take action against the attacker/ perpetrator. The person responsible for information security is in charge of security incident management.

5. Transitional and Final Provisions

The Information Security Policy for Users shall apply to all users of UM's information system.

Any violation of the rules laid down in this document shall be considered a breach of professional or academic obligations.

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

The Information Security Policy for Users 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