Information Security Policy for Outsourcers

Index

1. Introduction

The document entitled "Information Security Policy for Outsourcers" contains information considered confidential in accordance with the relevant document classification. Information contained herein may be made available only to UM's employees and outsourcers.

The security of the information system is an integral component of UM's operation.

Due to the complexity of the information system, specific skills and technical know-how are required. Therefore, certain jobs are sometimes outsourced. The aim of the security policy for outsourcers is to ensure supervision of the work performed by outsourcers and to identify risks brought into the business processes by outsourcers.

The document is divided into four chapters defining working methods, access to information media, outsourced work and contractual obligations.

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. Type of Work

Before outsourcers can obtain access to UM's information system, the impact of outsourcing on the business process and especially the uninterrupted operation must be examined. An analysis of implications shall be conducted by the security engineer. The analysis shall also include measures in the event of unexpected termination of the outsourcing agreement.

If the protection of information is managed by an outsourcer, the method for the provision of security with regard to the risk estimate (security customization, identification and examination of all changes related to risks) shall be determined.

The activities of outsourcers are subject to periodic reviews with the purpose of assessing the suitability of outsourcing and ensuring high-quality services.

2.1. Maintenance – unlimited outsourcing

Maintenance comprises all operating activities required for daily work.

Control 1: Monitoring and supervision of outsourcing.

For outsourcing unlimited in time, supervision shall be conducted on the basis of criteria agreed in advance and mutual contractual obligations. In case of sudden cancellation of the outsourcing agreement, alternative procedures and modus operandi in the event of shorter and longer disturbances shall be laid down in the business continuity plan.

2.2. Projects – temporary outsourcing

Projects encompass the development of new products or the installation/configuration of information sources within an agreed time limit. Temporary outsourcing shall also include tasks such as consulting or maintenance despite the fact these are not projects by definition.

Control 2: Monitoring progress with regard to development in accordance with the agreed milestones.

In terms of temporary outsourcing, progress with regard to development or installation shall be monitored in accordance with the agreed project milestones.

Control 3: Measures in the event of deviations from the initial roadmap for implementation.

If deviations from the initial plan occur, all risks shall be re-assessed and measures for a timely project implementation shall be adopted. In the event of larger deviations, UM may terminate the agreement based on risk assessment and complete the project with its own resources or by hiring another outsourcer. With regard to software development, the outsourcing agreement shall also include a provision laying down the ownership of the source program code.

3. Access to Information Resources

The responsible person at UM is obliged to inform outsourcers of the following prerequisites for working on UM's premises:

- Outsources must communicate an advance notice (at least 24 hours) before starting work except in urgent cases where intervention has been requested by the responsible person at UM.
- The following data must be submitted when communicating the advance notice:
  - name and surname of outsourcer,
  - name of outsourced company.

The responsible person at UM shall keep an updated list of outsourcers, which must also include a list of administrators.

3.1. Access eligibility

Control 4: Only outsourcers who signed an outsourcing agreement with UM have access.

Prior to starting work, outsourcers must signed an agreement and, where applicable, sign a confidentiality clause.

Control 5: The procedure for annual verification of access eligibility of outsourcers has been established.

Access rights for individual information resources shall be reviewed on an annual basis. In addition, it shall be established whether access is still required. The verification shall be conducted in cooperation with the owner of the information source.

Control 6: Access of outsourcers to UM's internal information resources must be approved by the management and technically limited to the minimum extent required for the implementation of agreed tasks.

At least once a year, access rights of outsourcers and business partners shall be reviewed. Where possible, access of outsourcers is granted at an explicit request and is limited in time.

Unnecessary access to UM's information resources shall be disabled or permanently revoked. The review shall be conducted by the administrator of the information source. Results shall be submitted to the responsible person at CCUM.

3.2. Access to information resources

Control 7: Each user of UM's information system (employee, business partner, outsourcer, student) shall be assigned a unique label.

University members are responsible for users. Users shall be entered in records of individual systems of university members or CCUM. If systems of university members and CCUM are not interrelated, individual administrators shall be responsible for updating data on users.

In order to provide remote access and access to web applications not owned by UM, separate authentication systems shall be used.

Control 8: The procedure for assigning, changing and deleting user identification has been established.

User identification shall be assigned, changed or deleted in accordance with a certain procedure.

Assigning user accounts:

- On the basis of the outsourcing agreements and data on persons performing work on UM's sources, login parameters for each person requiring access shall be determined.
- Based on business needs and in accordance with his/her powers, the chief officer responsible for the performance of work shall determine access rights in greater detail and submit this information to the administrator of the information resource.
- The administrator of the information resource shall adjust the settings of the information system and inform the chief officer of the executed action.

Deleting user accounts:

- The chief officer responsible for the performance of work shall forward the data required for deletion to the administrator of the information system.
- If the need for access no longer exists (termination of agreement, project completion), access rights to all system shall be terminated.
- The administrator shall disable user account.

Changing user accounts:

- The chief officer responsible for the performance of work shall forward the request for change to the administrator.
- The administrator of the information source shall adjust the settings of the information system and inform the chief officer of the executed action.

Control 9: Authorization for administrator access shall be based on business needs and determined by the owner of the information resource or system.

Administrator authorization may be assigned in accordance with a predefined procedure, which includes need examination and signature of a confidentiality agreement. Authorization shall be removed as soon if possible or within three working days from the detected cessation of the business need at the latest or after receiving a relevant notice.

Control 10: A process for the regular verification of eligibility of external users with an assigned identification for access to production systems has been established.

The verification of eligibility of access to individual information resources shall be implemented for each information source separately. Owners of information resources shall be responsible for reviewing data.

Control11: The identity of external users shall be authenticated before they start using the information system or application.

Authentication methods:

- Active directory (AD),
- Open Lightweight Directory Access Protocol (LDAP),
- Authentication implemented in individual information solutions (e.g. Oracle, OpenVMS).

User authentication represents merely the initial verification. On each information source, access authorization for individual parts or sections shall be implemented after basic authentication.

Control 12: Passwords for privileged access shall be available only to persons requiring it for execution of their tasks. Passwords are not related to the person in exceptional cases only.

All passwords shall be kept in a secure place (sealed envelope). Only administrators of information sources and the communication network have access to passwords. Each password access shall be recorded. After outsourcers stop using passwords for privileged access, all disclosed passwords shall be reset to a new value.

Control 13: Passwords for repeated use that are being used for identity verification shall take into account the following requirements provided the technology enables it:

1. The password must contain at least eight characters.
2. The password must not contain the username.
3. The system automatically requires a change of password every 180 days.
4. The password must not be repeated at least five times or two years.
5. The support service shall set the password to "expired", which means that users must reset the password upon first login.
6. The password should consist of letters and other characters (numbers, punctuation marks, signs).
7. Password requests are defined in great detail on CCUM's website.

Control 14: Passwords for repeated use that are being used for identity verification are protected:

1. Passwords are encrypted (only the cryptographic hash function is recorded) provided they are stored on UM's information systems. If encryption is not possible, access to passwords is limited to authorized system administrators only.
2. Passwords must not be used by multiple users except if control and audits of use according to user are ensured.
3. A security procedure including request verification has been established for password reset.

4. The default password set upon the installation of the operating system or application must be changed during or immediately after the installation.
5. Transmission of decrypted passwords via the internet, public networks or wireless networks is prohibited.

Control 15: All idle sessions shall be disconnected after a certain period of time.

Idle sessions shall be disconnected after a certain period determined by the administrator of the information source. After the expiry of this period, user must log in again.

Control 16: The supplier or the relevant support service shall ensure relevant security settings of user sources enabling access only to authorized users approved by the administrator of the information source.

Prior to the transition into the production environment, default user names must be disabled and default passwords on all systems must be changed.
Access to the information system shall be enabled only for users requiring access for the execution of their tasks.

4. Managing information resources

Control 17: Outsourcers may have network access only with parameters determined by the responsible person.

To access to UM's network and information resources, only software prescribed and approved by the person responsible for information security may be used. The responsible person shall communicate the required parameters for network access to the outsourcer after the agreement has been signed. All technical problems shall be solved by the outsourcer in cooperation with the system administrator or responsible person.

Control 18: Outsourcers may use only inspected and licenced information equipment for network access.

The administrator of UM's information system has the right conduct a security screening of the outsourcer's equipment. In the event of deviations from standards of protection, the administrator has the right to abort (deny) the outsourcer's access to UM's network and/or systems.

Control 19: Outsourcers may perform work only in approved areas.

If outsourcers perform work on UM's premises, they may connect to the network and perform their tasks only in areas approved by the responsible person.

Control 20: Outsourcers may perform work only in the presence of one of UM's employees.

Work in secured places (e.g. server room) and on critical systems may be conducted by outsourcers only in the presence of one of UM's employees

Control 21: Remote access for telework shall be approved on a case-by-case basis.

Access shall be approved by the responsible person who must make sure that the outsourcer's access to UM's network and/or information resource is enabled in accordance with the prescribed software and relevant parameters. Remote access is limited in time and should not be used outside normal working hours unless specifically approved.

Control 22: Outsourcers must use the prescribed software to connect to UM's network and/or information resource.

Access from workstations outside UM's network shall be enabled via a secure connection with the prescribed client.

Control 23: Working via an external connection is possible only for interventions agreed in advance.

Control 24: In the development phase, external software developers must conduct a product security testing.

Test parameters for security testing shall be determined by the project manager in cooperation with the person responsible for information security. Test results must be submitted either immediately after testing or later but prior to software implementation.

Control 25: In the context of final product version preparation phase, external software developers must conduct a security screening (malware screening).

The implementation of this requirement must include the following:

- Before being transferred to the production environment, the application must undergo a security screening.
- A security screening must also be conducted for new versions of existing applications.

Control 26: Control records must be created for all successful and unsuccessful attempts to access UM's network from external locations.

All records must be kept in a separate system in UM's network. No exceptions are allowed.
Records must be reviewed on a weekly basis (automatically or manually) in order to detect systematic attacks.

Control 27: Information on activities must include at least the following parameters: date and time, type of access attempt, user identification.

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

Control 28: On completion of work, outsourcers must submit all UM material acquired at UM during the execution of the agreement.

Outsourcers must submit all material obtained during the execution of contractual obligations from the employees at UM prior to completion of activities.

5. Recommended contractual provisions

Before enabling access to UM's information sources or network, a written outsourcing agreement must be concluded.

The person responsible for information security shall assist the legal department in the preparation of the agreement by identifying risks, planning relevant controls and the reporting system and later by overseeing the execution of contractual obligations.

The agreement shall lay down work methods and access to UM's network and services, which are the subject of outsourcing or maintenance. Detailed data on access shall include the name and surname of the employee of the outsourced company and a confidentiality clause.

The outsourcing agreement shall include:

- security obligations of outsourcers and their subcontractors;
- maintenance and testing methods for equipment, which is the subject of the outsourcing agreement, in order to protect confidentiality and integrity of information;
- procedures and security mechanisms to be taken into account in the outsourcer's access;
- method of ensuring protection of equipment and data brought in or out of UM;
- the right of authorized employees to continuously monitor the execution of tasks on the part of outsourcers;
- ensuring compliance of the outsourcer's activities with the legislation and regulations in force;
- criteria on the basis of which the contracting entity (UM) and outsourcers may assess the quality of delivered services.

Prior to the execution of the outsourcing agreement, the provisions shall be harmonized in such a manner as to not impair the following:

- implementation of operating activities,
- risk management process,
- internal control system.

This shall apply especially to agreements drawn up by outsourcers.

Contractual obligations of outsourcers shall be determined on the basis of requirements arising out of quality assurance with regard to services and identified risks related to services or operating activities performed by outsourcers on behalf of UM.

In order to ensure the required degree of quality of the service, the agreement shall include quantitative and/or qualitative criteria on the basis of which outsourcers and UM can conduct quality assessment.

Before using the UM's name for any purpose (e.g. marketing, references), outsourcers must obtain the consent of the responsible person at UM.

Controls in outsourcing agreements

Control 1: Work may be performed only by outsourcers who concluded an agreement with UM. The outsourced company shall determine who will perform the tasks. Each change of person requiring access to UM's sources, must be communicated in advance.

Control 2: All interventions shall normally be conducted only in testing or development environment. In exceptional cases, direct interventions in the production environment are allowed. Any interventions in the production environment must be approved in advance by the responsible person and suitably monitored.

Control 3: Outsourcers must take into account all internal procedures and security mechanisms for working with UM's information resources.

Control 4: The execution of tasks must be dully notified at least 24 hours prior to the intervention except in urgent cases where the intervention is requested by the responsible person at UM.

Control 5: The notification must include the following data:

- Name and surname of the person conducting the intervention;
- Name of outsourced company;
- Purpose or description of intervention.

Control 6: All interventions of outsourcers must preserve confidentiality, availability and integrity of existing information.

Control 7: The responsible person at UM has the right to continuously monitor the execution of the outsourcer's tasks.

Control 8: Outsourcers may perform work in approved premises or telework provided approval has been granted. With regard to telework, outsourcers must take into account all prescribed security mechanisms.

Control 9: Outsourcers may perform tasks requiring physical access only in the presence of the responsible person at UM.

Control 10: Access for teleworking shall be approved on a case-by-case basis.

Control 11: Outsourcers may connect to the network only with parameters determined/communicated by the responsible person at UM.

Control 12: Outsourcers must use the prescribed software and work methods to connect to UM's network.

Control 13: Working via a permanent external connection is possible only for interventions agreed in advance.

Control 14: Longer projects/interventions shall be monitored in order to track progress with regard to development in accordance with the determined milestones.

Control 15: Each intervention shall be recorded in order to monitor and assess quality and supervise outsourcers.

Control 16: Upon completion of the intervention, outsourcers must prepare a report on the conduct and success of the intervention. The report shall be submitted to the responsible person at UM.

Control 17: Upon completion of the intervention, outsourcers must submit all information obtained in the context of the project to the responsible person at UM.

Control 18: The intervention or activity shall be completed after the report has been submitted and approved. The report shall be approved by the responsible person at UM.

6. 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 Outsourcers shall apply to all outsourcers of UM.

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

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