UPPSALA
UNIVERSITET

Dnr UFV 2020/2599

Procurement and operation of IT systems

Procedures for information security

Ratified by the Chief Security Officer	2017-01-16
Latest revision date	2021-05-07
Translation date	2021-10-07

Innehållsförteckning

1 Introduction 3

2 Responsiblity 3

2.1 Compliance 3

2.2 Procedure updates 4

3 Definitions 4

4 Scope 4

4.1 Security requirements for procuring systems and other external IT services 4

Requirement specification for procurement and call-off agreement 5

Establishing a supplier agreement/contract 5

4.2 Asset management 6

4.3 Documentation of operational environments 7

4.4 Requirements for operational environments 7

Access control 7

Cryptographic storage and key management 8

Physical and environmental security 8

Operations security 9

Communications security 10

4.5 Connection to the university's network 10

4.6 Backup in operational environments 11

4.7 Logging 11

Log management 12

Log management in association with The General Data Protection Regulation (GDPR) 12

Log disclosure 13

1 Introduction

These procedures complement Uppsala University's procedures on the use of IT systems (UFV 2014/1171), and are based on the university's guidelines for security and safety at Uppsala University (UFV 2009/1929), guidelines regarding IT (UFV 2016/896) as well as the Swedish Civil Contingency Agency's regulations on information security for governmental authorities (MSBFS 2020:6) and regulations on security measures in information systems for government authorities (MSBFS 2020:7).

These procedures have been established for the purpose of

- ensuring that the procured systems and services meet the university's requirements for adequate information security
- Maintaining a high level of security in operating environments and in the university's computer network
- guaranteeing access to information and systems in the event of loss or corruption of information in a regular storage environment or similar event
- ensuring secure log management for all servers and other equipment that provide online services at Uppsala University
- ensuring that personal information processed in systems and services are in accordance with the General Data Protection Regulation (GDPR).

2 Responsiblity

2.1 Compliance

Responsibility for compliance with the procedures lies with, respectively:

Heads of departments/equivalents at their departments, divisions or equivalents.

Campus directors for compliance with the procedures when coordinating their campus areas.

System owners, e-area managers/equivalents for compliance with the procedures in their development and administrative work as well as in their operational duties. Responsibility for compliance with these procedures also lies with internal and external parties that are employed for these purposes. The responsibilities of the employed parties regarding the procedures must be defined in the so-called service-level agreement.

The Chief Security Officer for planning, coordinating and following up as well as monitoring compliance.

All parties engaged in any activity pertaining to the university must follow the procedures.

2.2 Procedure updates

The Chief Security Officer is responsible for keeping the procedures up to date and creating related supporting documents.

3 Definitions

Information classification is a fundamental process where the information handled, for example in an IT system, is assessed based on the aspects of confidentiality, integrity and availability.

System owner describes, in this document, the role that has the overall responsibility for the management and operation of one or more IT systems. The role of e-area manager, which is used within the parts of the university that implement the university's e-administration model, is included in the term system owner.

Outsourcing is, according to Oxford reference dictionary, described as "*The buying in of components, sub-assemblies, finished products, and services from outside suppliers rather than by supplying them internally.*"

4 Scope

Deviations from the following procedures must be documented.

4.1 Security requirements for procuring systems and other external IT services

The process of procuring a system or employing a supplier for an external IT service must always be preceded by information classification and risk assessment, as well as a requirement analysis based on the result of the information classification carried out- see section 4.2 Asset management below.

When using supplier's services for storage, functionality, computing capacity etc. where these services are entirely or partly outside the university's internal IT environment, the following steps must be included as an introductory part of the procurement procedure:

- Contact servicedesk (servicedesk@uu.se or 018/471 44 00) to find out whether the university already provides a central service that meets the current need.
- See the procedures for secure information management, section 4.2, “Use of cloud services and other external IT services”.
- The procurement process must include dialogue with representatives of the Legal Affairs Division and the Security Division. In a case where the handling involves personal information, the university's data protection officer must also

be included in the dialogue. The question of whether it is appropriate to use an external supplier needs to be assessed in each unique situation.
- Results from information classification/requirement analysis, dialogue and the decision-making process must always be documented.

If the system in question handles sensitive information, a risk assessment must be done before suppliers or other external parties are given access to the information.

If personal information is handled, the supplier must sign a personal data assistant agreement.

Relevant information security requirements must be defined in an agreement with the supplier. This agreement must also include a confidentiality agreement. All personnel hired from suppliers to work with the system/systems must be informed about the security and confidentiality requirements that have been agreed upon.

Requirement specification for procurement and call-off agreement

When a system or service is procured, relevant information security requirements must be included as part of the requirement specification. The result from the requirement analysis carried out, sets out which requirements should apply in the context. In general the requirement specification in the procurement documents should provide answers to the following questions:

- How the supplier monitors and follows up information about new vulnerabilities regarding the operational environment, and handles IT security incidents
- How the university's information is protected from the supplier's other clients
- How connections to underlying or adjacent systems (e.g., LTI) are handled
- In which country/countries the information is stored and handled, both in the system and any underlying systems
- Requirements regarding the informing of the client in the event of migration of data between the supplier and a subcontractor or between countries
- Which procedures should be applied to the integrated systems developed by the university or in consultation between the university and the supplier, for example in case of upgrades, backward compatibility and more
- How logs are handled and how the university can access the log data when necessary
- How the university can access its information if/when the system is discontinued
- How the system is archived
- How the supplier prioritize its customers in the event of major system failure.

Establishing a supplier agreement/contract

When an operational task is outsourced to another party, a contract must be established between the parties. The contract should among other things define

- Impact on, and dependence on other services
- Any third-party services that are included in the agreement
- The respective responsibilities of the client and the supplier
- Procedures for backup and backup verification as well as restore
- Procedures for restoring the service
- The accessibility time frame agreed upon, i.e. the agreed upon time frame that the service must function, and have support of some kind
- Agreed upon support and issue management process
- Procedures for change management (problems, incidents and change processes where ITIL is applied)
- Procedures for reporting, including announcement of downtime - planned and unplanned
- The level of automation of the monitoring process
- Continuity management in the event of major system failure
- Procedures for supplier contact and status update meetings

A review and, if needed, a revision, of existing agreements must be done annually.

4.2 Asset management

An information classification must always be carried out as an initial step – regardless of whether a system is put into production for the university to operate, a supplier is employed, or an outsourced operational service is procured.

When conducting an information classification, the information's need for security measures is assessed based on the requirements for confidentiality, integrity and availability. As a result of the requirement analysis that follows the information classification, some requirements are imposed on the system/service.

When procuring systems and services, the requirements that are defined in the requirement analysis must, as far as possible, be clearly stated in the relevant procurement documents. For systems that are already in operation, the results of previous requirement analyses must be reviewed regularly. Requirements that are not met must be subject to a risk assessment and addressed based on the priority specified by the risk assessment.

The university's procedures for risk management *(UFV 2018/211)* provide guidance for conducting information classification and requirement analysis. They also contain a section regarding risk analysis that ideally can be used for conducting the risk assessment.

NB! An outsourced operational service where storage according to the EU’s General Data Protection Regulation (GDPR) cannot be guaranteed, must not be used for the storage of confidential information or sensitive personal information.

According to GDPR the following are viewed as sensitive personal information: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, personal data relating to health or sexual life, genetic data and biometric data uniquely identifying a person.

4.3 Documentation of operational environments

The university must maintain updated documentation of:

- hardware and software used in each individual information system,
- dependencies between different internal information systems as well as dependencies on information systems hosted by external parties,
- which information systems are in need of more extensive protection; and
- which information systems are essential for the authority's ability to carry out its mission

4.4 Requirements for operational environments

As a result of the requirement analysis (see section 4.2 above), a set of requirements is obtained directly adapted to the level of security that the information classification carried out indicates.

The set of requirements obtained from requirement analysis is largely based on the requirements described in the sections below.

Access control

All systems should, if possible, be linked to the university's joint web login and be used in accordance with the password management policy. Passwords used for other systems must also be created, handled and used in accordance with the university's *procedures for password management (UFV 2013/1490).*

For traceability purposes, all system users must have unique user identities, i.e. no group identities may exist. Exceptions may be granted in specific cases, following a dialogue with the Security Division.

A documented procedure for access administration and assignment of access rights must be implemented and followed. The access administration procedures must specify procedures for allowing, changing and revoking access to information, systems and services. They must also state that the allocation of sysadmin and user accounts with privileged access rights must be limited, reviewed and revised at regular intervals.

It should be possible to restrict users' access to systems and databases based on role, organizational affiliation, etc.

Access to services and tools (operating systems, network services, system tools, etc.) with possible impact on system's security, as well as the use of tools (e.g., SQL tools)

that might be capable of overriding security and logging measures in the system, must be restricted and tightly controlled.

Authentication to systems and services containing sensitive information must be done with so-called multifactor authentication (MFA). Multifactor authentication must also be used for university and contract personnel's access to the production environment via external network as well as system administrative access to information systems.

If systems containing sensitive information are accessed remotely, the university's VPN services for secure internet connection must be used.

IT systems must be protected against unauthorized access by replacing preset authentication information and removing or blocking redundant system functions.

Software vendors' and other service personnel's access to sensitive information must be restricted and regulated in and confidentiality agreement. Contact the Security division (security@uu.se) for help with preparing confidentiality agreements.

Cryptographic storage and key management

When storing sensitive information, encryption of disks, separate files and databases must be considered. The need for cryptographic storage is determined based on other measures protecting the information.

The Cryptographic algorithms and key lengths used must be in accordance with recommendations from NIST - see NIST's[1] publication SP 800-131.

The life cycle of cryptographic keys and all phases of key management must be documented and procedures for key management must be verified at least once a year or when there is a change.

All parties involved in a key exchange should be identified with strong authentication. Exchange of cryptographic keys must take place over an encrypted connection.

Regular exchanges of cryptographic keys should be considered. The context determines the need for exchange and at what time intervals the exchange should take place.

Cryptographic keys shall, depending on the purpose of the keys and how they are used, be stored in the safest possible way and in as few copies as possible, however, at least one backup copy must be available.

Physical and environmental security

Premises where the system/systems operate or where data media are stored must be protected with appropriate exterior protection - locks, alarms, entry systems with key card and pass code etc. to minimize the risk of unauthorized access.

Special protection measures should be considered for premises containing sensitive or critical information or equipment.

Only authorized personnel should have access to the premises or spaces where such restrictions apply. Documented procedures must be in place and followed for access to, and work in, the premises.

[1] https://csrc.nist.gov/

The system equipment must be located and protected in such a way that the risks of environmental threats (temperature, fire, water) are minimized. The physical parts (hard drives, cables, fans, etc.) must be maintained and updated in a correct manner that ensures continued availability and integrity. These requirements should be regulated in the agreement.

If the system/systems have high or special requirements for availability, an uninterruptible power supply (UPS) must be installed by the IT operations supplier who must also be able to present procedures and documentation that regular tests of the UPS system are carried out.

Documented regulations and procedures must be in place for the physical transport of data, for example via portable storage media such as USB sticks.

When equipment that may contain protection-worthy information is to be moved between users within or between departments or is to be decommissioned or disposed of (discarded, exchanged or sold), the university's procedures for handling discared IT equipment (UFV 2014/1279) must be followed.

Operations security

A formalized change management (e.g. change management where ITIL is applied) must exist and be applied by the IT operations supplier regarding new versions of current services, hardware, system software and operating systems. In addition, a formalized problem and incident management procedure must be applied by the IT operations supplier.

Development, test and production environments must be separated to reduce the risk of unauthorized access or changes in production environments.

If the system has high or special requirements (classified at level 3) for the availability aspect, the supplier must monitor and, if necessary, adjust the capacity requirement. The IT operations supplier must also make regular forecasts of future capacity requirement.

User activities in the system/systems, as well as the activities of system operators and administrators, must be logged and the logs must be saved in a secure manner. See section 4.6 *Logging* below. Logs and logging tools must be protected against unauthorized access and tampering.

The system(s) must be connected to a Network Time Protocol (ntp) for time synchronization to one and the same reference source. The university's central time servers must be used by the systems that are connected to the university's network.

Backups of databases, software and other critical features or parameters must be taken and tested regularly.

Software that provides protection against malicious code must be used. For IT systems where such software is not available, other measures that provide equivalent protection must be taken.

The university must prevent the spread of incidents and reduce the consequences of attacks by placing IT systems with different functions in separate network segments in the production environment. Network traffic must be filtered so that only the necessary data is communicated between different network segments.

Communications security

The networks used for data communication must be built, administered and monitored by the IT operations supplier in a manner that ensures adequate security.

Security measures that meet the system's requirements for secure data communication in the network services, must be agreed upon and specified in the contract with the IT operations supplier.

When communicating sensitive information to other systems, other authorities or other external parties, protection measures regarding processing, storage and publication of the information must be regulated in a contract.

If the system handles information (classified at level 3) with high or special requirements on confidentiality, the information must be communicated in an encrypted form. All traffic for authentication and all personal information must be encrypted.

All ports and protocols that the system uses must be documented for the purpose of establishing regulations for perimeter protection (firewalls etc.).

For web servers for which secure verification of the server's identity is an important protection measure, SSL certificates obtained through the university's SUNET membership should be used, since it provides advanced protection against irregularities. Certificates obtained via SUNET are protected by an authentication system provided by SWAMID, where individuals are given the right to order certificates for their own domains and where the certificate orders are always approved by a third party.

4.5 Connection to the university’s network

Network equipment, such as routers and switches, must not be connected to the network without the permission of the IT manager or the person responsible for the network segment.
Routers with wireless networks must be configured with the strongest encryption possible.

The department/equivalent must have a list of the installed equipment. Sufficient documentation must be available to make it possible to locate the connected equipment. The documentation must state

- who is responsible for the equipment,
- purpose, and
- identification (e.g. MAC address, router’s SSID.

Only services that are used, and that are in line with the purpose for which the equipment is employed, may be activated on the equipment.
Services that are not used must be deactivated.

Equipment and all software must be up to date. If the supplier no longer maintains the equipment, it should not be connected to the university's network.
NB! Exceptions to this may be granted in specific cases, following a dialogue with the Security Division.

The equipment must be located so that physical access is only possible for authorized personnel.

If the network equipment is used for storing sensitive information, it must be encrypted.

4.6 Backup in operational environments

Backups must be made regularly and include all information that is of value to the university and that is difficult, costly or time consuming to restore.

The system owner must decide which information needs to be backed up, as well as the backup and verification intervals, which are regulated in a contract.

A procedure for restoring the system, comparable to that of a new installation, including all customizations and all configuration as well as restore of the backup, must be established and documented and managed. Backups must be regularly verified according to the method and interval stated in the contract.

Backups should be stored in several generations so that information can be restored even if problems arise when using the most recent backup.

Backups must be stored securely and separate from the computers they back up. If the information includes parts that according to the information classification belong to the special requirements level (classified at level 3), encryption of the backup must be considered.

In addition to the backups that are taken regularly, according to the agreed upon interval, backups must take place before and after the implementation of a major change in the system or in the operational environment. IT systems and stored information must, as far as possible, be able to be recreated on other hardware.

4.7 Logging

The term *Log* in this context refers to the information that is continuously collected about the operations performed in a system or in a network.

The university must, in order to ensure traceability in IT systems, log the following security-related events:

- Unauthorized access and attempts to access to the IT environment and specific information systems without authorization.

- Changes to configurations and security features that require privileged rights.
- Changes in permissions for users and information systems.
- Access to information that is deemed to be in need of more extensive protection.

Security logs are used as a collective term for authentication logs, traffic logs and other logs that enable traceability to an individual. Security logs are stored primarily for forensic purposes, e.g. in the investigation of attempted or successful intrusions.

Application logs are primarily used as a tool to track events in a specific IT-based system. *Transaction logs* or *System Logs* can be used synonymously. For certain types of information, such as financial transactions, there is legislation that sets out the rules for how logging should take place.

Log management

The following applies to all servers and other equipment that provide network-based services at Uppsala University.

System owners must decide which logs to store. As a minimum, all authentication logs and access logs from network-based services should be stored.

Application logs must be stored for at least 6 months or for as long as it is required by law. The duration for which application logs are stored must be agreed upon with the IT operations supplier.

When updating information that is classified at level 3, the logging should include information about who performed the transaction and what was updated.

If information stored in a log file can be linked to an individual, it is considered personal information. It is not permitted to use logs in a way that violates the privacy rights of an individual. For example, the use of logs to, for whatever reason, map a person's browsing habits on the Internet is not permitted.

All logs must be protected against unauthorized access and unintentional change. Moreover, logs must be stored in a secure manner, preferably not in the immediate vicinity of the operations premises. Only persons who in the performance of their duties are in need of the information in the logs should be given access.

Log management in association with The General Data Protection Regulation (GDPR)

One of the main purposes of logging is to protect information from unauthorized access and unauthorized handling. Proper logging ensures the fulfilment of GDPR’s basic requirement that personal information must be protected from unauthorized access, loss or corruption.

Regarding the duration for which the logs that contain personal information are stored, one of the basic principles of GDPR applies. This principle states that personal information must not be stored for longer than necessary for its purpose and must then be deleted. This GDPR principle overrides the requirement that logs must be stored for

at least 6 months. Depending on the purpose of the logging, in some cases logs containing personal information must be stored for a much shorter period than 6 months. However, the stated period of 6 months does not constitute an absolute time limit in this context. A balance based on the principles of the GDPR needs to be struck in the context in question.

When logging of personal information, it is also important to take account of another GDPR principle that states that only data that has a clear purpose may be stored. There must therefore be a clear purpose for logging specific piece of personal information.

Log disclosure

The Principle of public access to official records is enshrined in the Freedom of the Press Act and means that everyone is entitled to request a public document from a public authority. The term public document includes texts, images and sound recordings that have been sent to or created by an authority.
Information created automatically via IT systems, for example in the form of logs, can also constitute a public document. Public documents are normally public, but disclosure of a document must always be preceded by an assessment.

To ensure that the disclosure of information does not risk violating an individual's privacy rights, the following applies to all disclosure of logs, security logs as well as transaction logs:

- Requests for disclosure of logs, security logs as well as transaction logs - or information included in the logs, must be addressed to the current system owner. It is the system owner who is responsible to assess whether or not the disclosure of the requested information risks violating an individual's privacy rights.
- The Security Division assists, if necessary, with identifying the concerned system owner, as well as with uncertainties with disclosure assessment. Information from the university's access control system that reveals a person's movement patterns in the university's premises, camera logs and information about a person's browsing habits on the internet, are clear examples of information linked to personal privacy.
- An individual always has the right to request their own information, i.e., all information that is stored at the authority or in a certain system with an identifiable connection to that specific person.