Dnr UFV 2018/668

UPPSALA
UNIVERSITET

Secure
Information management

Procedures for information security

Ratified by the Chief Security Officer 2018-03-23
Latest revision date 2022-12-15
Translation date 2022-12-15

Table of contents

1 Introduction

The following procedures 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).

The procedures have been established for the purpose of

- Ensuring that all handling of information meets the university's requirements for adequate information security.
- Providing advice and support to individual employees and heads of departments or equivalent when considering using cloud services.
- Demonstrating the importance of carrying out information classifications and requirement analysis in all activities where information is handled.

The university's work with information security is conducted in accordance with the Swedish Civil Contingency Agency's regulations on information security for governmental authorities (MSBFS 2020:6) and the Swedish standards SS-ISO / IEC 27001 and SS-EN ISO / IEC 27002. The standards mentioned form the basis of the university's guidelines for information security as well as the materials and documents created for the implementation of information classification and requirement analysis. In many cases, information management is affected by legal aspects as well. However, the scope of this document is limited to the security aspects of information management.

2 Responsibility

2.1 Compliance

Responsibility for compliance with the guidelines lies with, respectively:

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

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

System owners, e-area managers/equivalents for compliance with the guidelines in their development and administrative work as well as in their operational duties. Responsibility for compliance with these guidelines also lies with internal and external parties that are employed for these purposes. The responsibilities of the employed parties regarding the guidelines 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 guidelines.

2.2 Guideline updates

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

3 Definitions

Information worthy of protection. Information that is subject to confidentiality concerns or is otherwise to be regarded as confidential, contains sensitive personal information, is business-critical, licensed or protected by laws and regulations. Also called sensitive information.

Business-critical information. Information that can be critical for e.g., an individual researcher, a group of researchers, a department or critical for the whole university – such as dissertations in the original, contracts in the original, data/information that has been collected over a long period of time and/or that cannot be recreated, information collected about valuable property etc.

Unencrypted information is displayed in plaintext. *Encryption* means that information is converted into a code and is only readable by those who have access to the corresponding encryption key.

Personal information. Any information related directly or indirectly to a natural identifiable living person is considered to be personal information according to the General Data protection Regulation (GDPR). Images (photos) and sound recordings of individuals that are processed on a computer can also be viewed as personal information, even if no names are mentioned. Encrypted information and various types of electronic identifiers, such as an IP address, are considered to be personal information if they can be linked to a natural person.

Sensitive personal information. The following personal information is considered to be sensitive:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- membership in a trade union
- health-related information
- a person's sexual life or sexual orientation
- Genetic data and
- biometric data that uniquely identifies a person

Genetic data is personal data that relates to an individual's inherited or acquired genetic characteristics, which can be obtained from a DNA analysis.

Biometric data are personal data relating to an individual's physical, physiological or behavioral characteristics obtained through special technical procedures, such as fingerprint data.

Information classification is a fundamental process where the information being handled is assessed based on the aspects of confidentiality, integrity and availability.

Requirement analysis. Is a process where the system or systems that are relevant to the context are checked against the result of the performed information classification, to ensure that the system lives up to a sufficient level of security.

Risk management. Methods for identifying possible risks and planning for risk mitigation measures. The procedures for risk management (UFV 2018/211) describes the risk management methods used at Uppsala University and includes, among others, guidelines for conducting information classification and requirement analysis.

4 Scope

4.1 Information in IT systems and storage solutions

The following applies to all IT systems and storage solutions used for processing information at the university. The guidelines apply to central solutions as well as solutions provided by campuses or departments/equivalent.

Information classification is the basis for secure information management – a process where the required level of protection of the information is determined based on the aspects of confidentiality, integrity and availability. The results from the performed information classifications together with associated risk assessments and requirement analyses determine which protection measures should be required from the systems /storage solutions used in the university.

Information classifications and requirement analyses aimed at university's central systems (Raindance, Primula, Ladok, etc.) should be performed in line with the work carried out in the university's e-administration. Departments/equivalents and managers are responsible for carrying out these processes for systems procured for local use.

Support tools for carrying out information classification and requirement analysis are available at Policys and Regulations (regler.uu.se). They have been provided by the university's security division, who can also assist with performing these tasks.

Procedures and support for performing information classification and requirement analysis can be found in the procedures for risk management *(UFV 2018/211).*

A system that has not yet been subject to requirement analysis is considered to fulfill the classification level of 111 in accordance with the description in Risk mangement.

4.2 Use of cloud services and other external IT-services

4.2.1 General

It is becoming increasingly common for organizations and government agencies to use cloud services and other types of external IT services. These services offer many benefits such as resource efficiency as well as increased availability and flexibility.

However, there is uncertainty about what is appropriate or legal to store in an external IT environment. Cloud services are often provided by international companies subject to the laws and regulations of other countries, and information stored in the cloud can in practice be processed in many different countries.

Defining cloud services and what distinguishes them from other external IT services and the so-called outsourcing services is very challenging. In recent years, there has been a shift in what the term entails and how it is used in comparison with previous definitions. Currently, within the public sector as well as in general, the concept of cloud services is often used as a multifaceted generic term. Hereafter in this section, the term external IT services, as a generic term, is used.

From the information security point of view, definitions and distinctions between external IT services are less important. Procuring and using third party services such as storage, functionalities, computing capacity etc., where these services are partly or entirely outside of the university's internal IT environment, necessitate fulfillment of specific requirements. This applies regardless of which term is used to refer to this phenomenon – the information security management aspect of it is always the same when using external IT services.

In order to know how to safeguard information, it is necessary to know what information is actually being handled in the context in question and from which aspects requirements for information management arise. Information classification, risk assessment and requirement analysis, see section 4.1 above, become of great importance when assessing whether it is appropriate to use external IT services in a given case.

See also *Procurement and operation of IT systems* (UFV 2020/2599), section 4.1.

4.2.2. User responsibility

The use of external IT services requires users to have an overview of the type of information that they, their group, their project or their division intend to handle with the external service, the required level of protection of the information and in what ways it will be managed and accessed.

Whether it is appropriate to use an external IT service needs to be assessed in each unique case. The university's procedures for *Procurement and operation of IT systems (UFV 2020/2599),* section 4.1, describe the processes that must be performed when procuring external IT services.

These processes include elements such as performing information classification /requirement analysis, dialogue with the legal affairs division, the security division and the university's data protection officer are essential in this context. These elements are even more crucial when use of external IT services is considered for handling sensitive personal information or classified information. Inadequate or incorrect handling of sensitive information can have legal consequences as well as lead to serious information security incidents.

N.B! When IT services are procured by solely approving the provider’s standard terms, it is unlikely that a complete requirement analysis can be performed. In accordance with the principle in section 4.1 above, these types of services do not meet a classification level higher than 111.

Processing personal information in external IT-services

The university is responsible for the handling of personal information even when an external party handles it on behalf of the university. Personal information includes all information that can, directly or indirectly, identify an individual.

The handling of personal information, e.g. storing or processing, must be in accordance with applicable legislations, and the necessary security measures must be taken to protect the information. The overall responsibility for this lies with the heads of departments, directors or equivalent. However, individual employees are also responsible for what they store in external IT services.

Login, passwords and user profiles

If the service in question cannot be accessed via the university's Joint Web Login, and requires that a separate user profile should be created for that specific service, the user account or the password used for the Joint Web Login must not be used.

Users must follow the university's guidelines for password management even when using external IT services. The procedures for password management can be found in Policys and Regulations (regler.uu.se).

Contractual terms

IT service providers often use standard agreements for all of their customers/users. These agreements are often created in advance with little or no room for adjustments. Regardless of whether standard or specific agreements are used, it is important to examine the way the agreement addresses various issues.

Anyone who procures an external IT service must read the terms of the agreement before accepting them. This is especially important when the agreement involves images, since the copyright of the images must be taken into account. If the external IT service provider is to be granted partial or total copyright of the images, this must be approved by the owner of the images.

4.3 Miscellaneous information handling

Most of the information handled daily at the university is stored and processed outside of the specific systems used at the university. It can, for example, be part of the procedures and processes surrounding the used systems or be about personal use of different standard programs and storage media. In addition to the requirements that, based on the performed requirement analyses, are placed on used systems there are guidelines and procedures that need to be followed when handling information in this manner.

The procedures for information security (UFV 2017/93) can be found in the university's Policys and Regulations (regler.uu.se). There you can also find guidelines for handling public documents as well as guidelines that describe correct information handling in more detail.

4.31. General

The required level of protection for the information needs to be determined even for the information that is processed outside the university's central and local systems. Information classifications that are carried out within the different parts of the university, such as departments/equivalents, need to include all the information that is handled in the context.

4.3.2 Communication and storage of information

Information must, even when processed outside of the university's central and local systems, be communicated and stored in a way that corresponds to the required level of protection. Section 4.4 below, *Regulations for secure information management*, sets out the protection measures that should apply to information with different degrees of sensitivity relating to the aspects of *confidentiality, integrity and availability.*

Currently, the availability of university-wide services for storing and sharing information is limited. Most of such services are offered by the University IT Services. There might also be some services offered at a few departments.
An organizational unit that operates and provides a service for sharing and storing information is also responsible for assessing the level of security within the service.

4.3.3. Personal conduct and responsibility

The security that protects the information is not stronger than the weakest link. Information that has been evaluated as sensitive when the security of a system has been assessed needs to be provided adequate protection in all types of handling.

Below are a few points to keep in mind for anyone who in the performance of their duties handles information that is evaluated as sensitive:

- Personal equipment used for handling and storing information must be protected from unauthorized access and kept under proper supervision.
- Software in IT devices, such as personal computers, smartphones, etc., used for handling of information must be kept up to date.

- IT devices must be equipped with an automatic screen saver/lock.
- When storing information on a USB flash drive, the information should be stored in encrypted form.
- Devices used in open office environments should be locked when left unattended.
- Non-digital information must also be provided protection that corresponds to the sensitivity of the information - see section 4.3.4 below.

The university's security and safety division regularly offers courses in information security. These courses put a strong focus on personal handling of information and personal devices. More information can be found in the university's Staff Portal (mp.uu.se) under Support and service, Security, Courses Workshops.

4.3.4 Non-digital information

At Uppsala University, all information must be handled in a secure and efficient manner. Information security applies to all the university's information assets, regardless of whether they are handled manually or processed with the help of IT, in whatever form or environment they may be found.

It is crucial to find a reasonable and adequate level of security in the area of activity in question. This is a challenge in open office environments and must be dealt with based on the type of information that is handled and the conditions of the environment in question. The conditions differ based on the physical environment.

Paper documents, magnetic tapes, images etc. may contain personal, sensitive and confidential information and must therefore be handled based on how the information in question is classified.

Storage and handling

For information where the confidentiality aspect is classified at level 2 or 3, appropriate protection measures must be implemented, for example an office room with limited access that is kept locked when unattended, or storage in a lockable cabinet.

Written material that contains confidential information must not be available for unauthorized reading. The material must be handled so that unauthorized persons cannot gain access to it. The "Clear desk" principle should be applied- sensitive material should not be left in the open and accessible. This also applies to notes and post-it notes.

Furthermore, it is essential to ensure that any sensitive documents taken outside the office environment are handled with adequate care.

Destruction

Paper documents that contain confidential information must be shredded with a so-called crosscut shredder, or destroyed in another secure way. For other media, the procedures described in *Managing decommissioned (phased out) IT equipment* (Dnr 2014/1279), section 5.3, must be followed.

4.4 Regulations for secure information management

For information about confidentiality, integrity and availability aspects as well as the existing levels of classification, see *Risk management* (UFV 2018/211).

4.4.1 Confidentiality

Regulations for class 0 *(public information)*

- The information may be stored on the workstation's local hard disk, file servers and removable media without restrictions. To assess whether it is also appropriate to store the information in a cloud service - see section 4.2, Use of cloud services, or contact the university's security and safety division for guidance.
- The information may be transmitted electronically, for example via e-mail or web, without encryption.
- The information may be made available for external access.
- The information may be sent by fax and post, both internally and externally.

Regulation for class 1

- The information may be stored on the workstation's local hard disk, file servers and removable media without restrictions. To assess whether it is also appropriate to store the information in a cloud service - see section 4.2, Use of cloud services, or contact the university's security and safety division for guidance.
- The information may be stored in a storage solution that meet the requirements for the security level 1 for the confidentiality aspect.
- The information may be transmitted electronically, for example via e-mail or web, without encryption.
- The information may be made available for external access provided that the sender is identified.
- The information may be sent by fax and post, both internally and externally.

Regulation for class 2

- The information may be stored on the workstation's local hard disk or removable media provided that the device is handled in accordance with the instructions in section 4.3.3, Personal initiative and responsibility.
  In addition, the information may, under certain conditions, be stored in a cloud service. For an assessment of whether it is appropriate to store the information in a cloud service - see section 4.2, Use of cloud services, or contact the university's security and safety division for guidance.
- The information may be stored on a file server located in a server room with access control.
- The information may be stored in a storage solution that meet the requirements for the security level 2 for the confidentiality aspect.
- The information may be sent electronically e.g. via email or the web, without encryption.
- The information may be sent by fax and by post, both internally and externally.
- When replacing a hard disk, all information on the discarded disk must be overwritten in such a way that it cannot be recreated.

Regulations for class 3

- The information may be stored on the workstation's local hard disk or removable media provided that the device is handled in accordance with the instructions in section 4.3.3, Personal initiative and responsibility. In case the device leaves the office environment, the device's hard disk or the sensitive information must be encrypted.
- The information may be stored in a storage solution that meet the requirements for the security level 3 for the confidentiality aspect.
- The information may be stored on a file server located in a server room with access control.
- The information must be encrypted for electronic transmission, for example via e-mail or the web, before it is transmitted internally or externally.
- The information may be sent by fax and mail, both internally and externally.
- A replaced hard disk must not be reused and should be wiped in accordance with the procedures for Managing decommissioned (phased out) IT equipment (UFV 2014/1279).

4.4.2 Integrity

See guidelines in section 4.4.1, Confidentiality. The regulations for the confidentiality aspect also apply to the aspect of integrity, with the exception for the destruction requirement when replacing a hard drive.

4.4.3 Availability

The availability aspect of information handled outside of the university’s central and local systems is to a large extent about backup - to prevent information loss when the information is stored on a workstation's local hard drive or on a removable medium connected to it. In such cases, the owner of the equipment in question is responsible for ensuring that backups take place with suitable periodicity and in a secure manner in accordance with the guidelines for IT services (UFV 2016/896).

4.5 Secure handling of keys

Keys (pseudonymization keys/encryption keys) and code lists must be
• stored separately from the information to which it is linked,
• stored in as few copies as possible, however at least one back-up copy must be available,
• stored in a storage solution that meets the requirements for classification level 332 according to the university's methods for information classification and requirements analysis,
• be protected with a strong password (must consist of at least 10 characters - of which at least one uppercase, at least one lowercase, and either at least one special character or a number.),
• communicated in a secure manner, only to authorized persons.