Guidelines for information security

LINKÖPINGS UNIVERSITET
UNIVERSITY MANAGEMENT

Innehåll

Background

This document establishes guidelines for information security at Linköping University (LiU). The guidelines are part of LiU's information security management system, which also includes an information security policy (dnr LiU-2018-02237) that describes the board of directors' overarching priorities for information security at LiU, and a description of the processes within the management system (dnr LiU-2019-03289.

The guidelines have been defined by LiU's IT security group based on the needs and conditions within the organisation, legal requirements, external analyses, general risk analyses of LiU's information assets, and an analysis of past incidents. The guidelines are revised at least every two years.

The word "guideline" is to be interpreted strictly. Unless explicitly stated the guidelines are binding when handling LiU's information. Some guidelines in chapters 5 and 6 may be set aside after a suitable risk analysis, as described in the introduction to chapter 5. Other deviations require specific approval as outlined in each section.

This translation is advisory only. Although all care has been taken to ensure that the translation is accurate, if there are any conflicts between the Swedish version and this translation, the Swedish version take precedence.

Reading directions

Definitions

These guidelines use the words “must” and “should” with the following meaning:

must	Indicates something that is required to follow the guideline. Phrases such as “is not permitted” or “may not” also indicate something that is required to follow the guideline.
should	Constitutes a strong recommendation that complements the guideline. The guideline is to be followed unless there is good reason not to.

A list of technical definitions is attached to the end of this document.

All readers

Chapter 1 contains a description of LiU’s models for classifying information assets and IT equipment. Since many guidelines refer to the classifications, this chapter should be read.

Chapter 2 contains guidelines for information security that apply to **staff**, **consultants**, **and others who work for LiU**. The chapter is intended to be independent of subsequent chapters. The guidelines are binding.

Account administrators/heads of departments and equivalent

Chapter 3 contains guidelines that target **account administrators** and **heads of department and equivalent** at LiU. Individuals who are authorised to create, terminate, and assist with resetting user accounts in LiU’s IT environment are considered account administrators. The guidelines are binding.

System administrators and the IT security group

Chapter 4 contains guidelines that apply to individuals who work as **system administrators**. Anyone who has elevated privileges in an IT system and who has signed a separate agreement is considered to be a system administrator. The guidelines are binding on anyone who has the role of system administrator. The chapter also includes special authority for system administrators who are part of LIU’s **IT security group.**

Information owners

Chapter 5 contains guidelines for handling LiU's information assets. This chapter is aimed primarily at **information owners**. Information owners are designated by head of department or equivalent. It is the information owner's responsibility to ensure that these guidelines are followed. Examples of potential information owners are the object owner, principal investigator in a project, or supervisor of a thesis project. If the information owner does not handle critical information, it is sufficient to read and ensure compliance with **sections 5.1 through 5.6**

Chapter 6 contains guidelines for IT systems used to process information assets at LiU, including systems built or acquired by individuals. Information owners may assume that solutions provided by the IT division[1] adhere to these guidelines. Information owners who acquire or use other IT services must ensure that the guidelines are followed.

Asset owners

In addition to chapters 5 and 6information owners who are also **asset owners** in LiU's ”förvaltningsmodell för informationsbehandlande system vid Linköpings universitet (LiU-2012-00330) are affected by guideline 4.1.1 in **chapter 4**.

[1] For example clients with protection level gold or silver (see chapter 1), Office 365 including email, Lisam, and storage solutions from the IT division. See https://insidan.liu.se/informationsskerhet.

1 Classification of information and IT equipment

1.1 Information classification

Information at LiU is classified along three dimensions: **confidentiality**, **integrity** and **availability**. Finally, the category **classified information** is an entirely separate class.

The purpose of information classification is to simplify the selection of technical and administrative security measures for LiU's information and to support individuals in determining how different kinds of information may be handled (for example, how a certain IT service may be used).

In the dimensions integrity and availability there are two levels: normal and elevated. For confidentiality there are four levels: negligible, normal, elevated, and extreme.

It is important to use the classification system sensibly. Too low a classification will expose LiU to unacceptable risks. Conversely, too high a classification may lead to an unnecessary administrative load and higher costs.

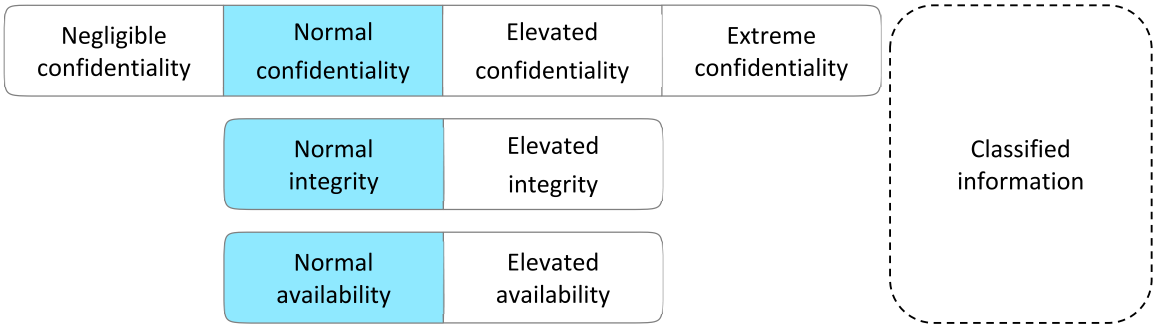


Figure 1. The information classification system at LiU.
Example of classification for an information asset with normal confidentiality, integrity and availability.

1.1.1 Classified information

Classified information (*säkerhetsskyddsklassificerad uppgift*) is information that concerns security sensitive activities as defined by the Protective Security Act (SFS 2018:658). Information that would be considered secret in accordance with SFS 1996:633 must be treated as classified information at LIU.

Classified information may under no circumstances be stored, processed or communicated using LiU's IT equipment, systems or networks, including all types of internal solutions and external cloud services. Neither hardware, software, networks, nor staff have security clearance for this.

Any classified information that is present must not be inventoried nor catalogued as described in section 5.1. Instead, the security protection officer or an official to whom the security protection officer has delegated the task must be informed. Such information is to be transferred orally at a physical meeting.

1.1.2 Extreme level (confidentiality)

Extreme level is used for large collections of information, where each item of information meets the criteria for **elevated** level (see below), for information that would cause significant risk to life or well-being if revealed, and for information that meets the criteria for **elevated** level and is judged to be the target of foreign intelligence activities or similar threats. **Extreme** level is also usually applied to information that is subject to absolute secrecy (*absolut sekretess*) according to the public access to information and secrecy act (2009:400).

Examples

- Medical information systems (collections of sensitive personal data).
- Home address to persons in exposed positions (risk to life and limb).
- Information about individual dissidents in totalitarian regimes (target of foreign intelligence activities).

1.1.3 Elevated level (confidentiality, integrity and availability)

The **elevated** level of the dimensions **confidentiality, integrity** and **availability** is to be used if **severe damage** may affect LiU, a collaboration partner or individual should the **confidentiality** be breached, the information **corrupted** (integrity) or the information **lost** (availability). **Elevated** level should only be used when there is risk of severe damage. Severe damage is to be considered from a LiU-wide, and not exclusively financial, perspective. Damage can be a significant financial loss or reduced reputation of LiU, or damage to an individual following exposure of personal data.

Additionally, elevated confidentiality applies to information that may be subject to strong secrecy (*stark sekretess, sekretess med omvänt skaderekvisit*) according to the Public Access to Information and Secrecy Act and to sensitive personal data (see 1.2.1). See further in "Vägledning om offentlighet och sekretess för stöd vid bedömning av sekretess och konfidentialitet" (only available in Swedish)[2].

When using elevated availability it must always be possible to express concrete availability requirements.

Examples

- Information about personal situation that is divulged during a counselling or therapy session (elevated confidentiality).
- Trade secrets (elevated confidentiality).
- Learning management system (elevated availability).

[2] Linked from https://insidan.liu.se/juridisk-radgivning/offentlighet-sekretess/

- Database of study results (elevated integrity).

1.1.4 Normal level (confidentiality, integrity and availability)

If the **elevated** or **extreme** levels are not used, **normal** level is usually appropriate as it still provides basic protection. Note that **normal confidentiality** does not refer to the absence of confidentiality: it signifies only that the basic protection is sufficient. Equivalent provisions apply to the other dimensions.

Examples

- A list of names and personal identity numbers for students.
- A list of employees' home addresses and telephone numbers.
- A document to which weak secrecy (*svag sekretess, sekretess med rakt skaderekvisit*) applies.

1.1.5 Negligible level (confidentiality)

Negligible confidentiality may be applied to information assets where the confidentiality requirements are particularly low or even non-existent, and where there are only **harmless personal data** (see 1.2.3). Such information assets do not require all protection mechanisms that apply to normal or higher levels. However, applicable legislation and regulation, such as data protection regulations, and document management must still be followed.

Examples

- A presentation about Linköping University.
- Published scientific papers.
- Manuscripts for scientific papers (if the author so desires).

1.2 Personal data

Personal data are any information relating to a identified or identifiable natural person. In order to classify confidentiality, it is vital to assess different kinds of personal data. The level of protection needed for personal data depends on how sensitive they are and what risk they pose to the person they concern.

1.2.1 Sensitive personal data

Sensitive personal data is defined by the General Data Protection Regulation[3] as information about:

- racial origin or ethnicity,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- health,

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council ("GDPR")

- a person’s sex life or sexual orientation, or
- genetic or biometric data for the purpose of uniquely identifying a person.

Additionally, data relating to criminal convictions and offences are considered to be sensitive personal data. Sensitive personal data are nearly always classified with at least elevated confidentiality, and large collections of non-pseudonymised sensitive personal data are typically classified with extreme confidentiality.

Information about children warrants special protection, and in many cases it may be appropriate to consider such information as sensitive personal data, and therefor classify them with elevated confidentiality.

1.2.2 Normal personal data

Personal data that is not sensitive is referred to as **normal personal data** in these guidelines. Although personal identity numbers are considered sensitive, they are considered normal personal data.

1.2.3 Harmless personal data

The term **harmless personal data**, which is used in some guidelines and decisions, refers to normal personal data that due to their nature and the context in which they are used have lower data protection requirements than other normal personal data. The assessment of personal data as harmless is also influenced on the general availability of the data.

For a datum to be considered harmless is must be, and be meant to be, readily and generally available. The individual it concerns must be aware that the information is available and may be disseminated. The information must be of a nature and used in such a way that the individual it concerns can be assumed not to object to its use or dissemination. Furthermore, the datum must be used in a context where it is not combined with other information, so that the combination cannot be considered harmless.

In most cases a name, professional contact information, authorship, professional affiliation, and area of research are generally and readily available, and are often used in situations and ways that satisfy the conditions to be considered harmless.

Note that the term harmless personal data is not defined in legislation. The General Data Protection Regulation remains applicable to these data. Through the use of the term harmless personal data more precise requirements can be made on the university’s handling of information and unnecessarily burdensome security measures can be eliminated where appropriate taking into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons[4].

[4] General Data Protection Regulattion, article 24.1.

Examples of harmless personal data

Names, contact information, affiliations in author and reference lists in scientific publication. The data is considered harmless in most cases. Authorship is easily available in the academic context, and authors rarely object to being associated with their work.

Examples that are *not* harmless personal data

Name and contact information to a person in the police or social services. The data are usually *not* considered harmless since there is good reason to assume that the individual or the agency would object to its dissemination.

Participant lists for conferences or courses. The data are usually *not* considered harmless since information concerning the whereabouts of each individual is added by being implied by the listing.

1.2.4 Pseudonymisation of personal data

Pseudonymisation of personal data occurs when a datum can no longer be associated with a specific person without the use of additional information. For example, data that can identify an individual is encoded in such a way that it is impossible to deduce the identity of the individual without access to an encoding key (pseudonymisation key). A pseudonymised data set is still considered personal data and if it contains critical information, such as information about health, then all regulation concerning sensitive personal information applies to the data set. However, when used correctly, pseudonymisation can be a very effective protection mechanism, which affects the level of confidentiality that can be used (see the flowchart in 1.3).

For pseudonymisation to be completely effective and warrant a reduction in confidentiality level, no indirect identifiers may be included in the pseudonymised data set.

When classifying the encoding key, its confidentiality must be classified using the criteria that would apply to the original data if pseudonymisation was not applied.

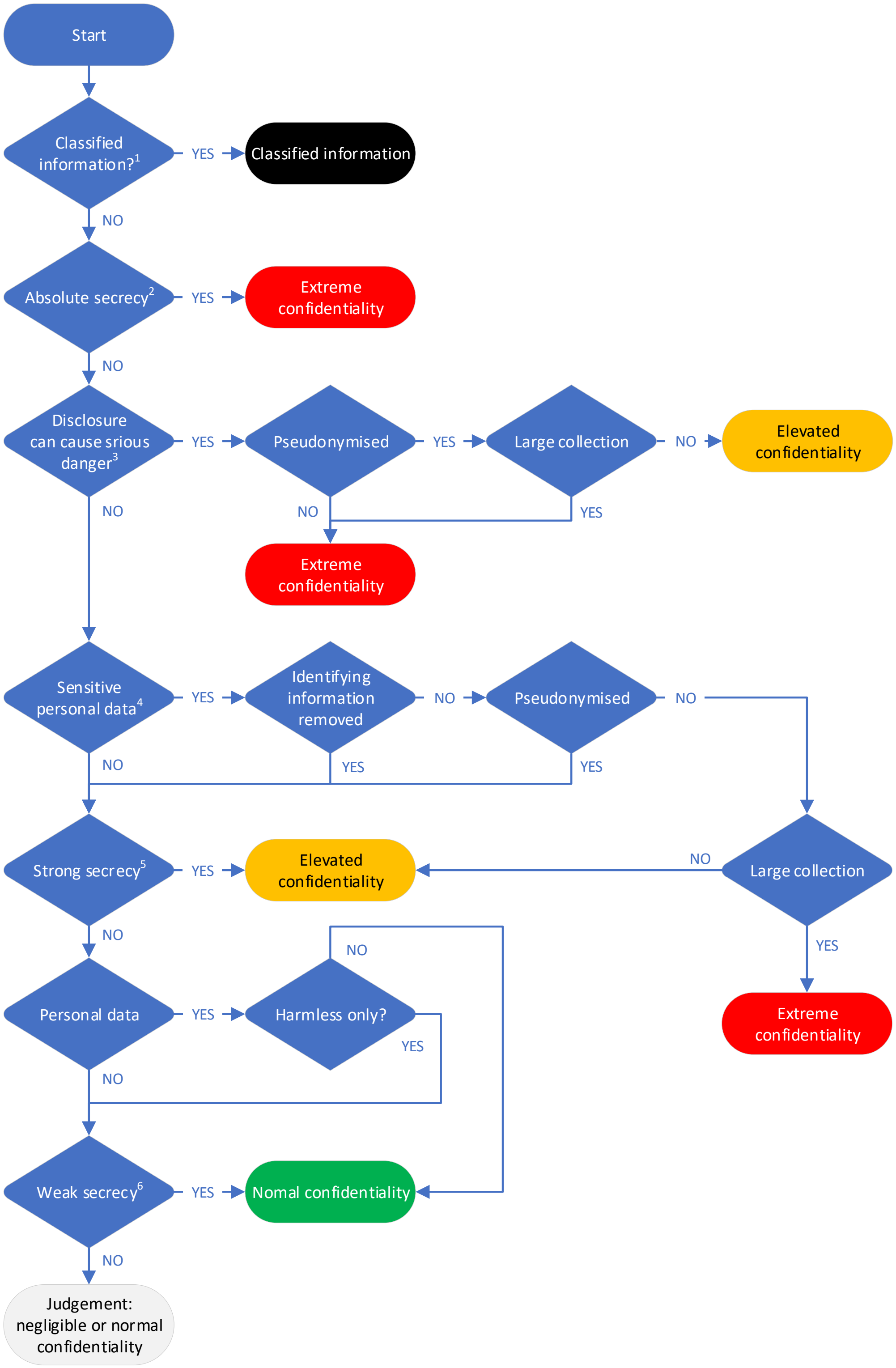
1.2.5 Anonymised personal data

If identifying information is completely eliminated from a set of personal data, so that none of the data can be directly or indirectly associated with an individual, then the data set can be considered anonymised, which implies that the data is no longer classified as personal data and the GDPR no longer applies.

Note that data can never be considered anonymised if there is any possibility for any individual organisation, in isolation or in collaboration, directly or indirectly, associate a datum in the set with an individual.

1.3 Flowchart for information classification

The flowchart below can be used to assist in classifying confidentiality. Note that information owners may, after analysis, select a higher or lower classification than indicated by the flowchart based on the consequences for LiU or an individual if the information is revealed.



[1] Classified information as defined in SFS 2018:658 or secret information as defined in SFS 1996:633.
[2] Secrecy according to SFS 2009:400 that applies unconditionally, without assessment of damages.
[3] Sensitive personal data that, if disclosed, can result in serious danger to life or health.
[4] Personal data that falls within one of the special categories of personal data defined in the data protection regulation.
[5] Secrecy according to SFS 2009:400 with reverse requirements of damage (defaults secret).
[6] Secrecy according to SFS 2009:400 with straight requirements of damage (defaults to public).

1.4 Critical information

The concept of **critical information** is refers to information classified with any one of the levels **elevated** or **extreme confidentiality**, **elevated integrity**, or **elevated availability**. Several guidelines apply to all these classifications and are simplified by the use of the term "critical information".

1.5 Classification of IT equipment into levels of protection

Depending on the classification of information, different levels of security measures are required to secure LiU's information processing. Furthermore, different people require different levels of flexibility in their IT environment. In order to simplify balancing security against flexibility and ease of use, IT equipment is classified into levels of protection.

The classification is based on the colours gold, silver, bronze, white and black. For normal IT clients (telephones, tablet computers, stationary computers and laptops), gold, silver, and bronze are used. Gold provides the strongest protection and involves the lowest risk (and a lower degree of flexibility), silver provides a high degree of protection while allowing higher flexibility, while bronze gives the lowest degree of protection and involves a higher risk (and a higher degree of flexibility).

Certain devices operate in special environments where normal security measures cannot be used. The colour white is used for these. The colour black is used for other IT equipment, such as privately owned computers.

Gold Equipment that is managed, maintained and inventoried by the IT Division. Has the highest level of protection.

Silver Similar to **gold**, but it is possible for the user to manage the equipment for a limited period of time.

Bronze It is possible for the user to deactivate further protective measures. The user may have administrator privileges for the equipment when logging in as a normal user.

White Equipment that is inventoried, but not managed or maintained, by the IT Division. Examples of such equipment are computers that are integrated into, or control scientific equipment or other machines. The managers of such equipment have a special responsibility for their security.

Black Equipment that is not inventoried by the IT Division, such as privately owned computers.

2 Guidelines for staff and contractors

This chapter lays down guidelines for staff, consultants and others who work at LiU. Students are not normally subject to these guidelines: they are subject to "Regler för studenters användning av IT-resurser vid Linköpings universitet" (LiU-2018-01846).

Everyone who works for LiU is required to be familiar with and follow these guidelines. Deviations from them are only permitted with prior written permission from the information security coordinator.

2.1 Use of IT resources and information

2.1.1 Users of LiU's IT resources must follow Swedish legislation. Furthermore, their use is to be conducted as specified by these guidelines and other regulations published at http://styrdokument.liu.se.

2.1.2 Slandering, insulting, humiliating or abusing other people when using LiU's IT equipment is not permitted.

2.1.3 Users of LiU's IT resources must follow instructions given by the IT director, the IT security group (IRT), or system administrators who are responsible for the particular resource.

2.1.4 Attempting to gain elevated privileges in LiU's IT systems without written permission from the object owner is not permitted. Using LiU's IT resources to attempt to obtain authorisation to which the user is not entitled in other systems is also prohibited.

2.1.5 LiU's IT resources are intended to be used for university business. Private use is permitted to the extent that does not interfere with work or expose LiU to unnecessary risks. LiU's IT resources may not be made available for private use by family members, acquaintances, or other people.

2.1.6 LiU's IT resources may not be used for commercial purposes.

2.1.7 When LiU's IT equipment is used, transported or stored outside of the work environment, the possessor must take appropriate measures to protect it. There are special guidelines for travel: "Riktlinjer för säkert resande" (LIU-2018-00399).

2.1.8 Employees and contractors must read and follow the instructions relating to the handling of information to which the person has been given access to in the course of their employment or contract. For private use of such information a request for access must be made to the registrar or to the person who is responsible for the records in question to ensure that an objective assessment of confidentiality is conducted, except if the information is of obviously general character, has already been made public, or the person has the right to dispose of it as a private person[5].

2.1.9 When new processing of personal data is introduced, the guidelines specified in chapter 5 and “Riktlinjer för behandling av personuppgifter” (LIU-2018-01540) must be followed.

2.2 Accounts and passwords

2.2.1 Access privileges to IT resources are personal and may not be made available to any other person except under direct supervision.

2.2.2 Revealing one’s password to any other person is not permitted. If it is necessary to allow another user access to a file, email message or any other IT resource, contact the helpdesk at the IT Division.

2.2.3 Requesting another person to reveal his or her password is not permitted.

2.2.4 Using the login details of any other person, regardless of whether that person has revealed them or not, is not permitted.

2.2.5 A unique password must be used for access to the LiU’s IT resources. This password may not be used for any external service.

2.2.6 When registering an email address or creating an account in an external service for work purposes, an address in the university’s email system must be used. See further in 2.5.2.

2.2.7 Passwords must be difficult to guess.[6]

2.2.8 A password must be changed immediately if it may have become known to anyone other than the user.

[5] This primarily refers to information such as patentable inventions that an employed educator at LiU disposes of in accordance with legislation (1949:345) concerning the right to employee’s inventions, or such works that an employee disposes of in accordance with LiU:s interpretation and application of 1 § act (1960:729) concerning rights to literary and artistic works, as is set out in “Allmänna råd om universitetets nyttjanderätt till upphovsrättsligt skyddat material (dnr LiU-2017-03903)”.

[6] It is a good idea to use a passphrase that consists of at least five randomly chosen words. Read more about passwords at https://insidan.liu.se/it/it-sakerhet/tips-for-ett-sakert-losenord.

2.2.9 Password managers may be used to store personal passwords. Recommendations concerning this are available from the IT Division.[7]

2.3 Basic IT and information security

2.3.1 Files should normally be stored on LiU's servers ("fillager" or OneDrive for business). Storage only on a local hard drive should be avoided. See below (2.3.2) for information about storing information classified with **extreme confidentiality** or **elevated integrity**.

2.3.2 Files that contain information classified with **extreme confidentiality** or **elevated integrity** should normally be stored on the IT Division service for secure storage, or other storage service specified by the information security coordinator. If the information owner has issued special instructions for storage, these should be followed instead.

2.3.3 Documents sent to a printer should be retrieved using a LiU card. When printing documents that contain **critical** information, the printout must either be retrieved immediately using a LiU card, or the printer kept under observation during the printing operation.

2.3.4 When disposing of printed documents that contain **critical** information, they must be destroyed using a shredder of security class 4 or higher.

2.3.5 When storage media that has contained **critical** information are no longer to be used, they should be submitted to the IT Division for destruction. Alternatively, the contents must be erased in such a manner that the information cannot be reconstructed.

2.3.6 A privacy filter[8] should be used when handling information classified with **elevated confidentiality** or higher in environments where there are people who do not have access to the information, such as train stations, on public transport, in lecture halls, or in meetings.

2.3.7 Users of computers are responsible for ensuring that the computer is locked when it is left unattended. Avoid leading computers of other devices unattended where the risk of theft is not negligible.

2.3.8 Users of mobile devices are responsible that the equipment is protected by screen lock (such as a six-digit PIN, password, or fingerprint).

2.3.9 Staff and others working at LiU should check the veracity in requests for actions that they suspect may come from an unauthorized source, such as in the case of phishing or other forms of attempted fraud.

[7] https://insidan.liu.se/informationssakerhet/rekommendation-om-losenordshanterare
[8] A privacy filter reduces the viewing angle of the screen, which makes it more difficult for people other than those directly in front of the screen to see its contents.

2.3.10 Non-trusted accessories may not be connected to LiUs computers.[9]

2.3.11 Users who discover security flaws in information systems or IT services that LiU uses or is responsible for must immediately report them to LiU's IT security group by email to infosec@liu.se.

2.4 Cloud services

2.4.1 The use of cloud services where an outside party is the principal and controls the purpose and means of processing is allowed provided compliance with applicable legislation.

2.4.2 When LiU is the principal, information classified with **negligible confidentiality**, **normal integrity** and **normal availability** may be processed in cloud services if the information owner approves (in accordance with section 5.3). The information owner is responsible to ensuring compliance with applicable legislation, particularly concerning data protection, public access, secrecy, and archiving. Approval to use a cloud service must be reported to the IT security group.

2.4.3 For information other than that indicated in section 2.4.1 and 2.4.2, the IT director determines which cloud services may be used at LiU. The current list of currently approved services is published at https://insidan.liu.se/it/godkanda-molntjanster. Processing of **critical information** in cloud services requires that the information owner has issued special instructions that allow such processing.

2.5 Email

2.5.1 Incoming email must be read regularly and always managed in compliance with legislation concerning public access and confidentiality. LiU's instructions concerning document management[10] must be followed.

2.5.2 All work-related email correspondence must use email system designated by the IT director, using an email address with the form firstname.lastname@liu.se or function@[domain.]liu.se. Private equipment may access the email system only through the LiU webmail system. See also 2.9.1.

2.5.3 Email may not be forwarded automatically to an external email provider. Sending email with a sender address that ends with "liu.se" from an external email provider is not permitted.

[9] For example devices that members of the public ask to connect, such as memory sticks or equipment to record screen contents.

[10] https://insidan.liu.se/dokumenthantering

2.5.4 **Critical information** that is processed by email must be encrypted and signed using S/MIME, PGP or another reliable method. Other processing of critical information by email is prohibited, with the exceptions described below. When the exceptions are used, the information is either to be registered and subsequently deleted from the email system or selectively erased within one week of the conclusion of the relevant case.

If an individual provides sensitive personal data about themselves through unencrypted without prompting from LiU, this data may be further processed using unencrypted e-mail only if such processing is necessary and there is no reasonable alternative. If possible, alternative communication channels must be used. Processing in unencrypted e-mail must cease as soon as the case is concluded or the person concerned so requests.

Information concerning an individual's trade union membership may be processed in an unencrypted form by email if the processing of personal data is necessary to ensure the rights of the data subject within employment law, unencrypted e-mail is the only reasonable means of communication, and both the sender and the recipient of the email message use email addresses that end with "liu.se".

2.6 Mass email

The term "mass email" is here used to denote email that passes through LiU's email system and is sent to a large number of recipients, several of whom do not know the sender. The guidelines also apply to other email distribution if an address that ends with "liu.se" is used as sender.

Mailing lists to which the recipients themselves have subscribed and can unsubscribe from are not subject to these guidelines. The same holds for department-specific lists; these may be subject to other regulations.

The IT division may prevent mass email that violates these guidelines or current best practice. The IT division may also prevent future mass email from sources that have previously violated these guidelines. Such a decision may be reviewed by the IT director. Technical limitations and spam filters may automatically prevent mass email for which support has not previously been given from the IT Division.

2.6.1 Mass email must be executed in such a way that the recipients are unable to see each other's addresses.

2.6.2 The following types of mass email distribution are prohibited:

- Advertising, including invitations to parties, employment opportunities, and other information from companies.
- Chain letters. A message that encourages the recipient to forward it is considered to be a chain letter.

2.6.3 Mass email is to be used with great restraint. This means that measures must be taken to ensure that the information is truly relevant for the recipients. Repeated mailings on the same subject should be avoided. In the event of uncertainty whether mass email is appropriate, the IT security group can provide guidance about current practice.

The mass email must have a clearly identified sender. The message must be readable using assistive technology. The messages should not have attachments. If the attachments are unavoidable, documents should be sent in PDF format.

2.6.4 Mass email with general study-related information or other information related to LiU activities, sent to its students and co-workers is normally permitted.

2.6.5 Surveys (questionnaires) are permitted only in the following cases:

- The survey is part of a university-wide commission or project.
- The survey concerns research projects carried out by researchers at LiU.

Recipients of surveys sent by mass email must be able to decline further mailings, including reminders, without having to answer any questions. Surveys should be conducted using the LiU survey application[11].

2.6.6 Course-related questions are permitted on course mailing lists. Course supervisors may also decide to approve mailings of course-related questionnaires to the course list. Note that course staff are not automatically subscribed to course lists.

2.6.7 Mass email from the student unions to their members is permitted.

2.6.8 The committees of sections and student unions may use programme lists for information about their operations, with the exception of mailings that violate 2.6.1.

2.6.9 Anyone who considers that an email message violates these guidelines can send a complaint to the IT security group by email to infosec@liu.se. In order for a complaint to be processed, the email message must be sent in its entirety, including complete message headers.

[11] https://insidan.liu.se/it/survey

2.7 Theft and loss of IT equipment

2.7.1 Theft or other loss of a computer, tablet computer, mobile phone or other IT equipment must be reported to the police by the staff member involved. Information about the loss and the case number assigned by the police must be sent to the IT division . The IT division will in turn notify the university's head of security[12] and when applicable report the loss as a personal data breach.

2.8 Disposal of IT equipment

2.8.1 Computers, telephones, tablet computers and other devices and storage media are not normally to be disposed of by the end user. If such disposal is carried out by the end user in spite of this, the guidelines given in chapter 5 of this document must be followed.

2.9 Use of private equipment

2.9.1 **Critical information** may not be processed using private equipment. This includes decryption keys for e-mail, such as private S/MIME or PGP keys.

2.9.2 Anyone who connects private equipment to the LiU network or uses a private computer to process LiU information is responsible for maintaining the equipment such that it does not constitute a security threat. The operating system and software must be kept updated, and the computer must have up-to-date protection against malware (antivirus protection).

2.9.3 Private equipment connected to the LiU network may be probed remotely (scanned) for vulnerabilities by the LiU IT security group. Equipment in which vulnerabilities are discovered constitute a risk to information security and access to the network may be denied to such equipment (blocked). Bypassing such blocking is not allowed.

2.10 Monitoring of IT resources and response to violations

2.10.1 System administrators may monitor systems and computer networks, and may access network traffic or stored data, in order to ensure reliable operation and an acceptable level of security for LiU's IT systems. Such access may also take place to investigate IT incidents or suspected breaches of LiU's regulations.

[12] In accordance with the guidelines concerning handling suspected misconduct and crimes (dnr LiU-2019-03689).

2.10.2 In the event of violations of these or other user-centred guidelines or instructions, access to IT resources may be limited. Such limitation may also be imposed in order to prevent an ongoing attack (such as unauthorised access or the introduction of malware).

2.10.3 Violation of these guidelines may be passed to the head of department or equivalent, or dealt with as specified in the LiU procedures for handling suspected misconduct and crime (LiU-2019-03869). Suspected criminal action may be reported to the police.

2.10.4 In the event of serious breach of these guidelines, or during an investigation into suspected improper use or criminal acts, IT equipment owned by LiU may be removed and examined by LiU's IT security group. This examination may include all data stored on the equipment or in LiU IT systems.

3 Guidelines for account administration

The account that staff, consultants, and others are given access to is the basis for access to IT resources at LiU and are a very important aspect of protecting LiU's information. Initial access to the account requires an activation key, that is issued by special **account administrators.** This chapter establishes guidelines for account administration and is aimed at account administrators and **department heads or equivalent**. The guidelines are binding and exceptions may be made only with written approval from the IT director.

3.1 Head of department or equivalent

3.1.1 The head of department (or whoever the head has delegated the task to) must ensure that accounts that are no longer needed due to the person's relationship with LiU ending are closed by the account administrator. The document *Tillgång till IT- och tekniska resurser* (LiU-2018-01792) specifies who is entitled to an account at LiU.

3.2 Account administrators

3.2.1 Account administrators are required to inform users about these guidelines, in particular chapter 2, when they issue an activation key. The account administrator indicates that this has been done by checking a box in the account activation tool.

3.2.2 When issuing an activation key, account administrators must ensure that identity verification takes place and indicate this in the account activation tool.

3.2.3 Computers used to issue activation keys must have protection level **gold** or **silver**. This guideline comes in to effect three months after computers with protection levels gold or silver become available.

3.2.4 Account administrators must transfer activation keys in person, through certified mail, or through other means that have the same level of protection directly to the recipient. Under no circumstances may any person other than the owner of an account set the account password.

4 Guidelines for system administrators

System administrators are those individuals who have a higher level of authorization than normal users in an IT system and who have signed a special form for system administrators at LiU (dnr LiU-2018-01854).

This chapter establishes guidelines for information security that apply to system administrators. If there are conflicts with guidelines in chapter 2, then this chapter takes precedence.

4.1 Object owners' designation of system administrators

4.1.1 Object owners determine who has the role of system administrator for the objects for which they are responsible. The object owner must ensure that designated system administrators confirm their knowledge of these guidelines by signing a special form.

4.2 General guidelines

4.2.1 Dedicated system administration accounts, or other accounts with elevated privileges, must not be used other than when required by the task at hand.

4.3 Special responsibilities

4.3.1 System administrators must keep confidential information of a personal nature, personal data, and confidential information (including information about protection mechanisms) that they learn through their role as a system administrator.

4.3.2 System administrators are required to notify the university's IT security group if they suspect security weaknesses or if there is an IT security incident. Suspicion of misconduct must also be reported in accordance with the university's guidelines for handling suspected misconduct and crimes (dnr LiU-2019-03689). Their responsibility to notify extends to the entire university's IT environment.

4.3.3 System administrators who become aware of a personal data breach must report it in accordance with current practice[13].

4.3.4 System administrators who become aware that IT resources are used in violation of current regulation and guidelines are required to notify those concerned. Repeated or serious violations, such as illegal activity, must be reported to the university's IT security group.

[13] https://insidan.liu.se/dataskyddsforordningen/personuppgiftsincident

4.3.5 System administrators are required to have a good understanding of these guidelines in their entirety.

4.4 Special privileges

4.4.1 System administrators have the right to monitor systems and network traffic as required for daily management of the system. The privacy of users must be protected to the extent possible. System administrators are therefore required to take appropriate measures to minimise the risk that they see individual users' data.

4.4.2 Access to students' stored data (for example home directory, OneDrive, or e-mail) may only take place as part of purely technical processing or with the consent of the affected individual. If a system administrator discovers a serious violation of LiU's rules or a violation of law, this is to be reported as indicated in 4.3.

4.4.3 System administrators have the right to clean e-mail accounts and storage spaces that are inactive or misused in systems they are responsible for. The affected users must be notified prior to cleaning, if possible. If this is not possible, the affected department or office is to be informed.

4.4.4 System administrators may restrict access to IT resources without prior warning in emergency situations.

4.5 Privileges for the IT security group

The IT security group is responsible for LiU's operational IT security work. The group's mission is to be defined on an annual basis as a tasking from the university director. Members of the IT security group are required to sign the form for system administrators.

4.5.1 The IT security group is permitted to evaluate and test the security of the university's IT environment.

4.5.2 The IT security group is permitted to monitor systems and networks, including the contents of network traffic and stored data, to ensure an adequate security level in LiU's IT systems and to investigate suspected information security incidents and violations of LiU's rules.

4.5.3 The IT security group is permitted to take action to ensure compliance with the university's rules and to prevent and manage information security incidents. Such actions may include limiting access to networks or other IT resources, and seizing and examining equipment owned by the university.

5 Guidelines for information owners

This chapter establishes general guidelines for handling information at LiU and is primarily aimed at information owners[14].

Information owners are designated by head of department or equivalent. It is the information owner's responsibility to ensure that these guidelines are followed. Examples of potential information owners are the object owner, principal investigator in a project, or supervisor of a thesis project.

Every information owner may, **after a risk analysis**, elect to add or remove suitable protection measures. The guidelines in chapters 5 and 6 constitute a set of basic protection measures. The decision to make an exception from the guidelines must be written, registered (*diarieförd*), and sent to the IT security group for information.

Some protection measures are based on legal requirements or affect the information security in multiple assets. Exceptions from these guidelines require the written approval of the chief information security officer (*informationssäkerhetssamordnaren*) to ensure compliance with relevant legislation as well as an acceptable level of security for LiU as a whole. Guidelines that require approval are in this document indicated by a star (☆) and a thick line in the right margin.

5.1 Inventory of information assets

5.1.1 Information assets[15] must be inventoried, classified, and documented in accordance with LiUs information security management system at least every three years. This guideline comes into effect when guidance for the inventory process has been established. ☆

5.1.2 Head of department or equivalent must keep the documentation of information assets updated when assets are introduced or removed. The head of department or equivalent may designate an information security contact whose responsibilities include this task. This guideline comes into effect when guidance for the inventory process has been established.

5.1.3 A preservation plan must be established for every information asset that contains public records and that is not intended for personal use, in accordance with LiU's strategy for preservation of documents (LiU-2018-01344).

[14] Guidance for inventorying information assets and designation of information owners will be published as part of LiU's information security management system. Some of these guidelines do not come into effect until such guidance is available.

[15] Information that has been collected or established for a specific purpose, as well as the resources used to handle the information, such as software, services, servers, IT systems, and storage areas (definition adapted from dnr LiU-2018-01344).

5.2 Acquisition, procurement, and disposal of IT systems

If the IT system handles personal data, see also 5.5, Specific requirements for handling of personal data.

5.2.1 When procuring or otherwise acquiring new IT systems, requirements related to information security must be stated to ensure compliance with technical aspects of these guidelines. The IT division maintains a catalogue with basic IT requirements that is to be used for procurement and other requirements specifications. By using this catalogue compliance with these guidelines can be ensured. The catalogue is available at https://insidan.liu.se/informationssakerhet.

5.2.2 Acquisition of domain names must be done through the IT division. LiU is to be registered as the owner of the domain name. Exceptions can be made if an external party is the principal.

5.2.3 Before IT systems are decommissioned the legal division (*document- och arkivenheten*) is to be contacted to establish a preservation plan (*bevarandeplan*) for the information asset, or to revise the current plan (see LiU's strategy for the presercation of documents, dnr LiU-2018-01344).

5.2.4 When media that has contained **critical information** is retired from use, the contents must be deleted in such a way that the information cannot be recovered. Alternatively such media can be deposited with the IT division for destruction.

5.2.5 Equipment may not be disposed of without erasing or destroying storage media. When computers, telephones, tablets, and other devices as well as storage media are disposed of, LiU's recycling policy (LiU-2015-02023) is to be considered.

5.3 Cloud services

5.3.1 The use of cloud services where an outside party is the principal and controls the purpose and means of processing is allowed provided compliance with applicable legislation.

5.3.2 When LiU is the principal, information may normally be processed in cloud services only after a positive decision by the IT directory. For information classified with **negligible confidentiality**, **normal integrity** and **normal availability** the information owner may determine which cloud services are permitted. Prior to such determination the information owner must ensure compliance with legislation and other regulation, particularly concerning data protection[16], public access and secrecy, and archiving. Such decision must be sent to the IT security group.

5.4 Access control

Examples of access control include verifying the identity of a user, authorisation in an IT system, or locked storage to which only authorised people have access.

5.4.1 Access to processing of an information asset must only be granted to those who need such access to perform their duties or tasks at LiU.

5.4.2 Access to a resource is to be revoked and an incident reported to LiU's IT security group if there are indications that user credentials, e.g. passwords, have been compromised. ☆

5.4.3 Access rights must be individual. Non-personal accounts must be avoided.

5.4.4 It must be possible to temporarily or permanently limit an individual's access to an information asset. For IT systems this can be achieved by applying 6.3.4.

5.4.5 Access to **critical information** must be audited regularly to discover and correct errors.

5.4.6 Access must be revoked when access is no longer needed.

5.5 Specific requirements for handling of personal data

Also take note of *riktlinjer för behandling av personuppgifter* (LiU-2018-01540).

5.5.1 Processing of personal data must be notified of any processing of personal data as stated in LiU's guidelines for processing of personal data. ☆

5.5.2 Pseudonymisation should be used, if possible, when processing sensitive personal data.

[16] See also LiUs guidelines for the processing of personal data (dnr LiU-2018-01540). In particular, note the documentation requirements in section 4.3 concerning the accountability principle (*ansvarsskyldighet*).

5.5.3 Processing of personal data may take place only if there exists a legal basis for such processing.

5.5.4 Data subjects are entitled to information about LiU's processing of their personal data, including the reason for such processing.

5.5.5 Only those data that are required to fulfil the purpose of the processing may be collected and stored. Only those who need access to the data may have such access. Personal data must be avoided entirely if it is possible, without undue effort, to achieve the purpose of the processing using anonymised data.

5.5.6 Personal data must be correct and kept up-to-date, and it must be possible to correct errors. This guideline does not apply to archived documents.

5.5.7 Personal data may be processed only for as long as it is necessary to achieve the purpose for which the data were collected, which implies that it must be possible to delete personal data. As soon as personal data are no longer required for their purpose, they must be archived, culled, or anonymised. Contact an archivist at the legal division for assistance, if needed.

5.5.8 Before initiating processing of sensitive personal data in large quantities, an impact assessment must be performed in consultation with LiU's data protection officer. Such an impact assessment is also to be performed if the processing of personal data may result in high risk to the privacy of the data subject.

5.5.9 Personal data breaches are to be reported immediately in accordance with current procedure[17]. The incident is also to be reported to LiU's IT security group.

5.5.10 Personal data may not be transferred outside the EU/EES unless the receiving nation has adequate protections in place or there is at least one appropriate protection mechanism in place, as per the GDPR, such as use of the EU commission's standard clauses or if the recipient participates in an approved framework regulating the exchange of personal data.

5.5.11 When personal data is processed on the legal basis of consent, the object owner must ensure that it is possible to delete personal data if the data subject revokes their consent.

[17] See https://insidan.liu.se/dataskyddsforordningen/personuppgiftsincident

5.5.12 When personal data are processed by a third party on behalf of LiU and in accordance with instructions from LiU, or when LiU processes personal data on behalf of some other party and in accordance with their instructions, a personal data processing agreement must be established. Consult the department contact for data protection issues if advice concerning data processing agreements is required.

5.6 Incident reporting and continuity planning

5.6.1 Information owners must ensure that breaches of confidentiality, integrity, and availability are immediately reported to LiU's IT security group. Personal data breaches must also be reported in accordance with current procedure.[18] ☆

5.6.2 Information owners must ensure that there is a plan for physical maintenance, appropriate for the desired level of availability, for any IT systems or other physical assets that process information classified with **elevated availability**.

5.7 Information security plan

5.7.1 Information owners should establish an information security plan for any **critical information**[19]. The plan should consider long-term availability of competence (5.8.2) and physical maintenance to ensure that availability requirements can be met by IT systems and other physical assets (5.6.2). The plan is also an appropriate location for asset-specific guidelines (such as those indicated in 5.9.11 and 5.9.12).

5.8 Information owners' responsibility for staff

5.8.1 Information owners must establish asset-specific guidelines for handling **critical information** assets. For other assets such guidelines should be established. ☆

5.8.2 Information owners must ensure that everyone who works with **critical information** assets have appropriate competence with systems where the asset is processed.

5.8.3 Before contractors, partners are given access to information at LiU, it must be ensured that they read and follow appropriate guidelines for handling the information they are given access to as part of their engagement or other collaboration.

[18] See https://insidan.liu.se/dataskyddsforordningen/personuppgiftsincident
[19] A general template is available at https://insidan.liu.se/informationssakerhet

5.9 Physical security

5.9.1 Access to facilities where a **critical information** assets or systems that process such assets are located must be limited to those individuals who need access to perform their work.

5.9.2 Access to facilities where **critical information** assets or systems that process such assets are located must be logged, for example through the use of an electronic locking system.

5.9.3 Individuals who lack access to a facility where **critical information** assets or systems that process such assets are located, and temporarily need such access, for example to service equipment, must be escorted by a person who has access to the facility.

5.9.4 Appropriate protection must be used when transporting **critical information** assets.[20]

5.9.5 Facilities where **critical information** assets or systems that process such assets are located must be protected by an alarm system that satisfies alarm class 2 according to SSF 130.[21]

5.9.6 Facilities where information assets are located must have appropriate environment with respect to e.g. temperature, humidity, flood protection, fire protection, and power. Facilities where information classified with **elevated integrity** or **elevated availability** must have monitoring to enable rapid detection of environmental problems.

5.9.7 Facilities where **critical information** or systems that process such information are located must fulfil the requirements for SSF 200, protection class 2 with respect to physical intrusion.[22]

5.9.8 Safes may be used to handle exceptions from 5.9.5 when the alarm system is lacking, the requirements on fire protection in 5.9.6, and the requirements for intrusion prevention in 5.9.7. The safe classification must be chosen based on the value of the asset being protected.

5.9.9 Physical c**ritical information** assets must be inventoried on a regular basis. Inventory entails one or more individuals verifying that the asset exists, is in the condition required, and is stored in an appropriate manner.

[20] Examples of appropriate protection may include certified mail or a trusted courier in combination with a temper-evident enclosure.
[21] An overview of SSF 130 is available in *Vägledning för fysisk informationssäkerhet i it-utrymment* (MSB629). Locked and alarmed areas at LiU normally meet the requirements for alarm class 2.
[22] An overview of SSF 200 is available in *Vägledning för fysisk informationssäkerhet i it-utrymment* (MSB629). Most facilities at LiU fail to meet the requirements for protection class 2.

5.9.10 Backups of physical assets classified with **elevated integrity** or **elevated availability** must be made, to the extent possible. Backups must be stored in such a way that an event that affects the integrity or availability of the original does not affect the copies (and vice versa).

5.9.11 When storing a **critical information** asset outside the work environment, appropriate protection must be present. These guidelines should be included in an information security plan (see 5.7.1).

5.9.12 Information owners should establish guidelines for how and where information classified with **elevated confidentiality** or higher may be communicated. These guidelines should be included in an information security plan (see 5.7.1).

6 Guidelines for IT systems

This chapter establishes guidelines for technical requirements on management, development, and maintenance of IT systems, and applies to both existing systema and when acquiring new systems.

Exceptions from the guidelines may be made only after a risk analysis as stated in the introduction to chapter 5.

6.1 End user equipment

6.1.1 Computers and mobile devices must be locked automatically after a period of no more than fifteen minutes for computers and no more than five minutes for mobile telephones and tablets, when not in use. This guideline does not apply during a presentation or lecture. Permanent exceptions for e.g. lab equipment can be granted by the IT director. ☆

6.1.2 Privately owned equipment, equipment that belongs to visitors, and other devices at protection level **black** that are connected to LiU's network must be connected to a network that is logically separated from LiU's other networks.

6.1.3 Systems that process **critical information** must require client devices to have at least protection level **gold** or **silver** and be connected to a network designated for such devices, or connected to VPN. This guideline comes into effect three months after client devices with protection levels gold or silver become available.

6.2 Basic security

6.2.1 Software and operating systems on servers, personal computers, and mobile devices that handle information belonging to LiU must be kept up to date with corrections to security issues and reliability that are made available by the manufacturer or vendor. Updates must be installed as quickly as possible, and there must exist a process for immediate installation of critical updates. ☆

6.2.2 IT systems connected to LiU's network must be configured in such a way that automated vulnerability scanning via the network can be performed from IP addresses specified by the IT security group.

6.2.3 Security vulnerabilities in IT systems must be addressed as quickly as possible when they become known.

6.2.4 Facilities where information assets are located must have appropriate environment with respect to e.g. temperature, humidity, flood protection, fire protection, and power. Facilities where information classified with **elevated integrity** or **elevated availability** must have monitoring to enable rapid detection of environmental problems.

6.2.5 Information in IT-system and, when necessary, software for IT systems must be backed up so they can be recreated if lost. When information is classified with elevated integrity, the same individual should not be able to alter both the original and the copies.

6.2.6 IT systems must only be used for their intended purpose. For example, a server or workstation intended for software development may not be used for word processing, reading e-mail or general web surfing. The number of installed programs is to be kept to a minimum.

6.2.7 Secure solutions, such as management servers or privileged access workstations, must be used for remote administration of IT systems. The IT division is to provide appropriate solutions.

6.2.8 Given a timestamp, IP address, and port, it must be possible to determine which user was logged in on the indicated device. For wire networks it must also be possible to determine which network socket was in use.

6.3 User management and authentication

6.3.1 Authentication to IT systems must use LiU:s ADFS with multi-factor authentication. Multi-factor authentication is not required for students or when connecting from a device with protection level **gold** or **silver** that is connected to a network designated for such devices. This guideline comes into effect when multi-factor authentication becomes available to staff. ☆

6.3.2 Authentication to web-based systems must not use direct connections to AD or LDAP. Systems introduced prior to 2018-06-30 that already use direct AD or LDAP connections for authentication may continue to do so during a transition period. Such systems are to be decommissioned or transitioned to use ADFS no later than 2021-06-30.

6.3.3 When passwords are used for authentication, these are to have sufficient complexity. The IT division establishes requirements for sufficient complexity.[23]

6.3.4 Passwords must be transferred using reliable encryption.

6.3.5 Access to systems is individual.

[23] https://insidan.liu.se/it/it-sakerhet/krav-pa-losenordskomplexitet

6.3.6 When using a local user database, identities may not contain LiU IDs. Passwords must be managed in accordance with the guidelines for accounts and passwords (see 2.2). Passwords are classified with **elevated confidentiality** and **elevated integrity.**

Passwords in a local user database must be encoded in a irreversible manner. Should that not be technically possible, then the system must prevent re-use of passwords from normal user accounts.

Users must be able to change their own passwords. Enforcement of periodic password changes should be avoided.[24]

6.3.7 Authorisation of users must be based on groups in LiU's AD. It must be possible to control privileges using group membership.

6.3.8 E-mail clients that are unable to use multi-factor authentication must use application-specific passwords. This guideline comes into effect when multi-factor authentication becomes available to staff.

6.4 Logging and transaction history

6.4.1 Events in systems that process critical information must be logged. The log itself is classified with elevated integrity. As a minimum, the following events must be logged:

- Reding information classified with **elevated** or **extreme confidentiality**.
- Erasure of information classified with **elevated availability** or **elevated integrity**.
- Changes to information classified with **elevated integrity**.
- Successful and attempted authentication.
- Termination of authenticated sessions.
- Changes to users and permissions.

6.4.2 Log events must contain at least information about the type of event, when the event occurred, the subject (user or system) that initiated the event, and data that were affected by the event. The timestamp must be correct25 and the time zone must be specified or known.

6.4.3 Logs should be retained for between six and eighteen months unless otherwise indicated in a document management plan (dokumenthanteringsplan).

[24] Periodic password changes to not contribute to increased IT security since many sers will choose simpler passwords and to a larger extent handle their passwords in an insecure manner.
[25] By using e.g. NTP for time synchronisation.

6.5 Encryption and digital signatures

6.5.1 Electronic transmission of **critical information** must use reliable encryption and digital signatures. For e-mail, see 2.5. ☆

6.5.2 Information classified with **elevated** or **extreme confidentiality** must be stored in encrypted form. Keys for access to such data have the same classification as the information itself.

6.6 Web-based systems

These guidelines apply to web-based systems that are provided by LiU and that handle LiU's information.

6.6.1 Web-based systems must function with the most and next most recent versions of the browsers that are supported. Users are expected to upgrade web browsers as soon as upgrades become available. ☆

6.6.2 Systems may not require the use of web browser plugins. They must function with web browsers as per 6.6.1 in their standard installation. This means that plugins like Java, Flash, Silverlight, or ActiveX may not be required.

6.6.3 Web-based systems must function without any special settings or security policies on the client. This means that the system must function with a browser on a newly installed computer or device without any further adjustments.

6.6.4 Web-based systems that are used by large numbers of users must be accessible using a domain of the form *service*.liu.se.[26] Systems that are managed in collaboration with an external party may use a different domain address after approval from the IT director. Redirects after the initial access are permitted.

6.6.5 Certificates for web services must be issued by a trusted certificate authority. Certificates for a web service that uses a domain owned by LiU (e.g. all addresses ending with .liu.se) must be issued through LiU CA (Sunet TCS)[27].

6.6.6 Web-based systems that are used by large numbers of users must work with the following web browsers and platforms:

[26] Using internal domain names improves the likelihood that people will recognise phishing attempts, since they almost exclusively use external domains.
[27] These certificates can be requested free of charge from the IT division.

- Edge (Windows)
- Chrome (Windows, MacOS, Linux, Android)
- Firefox (Windows, MacOS, Linux)
- Safari (MacOS, iOS)

6.6.7 Web-based systems must be accessible using HTTPS. Systems should not be available using HTTP but should redirect HTTP access to HTTPS. Furthermore, HTTP Strict Transport Security should be used..

6.6.8 HTTPS for web-based systems must be configured according to the IT security group’s recommendations.[28]

6.7 Server security in networked services

The following guidelines apply both to web-based systems and to other systems that communicate over the network.
It must not be possible to use the service with protocols that have significant vulnerabilities. Examples of such protocols include NTLM. SSL (versions 1-3), and TLS version 1.0-1.1. ☆

6.7.1 Certificates for TLS must be kept valid as long as the service is in use. Certificates must be renewed before they expire. Certicate expiration should be monitored.

6.7.2 IT systems that handle critical information must be protected by a network firewall with an appropriate configuration.

6.7.3 Servers and other equipment connected to the LiU network may be probed remotely (scanned) for vulnerabilities from addresses designated by the IT security group. This does not apply to devices that do not belong to LiU. However, such devices will be subject to vulnerability scans while connected to LiU’s network.

6.8 IT systems with client software

These guidelines apply when acquiring or developing IT systems that contain a client software component.

6.8.1 Client software must not prevent updating the operating system or other software (web browsers, Java, plug-ins, and so on). ☆

6.8.2 Client software may not require exceptions in the operating system security settings. For example, it may not require obsolete software, configuring trusted sites, or exceptions in security software.

[28] https://insidan.liu.se/informationssakerhet

6.8.3 Client software may not require that the user has administrative rights to the computer where the software is run.

6.9 System development

These guidelines apply to anyone who develops software at LiU.

6.9.1 When developing systems, including software development, security aspects must be considered in a systematic manner.

6.9.2 When procuring or developing IT systems the ability to satisfy right of access by the data subject as per the GDPR and other legislation must be ensured.

6.9.3 When procuring or developing IT systems, the ability to correct personal data must be ensured.

6.10 System management

6.10.1 Changes to systems that handle critical information must be made in sa manner that reduces the risk that confidentiality, integrity, or availability are affected negatively. Processes such as checklists, reviews, or requiring two people to act in concert may be used.

6.10.2 The ability to restore backups of information classified with elevated availability or elevated integrity must be tested at least annually. Such tests must verify that restoration is possible and can be completed within the expected time with respect to availability requirements.

6.10.3 Changes to IT systems that process critical information must be tested in a test environment before being deployed to production.

6.11 Backups

6.11.1 Information classified with elevated confidentiality or higher must be encrypted. The encryption keys have the same classification as the information being encrypted.

Terminology

AD

Active Directory. Directory service from Microsoft that contains user accounts.

ADFS

Active Directory Federation Services. Enables single sign on (authenticating once) to multiple IT services.

Trusted certificate authority

Issuer of certificates that the IT security group has designated as trusted, which typically includes the issuers that are trusted by operating system and web browser vendors.

Irreversible

A process that can only be performed in one direction. In the context of security is predominantly used to denote the process of computing a cryptographic hash that, given a segment of text, computes a new text that appears to be completely random. The process can be repeated but it is impossible to recreate the original text from the generated one.

Indirect identification

Determining which individual a set of data refers to by using multiple pieces of information that in isolation cannot identify the person, but taken together can (for example, address and age taken in combination).

Information asset

Information that has been collected or established for a specific purpose, as well as the resources used to handle the information, such as software, services, servers, IT systems, and storage areas (definition adapted from dnr LiU-2018-01344).

Information owner

An individual who has the mandate to control an information asset. The information owner has rights and responsibilities with respect to these guidelines and is appointed by the head of department or equivalent.

Confidentiality

Protection against unauthorised access. ISO 27000:2017 states: “to protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorised entities”.

LDAP Lightweight Directory Access Protocol. A protocol commonly used by directory services such as Active directory. LDAP is also used here to denote an (older) directory server used at LiU.

LiU CA LiU Certificate Authority. A group at LiU responsible for managing the TLS certificate service procured by Sunet TCS.

Logical separation The placement of devices on separate network segments, for example by using virtual local area networks (VLAN).

Cloud service Any IT service provided over the internet by an external provider.

Object owner The individual responsible to an information processing system. See the management model described in dnr LiU-2012-00330. See also information owner.

Personal data breach An incident that least to the unintended or illegal destruction, loss, or change of personal data, or to disclosure of personal data to an unauthorised entity.

PGP One method for encryption and digital signing of e-mail. See also S/MIME.

Integrity The property that information is not changed without authorisation.

S/MIME Another method for encryption and digital signing of e-mail. See also PGP.

Secrecy A legal obligation not to disclose certain information. (SFS 2009:400)

SSL Secure Sockets Layer. An older protocol for encrypting and signing data traffic. Replaced by TLS.

Sunet The Swedish national research and education network (NREN).

Sunet TCS Sunet Trusted Certificate Service. Provider of TLS certificates to LiU CA.

System administrator An individual with higher authorization in an IT system than is normally assigned. For example, a person with administrative access to the operating system or an application.

Critical information

Information classified with **elevated confidentiality**, **extreme confidentiality**, **elevated integrity**, or **elevated availability**.

Reliable encryption and digital signatures

A published methods for encryption or digital signatures that is used in the intended manner and has have no relevant known weaknesses.[29]

Availability

Access to an authorised entity at the appropriate time. ISO 27000:2017 states that “something is available if it is accessible and usable when an authorised entity demands access”.

TLS

Transport Layer Security. A protocol for encrypting and digitally signing data traffic. Replaces the older SSL protocol.

Multi-factor authentication

Authentication (proof of identity) using at least two different methods, such as password in combination with a one-time code or a PIN code in combination with a smart card. When two factors are used, it is sometimes called **two-factor** or **two-step** authentication.

VLAN

Virtual LAN. Virtual network that separates equipment connected to the same physical network.

VPN

Virtual private network. A mechanism mainly used to establish a protected connection over an unprotected network.

[29] For technical details, see https://insidan.liu.se/informationssakerhet

Legislation and other regulation
This section is only available in Swedish. It outlines related legislation and other regulation, most of which is also only available in Swedish.