Directives for information security at Linköping University

Contents

Introduction

This is an advisory English translation of key portions of the document ”Riktlinjer för informationssäkerhet vid Linköpings universitet” (Dns LiU-2018-01814), which sets out directives for information security at LiU. The word “directive” should be interpreted in the strictest sense. Unless otherwise stated the directives are mandatory. This translation only includes chapters 1 and 2 since these apply to everyone who works are LiU.

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

must	Indicates something that is required to follow the directive.
should	Constitutes a strong recommendation that complements the directive.

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 directives refer to the classifications, this chapter should be read.

Chapter 2 contains directives 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 directives are binding.

Account administrators/heads of departments and equivalent

Chapter 3 contains directives 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 directives are binding. **This chapter has not been translated.**

System administrators and the IT security group

Chapter 4 contains directives 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 directives 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. This chapter has not been translated.**

Information owners

Chapter 5 contains directives for handling LiU’s information assets. This chapter is targeted primarily at **information owners**, who are responsible for ensuring that the directives are followed. An individual with authority to control or decide to destroy a particular information asset is considered to be an information owner. **This chapter has not been translated.**

Chapter 6 contains directives for IT systems used to process information assets at LiU. Information owners may assume that solutions provided by the IT division adhere to these directives. Information owners who acquire ot use other IT services must ensure that the directives are followed. **This chapter has not been translated.**

Asset owners

In addition to chapters 5 and 6 information owners who are also **asset owners** in LiU:s ”förvaltningsmodell för informationsbehandlande system vid Linköpings universitetW (LiU-2012-00330) are affected by directive 4.1.1 in **chapter 4** (not included in this translation)**.**

1 Classification of information and IT equipment

1.1 Information classification

Information at LiU is classified along four dimensions. In addition to the three perspectives **confidentiality**, **integrity** and **availability**, **personal data** is also used as a dimension. Finally, the category **secret information** is en entirely separate class. Personal data has been given special status since society's confidence in LiU as a government agency is affected by how LiU handles personal data. Furthermore, sensitive personal data is frequently found in many of LiU's activities.

The purpose of information classification is to simplify the selection of technical and administrative security measures for LiU's information. In order to create an efficient and easy-to-use management system, only two levels have been defined in the dimensions confidentiality, integrity and availability: **normal** and **elevated**. The levels used in the personal data dimension are: **no personal data**, **normal personal data** and **sensitive personal data**.

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 technology costs.

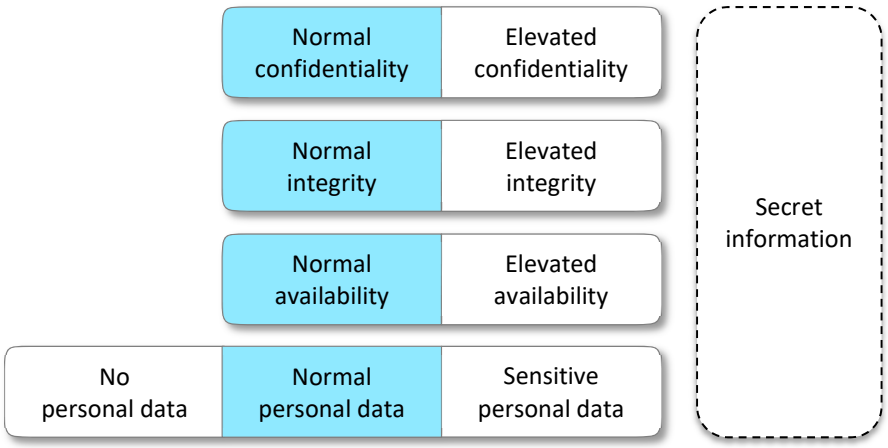

Figure 1. The information classification system at LiU.
Example of classification for an information asset with normal confidentiality, integrity and availability, for normal personal data.

1.1.1 Secret information

Secret information (hemlig uppgift) and secret documents (hemlig handling) as defined by the Security Protection Ordinance (SFS 1996:633) 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-based services. Neither hardware, software, networks, nor staff have security clearance for this.

Any secret information that is present must not be inventoried nor catalogued as described in chapter 5. Instead, the security protection officer or an official with security clearance 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 Elevated level (confidentiality, integrity and availability)

The **elevated** level of the dimensions **confidentiality, integrity** and **availability** is to be used only 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). Severe damage is to be considered from a LiU-wide perspective. A loss amounting to less than SEK 500,000 is probably not severe damage whereas loss of confidence in LiU as an organisation as a consequence of a personal data breach might be severe for LiU. Additionally, **elevated confidentiality** applies to information that is likely subject to confidentiality according to the Public Access to Information and Secrecy Act (2009:400).

1.1.3 Normal level (confidentiality, integrity and availability)

If the **elevated** level is not used, the **normal** level 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.

1.1.4 Personal data and sensitive personal data

It is generally easier to classify personal data than it is to classify the other dimensions. Either no personal data is present (**no personal data**), only personal data that is not sensitive is present (**normal personal data**) or **sensitive personal data** is present.

Personal data are any information relating to a identified or identifiable natural person. **Sensitive personal data** is defined by the Data Protection Regulation as information about:

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

1.2 Critical information

The concept of **critical information** is refers to information classified with any one of the levels **elevated confidentiality**, **elevated integrity, elevated availability**, or **sensitive personal data**. Several directives apply to all of these classifications and are simplified by the use of the term “critical information”.

1.3 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 Directives for staff and contractors

This chapter lays down directives for staff, consultants and others who work at LiU. Students are not normally subject to these directives: 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 directives. 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 directives 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 obtain higher authorisation 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 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 Staff and others working for the university must read and follow the instructions relating to the handling of information to which the person has been given access in the course of their work. Such information shall normally be used solely for university business. For private use of information that is not clearly of general character, has previously been published, or is covered by the intellectual property rights of academic staff, a request for access to the documents is to be submitted through the registrar or the person who is responsible for the document in order to ensure an objective assessment of confidentiality.

2.1.9 When new processing of personal data is introduced, the directives 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 passed on to any other person. 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.

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

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

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

2.2.5 Passwords must be difficult to guess.[2]

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

2.2.7 Password managers may be used to store personal passwords. Recommendations concerning this are available from the IT Division.[3]

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 **critical** information.

[2] It is a good idea to use a passphrase that consists of at least five randomly chosen words.
[3] https://insidan.liu.se/informationssakerhet/rekommendation-om-losenordshanterare

2.3.2 Files that contain **critical** information 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 Users of computers are responsible for ensuring that the computer is locked when it is left unattended.

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

2.3.8 Users of computers and other devices must use LiU's VPN service when using open wireless networks for LiU work.

2.3.9 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 abuse@liu.se.

2.4 Cloud-based services

2.4.1 The IT director determines which cloud-based services may be used at LiU.[4] The list of currently approved services is published at https://insidan.liu.se/it/godkanda-molntjanster. Other cloud-based services may only be used after a positive determination by the IT director. Information that has been classified as **elevated confidentiality** or **sensitive personal data** may not be processed in cloud-based services unless the owner has issued special instructions that allow such processing.

2.4.2 Cloud-based services other than those approved by the IT director may not be used for the processing of LiU's information.

[4] Stärkt informationssäkerhet på LiU (LiU-2014-00052), Section 5.

Note that the prohibition applies to popular services, such as Google's cloud-based services (G Suite including Google Mail and Drive), Apple iCloud (including file storage and backup), Dropbox, Mailchimp, Evernote, Doodle and Adobe Document Cloud. Exemptions may, however, apply, if the client is an external partner and ensures compliance with legislation.

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[5] 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 2.9.3.

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.

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.

Sensitive personal data that an individual provides about themselves through unencrypted email without a previous request from LiU may continue to be processed using unencrypted email until the relevant case has been concluded or the individual involved requests that the processing is to cease.

Information concerning trade union membership may be processed in an unencrypted form by email if the processing of personal data takes place to ensure the rights of the data subject within employment law 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 directives also apply to other email distribution if an address that ends with "liu.se" is used as sender.

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

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

The IT security group may prevent mass email that violates these directives or current best practice. The IT security group may also prevent future mass email from sources that have previously violated these directives. 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 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.

2.6.2 Mass email is to be used with great discrimination. 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.

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

2.6.4 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[6].

2.6.5 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.

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

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

2.6.7 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.

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

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 security group by email to abuse@liu.se.

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 directives given in chapter 5 of this document must be followed.

2.9 Use of private equipment

2.9.1 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).

2.9.2 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.

2.9.3 **Critical information** may not be processed using private equipment. This includes the decryption key for email that has been encrypted by, for example, S/MIME or PGP.

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.

2.10.2 In the event of violations of these or other user-centred directives 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 directives may be passed to the head of department or equivalent, or dealt with as specified in the LiU procedures for handling improper use (LiU-2016-00759). Suspected criminal action may be reported to the police.

2.10.4 In the event of serious breach of these directives, 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 Directives for account administration

This chapter is only available in Swedish.

4 Directives for system administrators

This chapter is only available in Swedish.

5 Directives for information owners

This chapter is only available in Swedish.

6 Directives for IT systems

This chapter is only available in Swedish.

Terminology

This chapter is only available in Swedish.