



LUNDS
UNIVERSITET

Vice-Chancellor

DECISION

1

22 June 2017

Reg. no STYR 2017/947

Guidelines on information security at Lund University

Background

The University generates and handles large amounts of information. This information must be managed in a way that ensures that the University's need for access is satisfied and that the University is able to comply with applicable regulations from, for example, the Swedish Civil Contingencies Agency, the Swedish Data Protection Authority, and the National Archives of Sweden. In order to fulfil our obligation, these guidelines concerning information security, including information and templates, have been updated.

In accordance with Section 11 of the Swedish Employment Act (MBL), the matter was negotiated with the staff organisations at the University on 20 June 2017.

Decision

The University has decided to adopt the enclosed *Guidelines on information security at Lund University*, including the following appendices, as of 22 June 2017:

- Appendix 1: *Instructions on information security: Users – Staff* (Information security A – staff)
- Appendix 2: *Instructions on information security: Users – Students* (Information security A – students)
- Appendix 3: *Instructions on information security: Administration* (Information security F), including sub-appendix Information security F – Appendix 1 – *Instructions on information classification*
- Appendix 4: *Instructions on information security: Continuity and operations* (Information security KD)

These guidelines replace the previous *Guidelines on information security*, adopted on 15 February 2012 (reg. no BY 2012/37).

The decision on this matter was made by the undersigned vice-chancellor, in the presence of university director Susanne Kristensson after a consultation with a representative of the Lund University Students' Unions, as well as a presentation by senior strategist John Westerlund. SamIT also participated in the processing of the matter.

Torbjörn von Schantz

John Westerlund
(Strategic Development)

Copies sent to:

All faculties

All divisions

USV/LUKOM/MAX IV

LUS

SamIT



Vice-Chancellor

Guidelines on information security at Lund University

The present information security guidelines¹ are intended for Lund University staff and students, as well as any collaboration partners involved in the University's activities.

At the University, there are large amounts of information, in and about research and teaching as well as in the administrative systems. It is important that the information is handled in a safe and efficient manner. The purpose of these guidelines is to describe the University's work to protect all information assets owned or managed at the University against all threats, both internal and external, intentional or unintentional.

General information about information security

The four main components of the University's information security objectives are that:

1. all employees must have access to the information they need to perform their duties and commitments (*accessibility*),
2. the information shall be correct at all times and the information resources shall ensure that the information cannot be corrupted through unauthorised or improper handling (*accuracy*)
3. the information and information resources must always be protected against unauthorised access (*confidentiality*), and
4. it shall be possible after an incident to demonstrate what happened, when it happened and who did what (*traceability*).

Information does not only refer to all forms of data, images, etc., stored in databases, computers, data media, online, in emails, written on paper or that is otherwise accessible (regardless of form or environment), but also the spoken word via e.g. telephone, in public places or other social contexts. The contents of the information security guidelines are specified in the instructions on information security for users², administration³, as well as in those concerning continuity and operations⁴.

General objectives and principles concerning the University's information security work

Active information security work helps to achieve set goals, create security for employees and collaboration partners, and to reduce/avoid damages.

The University's information security work is to be performed as a long-term objective, in a cost-effective and structured manner.

¹ The *Guidelines on Information Security* are part of the University's information security management system, LIS, and correspond to what is referred to as information security policy in the regulations of the Swedish Civil Contingencies Agency, MSBFS 2016:1.

² Appendix 1: Instructions on information security – User (Information security A – Staff), Appendix 2: Instructions on information security – User (Information security A – Students)

³ Appendix 3: Instructions on information security – Administration (Information security F)

⁴ Appendix 4: Instructions on information security – Continuity and operations (Information security KD)

The work is to be governed by the following principles:

- Information security issues are to be an integral part of the daily work.
- All employees and students are to be familiar with the content of, and be obliged to follow, applicable laws, ordinances, rules, regulations and agreements, and be aware of the responsibility involved when handling information.
- The same level of information security is to be maintained, regardless of where and in what form the information processing takes place.
- All information within the University is to be categorised so that it is possible to determine the type of protection required, and how the information can be managed.

Annual objectives for the work are to be decided and included in the planning of operations. For each annual objective, information is to be provided with regard to what is to be done during the year, including when and how, any need for staff and financial resources, when and how follow-up, evaluation and reporting will take place, as well as when and how employees will be informed and trained.

Allocation of responsibilities

In accordance with the University's rules of procedure and delegation, as well as other documents, the following stipulations particularly apply to information security:

- The vice-chancellor has overall responsibility for the information security within the University⁵.
- Managers and system owners are responsible for maintaining information security within their respective areas of responsibility, and for making sure that employees are informed and trained⁶.
- The chief security officer is responsible for supporting, training, implementing, and following up on the information security work conducted at the University.
- All students and staff are responsible for complying with the present information security guidelines and associated instructions⁷.
- All employees must undergo information security training⁸, offered by the University.

Appendices:

Appendix 1: Instructions on information security: User –Staff (Information security A – Staff)

Appendix 2: Instructions on information security: User - Students (Information security A – Students)

Appendix 3: Instructions on information security: Administration (Information security F), including sub-appendix Information security F – Appendix 1 – Instructions on information categorisation

Appendix 4: Instructions on information security: Continuity and operations (Information security KD)

⁵ Rules of Procedure for Lund University, reg. no STYR 2017/783

⁶ Appendix 3: Instructions on information security – Administration (Information security F)

⁷ Appendix 1: Instructions on information security – User (Information security A – Staff) or Appendix 2: Instructions on information security – User (Information security A – Students)

⁸ www.lu.se/kompetensportalen, decision, reg. no BY 2013/134



LUNDS
UNIVERSITET

Vice-Chancellor

22 June 2017

Reg. no STYR 2017/947

Instructions on information security: User – Staff

1. The document's role in information security work

This document is intended for all employees at Lund University, and contains instructions and information regarding information security work in the implementation of education, research and support activities within the University.

2. User responsibility

Every employee is responsible for complying with these information security instructions, and is required to undergo university-designated training.

Information that is published, made available or otherwise managed must comply with SUNET's rules¹ and not violate any laws, ordinances, regulations, rules and agreements.

3. Information management

Employees at Lund University are only allowed to process personal data to the extent and for the purposes that are included within the scope of their employment and the employee's work duties. Searching for, and viewing, data in IT systems out of pure curiosity or for other reasons not covered by the employment or user instructions is not permitted. This applies even if the information itself is a public document for which access may be requested in accordance with the Principle of Public Access.

4. Access to information

4.1 Login and password to protect information

Passwords assigned at the University are to be changed immediately to a personal password. Passwords must not be disclosed or stored in such a way that it may become accessible to others.

4.2 User terms

All users will be required to approve the University's user terms² in connection with the award of a LUCAT ID.

5. Workplace protection, etc.

5.1 Equipment

All installation, configuration, operation and utilisation of equipment connected to the University's computer network shall be performed in a way that ensures high information and computer security. If different options are available, the option

¹ <https://www.sunet.se/policy-for-tillaten-anvandning/>

² IT user terms, STYR 2016/361

that requires reasonable effort in order to provide the highest level of security shall be chosen.

5.2 Connection to the University's network

Only University equipment or equipment approved by an authorised technician may be connected to the University's physical network. Using the University's computer network for non-university purposes without permission, transferring or reselling computers or network capacity to other persons or organisations, is not permitted.

5.3 Software

Only authorised persons may install software on the University's computers. Installation is normally to be performed after receiving approval from the relevant manager. Only software that has a valid license, or software that may be shared without a license, can be installed on a University computer. It is not permitted to modify or copy the University's licensed software or to make these available to people outside the organisation.

Software installed on private devices, with reference to Home Usage Agreements, must be uninstalled immediately after the employment has ended.

5.4 Service on equipment

Before handing over equipment to an external party for service, any confidential information must be removed, as far as possible.

5.5 Discarding of equipment

Equipment which is to be discarded must be handed over to the person who is technically responsible for ensuring that it is handled properly, from an environmental and security perspective.

5.6 Mobile phones, tablets, etc.

Mobile phones or other similar equipment belonging to the University, or configured to connect automatically to the University's services, e.g. an email server, are to be configured so that the enable screen lock (equiv.) is activated automatically if the device is not used within a maximum of five minutes. It is not permitted to bypass the operating system's built-in security functions on equipment owned by the University.

5.7 Storing of information

Information may be stored in cloud services if the following three criteria have been fulfilled:

1. A documented legality assessment based on the Personal Data Act has been implemented, and the use of the cloud service is deemed to be in accordance with the Personal Data Act. Among other things, this means that a personal data assistance agreement has been established with the cloud supplier. Furthermore, a position must have been taken with regard to:
 - whether there is a risk that personal data may be processed for purposes that are contrary to the original one,
 - whether the cloud supplier may transfer personal data to a non-EU/EEA country and, if so, what legal support for the transfer can be found in the Personal Data Act,

- which security measures need to be taken to protect the processed personal data.
2. A risk and vulnerability analysis has been carried out, and the analysis does not demonstrate any risks that justify that the operation should abstain from using the cloud service.
 3. The head of department (equiv.) is responsible for the implementation of the legality assessment and risk and vulnerability analysis before the cloud service is ordered and put into use.

Every user must ensure that documents, data files, etc. are backed up to a location where the University has access to the information.

Storing occasional private images, files or texts on university equipment is permitted; however, the user responsibility under item 2 above must be observed.

5.8 Private use

The University's equipment may be used for private purposes, but only to such an extent that it does not interfere with the work or involve unnecessary costs for the University.

6. Internet

Visits to websites on which the content may be perceived as offensive, unethical or otherwise objectionable must first be approved by the head of department and communicated to the University's information security coordinator³.

6.1 General use

The following rules apply to internet use:

- The use must not risk damaging the public's confidence in the University.
- Access to university e-services, etc. for students, staff and collaboration partners must not be adversely affected.
- The use must not conflict with the University's core values.

6.2 The University's right to suspend access to the University's network

The University has the right, for safety reasons without prior warning, to temporarily suspend all or parts of the network and its services if necessary to protect the University's activities. The decision to suspend is made by the University's chief security officer or in accordance with the provisions of the LU-IRT⁴.

6.3 Private use

The internet connection may be used for private purposes, but only to such an extent that it does not interfere with the work, affect accessibility to the University's online services, etc., or involve unnecessary costs for the University.

7. Email

7.1 Email management

³ The University's chief security officer

⁴ <http://www ldc.lu.se/tjanster/it-sakerhet>

The following rules apply to the use of email:

- Information subject to confidentiality or secrecy must not be sent via unencrypted communications (as regular email). When such information is communicated electronically, via e.g. email, the data must be encrypted in such a way that only the intended recipient can access the data.
- Receiving and sending university-related matters from and to your own private email address is not permitted.
- Automatically forwarding emails to an external email address is not permitted.
- Private emails may only be received and sent from the University's email address to a limited extent.
- Private emails are to be deleted immediately or stored in a special folder marked "Private".

8. Control of computer usage

8.1 Logging

All emails and internet traffic in the University's network are logged and, as an employer, the University has the right to review these logs and, in certain circumstances, read the content of emails in order to make sure that the rules in legislation or public authority guidelines are followed, and in order to perform the duties of the University as well as to identify, manage or counteract information security threats. The same applies to files and other materials stored in computers and transported through networks.

Information systems log information that is relevant to the operation of the service, e.g. usernames, times, computer addresses etc. For network traffic, the username, computer address, destination address, type of service, visited websites and times are logged.

Log files are deleted after no later than three months. If an investigation has begun, the data will be retained as long as the investigation requires it.

8.2 Control measures

As an employer, the University does not regularly check the content of employees' computers, emails, or internet traffic, in order to respect their privacy as far as possible. However, the University may check information stored on a computer, emails and internet traffic if necessary

- in order to fulfil its obligations as a public authority, such as public access to official documents,
- in case of a threat to information security,
- in order to investigate or prevent crimes and professional misconduct in accordance with the University's guidelines⁵,
- on behalf of the police or other law enforcement authorities,
- in case of a threat to someone's life or health.

If abuse is investigated by someone other than the University, data may be provided to law enforcement authorities.

⁵ Guidelines for the handling of cases of suspected professional misconduct, reg. no STYR 2014/410

Decisions concerning control measures are taken by the head of department (equiv.) or higher authority. The University's chief security officer is to be notified immediately of any decisions on control measures.

9. Sanctions

Failure to comply with these information security instructions may lead to legal sanctions with regard to your employment, or other measures⁶. If a government employer finds that an employee is justifiably suspected of certain crimes that may lead to a penalty other than a fine, the employer is obliged, in accordance with Section 22 of the Public Employment Act (1994:260), to bring the suspected crime to prosecution. Other cases may also be reported to the police for investigation.

⁶ Legal sanctions relating to employment include disciplinary measures such as a warning or a deduction from wages, notice of termination of employment or, in serious cases, suspension or immediate termination of employment.



Instructions on information security: User – Students

1. The document's role in information security work

This document is intended for all students at Lund University, and contains instructions and information regarding information security work in the implementation of education and research at the University.

2. User responsibility

Every student is responsible for complying with these information security instructions. Information that is published, made available or otherwise managed must comply with SUNET's rules¹ and not violate any laws, ordinances, regulations, rules and agreements.

3. Information management

The University is responsible for personal data processed within the context of studies at Lund University. Personal data may only be processed to the extent and for the purposes that are included within the scope of study. This applies even if the information itself is a public document for which access may be requested in accordance with the Principle of Public Access.

4. Access to information

4.1 Login and password to protect information

Passwords assigned at the University are to be changed immediately to a personal password. Passwords must not be disclosed or stored in such a way that it may become accessible to others.

4.2 User terms

All users will be required to approve the University's user terms² in connection with the award of a StiL ID.

5. Study space protection, etc.

5.1 Connection to the University's network

Only University equipment or equipment approved by an authorised technician may be connected to the University's physical network. Using the University's information network for non-university purposes without permission, transferring or reselling computers or network capacity to other persons or organisations, is not permitted.

5.2 Software

¹ <https://www.sunet.se/policy-for-tillaten-anvandning/>

² IT user terms, STYR 2016/361

Only authorised persons may install software on the University's computers. Only software that has a valid license, or software that may be shared without a license, may be installed on a University computer. It is not permitted to modify or copy the University's licensed software or to make these available to people outside the organisation.

Software installed on private devices, with reference to Student Usage Agreements, must be uninstalled immediately after the termination of studies.

5.3 Mobile phones, tablets, etc.

Mobile phones or other similar equipment configured to connect automatically to the University's services, e.g. an email server, are to be configured so that the enable screen lock (equiv.) is activated automatically if the device is not used within a maximum of five minutes.

5.4 Private use

The University's equipment may be used for private purposes, but only to such an extent that it does not infringe on the University's activities, or involve unnecessary costs for the University.

6. Internet

6.1 General use

When using the University's internet connection, the following rules apply:

- The use must not risk damaging the public's confidence in the University.
- Access to university e-services, etc. for students, staff and collaboration partners cannot be adversely affected.
- The use cannot conflict with the University's core values.

6.2 The University's right to suspend access to the University's network

The University has the right, for safety reasons without prior warning, to temporarily suspend all or parts of the network and its services if necessary to protect the University's activities. The decision to suspend is made by the University's chief security officer or in accordance with the provisions of the LU-IRT³.

6.3 Private use

The internet connection may be used for private purposes, but only to such an extent that it does not affect accessibility to the University's online services, etc., or involve unnecessary costs for the University.

7. Email

7.1 Email management

The following rules apply to the use of email:

- Information subject to confidentiality or secrecy must not be sent via unencrypted communications (as regular email). When such information is communicated electronically, via e.g. email, the data must be encrypted in such a way that only the intended recipient can access the data.

8. Control of computer usage

8.1 Logging

³ <http://www ldc.lu.se/tjanster/it-sakerhet>

All emails and internet traffic in the University's network are logged and, as a network owner, the University has the right to review these logs and, in certain circumstances, read the content of emails in order to make sure that the rules in legislation or public authority guidelines are followed, and in order to perform the duties of the University as well as to identify, manage or counteract information security threats. The same applies to files and other materials stored in computers and transported through networks.

Information systems log information that is relevant to the operation of the service, e.g. usernames, times, computer addresses etc. For network traffic, the username, computer address, destination address, type of service, visited websites and times are logged.

Log files are deleted after no later than three months. If an investigation has begun, the data will be retained as long as the investigation requires it.

8.2 Control measures

The University does not regularly check the content of students' emails or internet traffic, in order to respect their privacy as far as possible. However, the University may check information in emails and internet traffic if necessary

- in order to fulfil its obligations as a public authority, such as public access to official documents,
- in case of a threat to information security,
- in order to investigate or prevent crimes,
- on behalf of the police or other law enforcement authorities.

If abuse is investigated by someone other than the University, data may be provided to law enforcement authorities.

Decisions concerning control measures are taken by the head of department (equiv.) or higher authority. The University's chief security officer is to be notified immediately of any decisions on control measures.



Vice-Chancellor

Instructions on information security: Administration

1. The document's role in information security work

This document is intended for system owners and administrators and regulates the basic information security requirements for those who own or manage information systems within Lund University.

2. Organisation and responsibilities

2.1 Management

The vice-chancellor makes the overall decisions on how information security work is to be conducted.

2.2 IT coordination group, SamIT¹

On behalf of the university management, the group is to handle and investigate general issues concerning the acquisition, operation, administration and discontinuation of information management resources. This includes issues relating to information security.

2.3 Information security coordinator

The information security coordinator² supports the work to achieve the objectives of the information security policy. The information security coordinator supports the system owners' efforts to carry out individual system security analyses. The information security coordinator may, if necessary, initiate system security analyses.

2.4 System owner

Within the scope of allocated delegations, the system owner makes decisions on the implementation, operation, administration and discontinuation of their own information systems. The system owner is responsible for ensuring that administration planning, including system security analyses, are conducted in accordance with the University's system administration model³ and that information security classification is conducted in accordance with Appendix 1 to this document – Instructions on information classification.

The system owner is responsible for ensuring that there are authorisation levels, user guides, manuals, etc. for the relevant system. The system owner is also responsible for informing users about their rights and obligations in the use of their respective information systems and, if necessary, offering training to obtain

¹ <http://www.lu.se/samit>

² The University's chief security officer has been appointed to this role

³ LU's system administration model, <http://www3.lu.se/luwiki/index.php/Systemförvaltning>. The model complies with the Swedish Civil Contingencies Agency's model, BITS Plus.

sufficient knowledge. The system owner is responsible for reporting system administration plans and appendices to the IT coordination group, SamIT.

2.5 System administrator

The system administrator has the operational expertise and is appointed by the system owner. The system administrator works with the day-to-day operation and administration of the information system concerned.

2.6 IT system owner

The IT system owner is responsible for making sure that the technical aspects of the information system are working. The IT system owner is responsible for establishing Information security KD⁴.

2.7 IT system administrator

The IT system administrator has the technical expertise, and works together with the system administrator to maintain the day-to-day operations in accordance with the administration plan.

3. Rules and procedures

3.1 Responsibility for assets

Every physical information processing asset (i.e., servers, computers, mobile phones, tablets, etc.) must be listed and have a unique number. The list is to indicate where the assets are located and who is responsible for the asset. Relocation and transfer of access may not be done without consultation with the person in charge.

3.2 Qualification requirements when using the University's information systems

The head of department/equivalent is responsible for giving new users an introduction to the University's information security work before assigning authorisations to the respective systems.

3.3 Secure spaces

Sensitive information from information systems shall be stored on resources in computer halls equipped with control systems for entry and exit. Logging of access is to take place. Spaces with console equipment shall be locked when vacated. Spaces equipped with access points are to be locked. Decisions on access are taken by the respective IT system owners.

Sensitive information not handled in information systems are to be stored in safety cabinets that are fire-rated for at least 120 minutes.

3.4 Control of external service suppliers

Those who order services from external suppliers are to follow up and review that the supplier meets the University's minimum security requirements.

3.5 Data media management

⁴ LU's system administration model, ITSÄ, Appendix 3 – Information security KD

Data media containing sensitive information which will no longer be used in the University's activities shall be handed over to the IT system owner responsible for ensuring that it is destroyed appropriately, from an environmental and security perspective.

3.6 Transfer of physical information storage access

If media containing sensitive information has to be transported physically, the chief security officer is to be contacted before taking any decision on how to proceed.

3.7 Surveillance

With regard to the information systems' logs, the system owner is to decide:

- the purposes for which a log may be analysed
- how often they are to be analysed
- who is responsible for analyses of them
- how long they are to be stored if deviation from the standard 90⁵ days is to be made
- how they are to be stored

3.8 Control of user access – authorisation management

In order to ensure that only authorised users are present in the information systems, control of access to information systems shall, as far as possible, be exercised through the University's identity and authorisation system⁶. The system owner decides on the access and any deviation from the aforementioned authorisation system.

The University applies two levels of authorisation management; partly a traditional authorisation management that determines which users have access, and partly the use of trust levels⁷ that signal how well the user has been identified.

3.9 Control of access to computer networks

All installation, configuration, operation and utilisation of equipment connected to Lunet⁸ shall be performed in a way that ensures high information and IT security and in accordance with the requirements set out in each case. Providing services that allow anonymous use of the computer networks is not permitted.

3.10 Control of access to operating systems

The IT system owner decides to what extent operating systems, administrative tools, or other system tools that can override system and application barriers, may be used.

3.11 Mobile computer usage and remote work

The system owner decides whether the data in an information system may be managed remotely on a desktop or mobile device.

⁵ Recommended time of storage, in accordance with the Swedish Data Protection Authority

⁶ LUCAT

⁷ The University applies the trust framework established in higher education in Sweden. *Confirming user* is to be used in information systems with a particularly high protection value. *Confirming users* are users who fulfil SWAMID Assurance Level 2. The trust framework, with levels SWAMID Assurance Level 1 and SWAMID Assurance Level 2, is based on the international trust framework, Kantara Initiative

⁸ The University's fixed and wireless computer network, <http://www ldc lu se/tjanster/natverk>

3.12 Security requirements for information systems

Prior to the acquisition and implementation of a university-wide information system, the manager in charge, in consultation with SamIT, shall draft a plan⁹ for the implementation, which shall also be possible to use for the procurement of such systems.

3.13 Security in development and maintenance processes

Suggestions for changes in the system are to be submitted to the system administrator. The work shall be conducted in accordance with the University's system administration model¹⁰, and project model¹¹.

3.14 Management of information security incidents and improvements

The system owner and IT system owner shall, via the University's incident reporting system¹², report:

- infringement and advanced attempts at infringement
- incidents that cause or could cause significant interruptions and disturbances
- sanctions and suggestions for measures after infringement or malfunction

Suspected breach of legislation or internal regulations must be reported in accordance with the University's *Guidelines for the handling of cases of suspected professional misconduct*¹³.

⁹ Containing a needs description, security analysis, commissioning requirements, etc.

¹⁰ <http://www3.lu.se/luwiki/index.php/Systemförvaltning>

¹¹ <http://www3.lu.se/luwiki/index.php/Projektkontoret>

¹² <http://www.lu.se/alarm>

¹³ <http://www.medarbetarwebben.lu.se/organisation-och-styrning/regler-och-beslut/regelverket/regler-juridik-och-dokumenthantering>



Information security F, appendix 1 – Instructions on information classification

Information classification with regard to the need for security

The purpose of classifying the information, based on the security aspects below, is to assess the requirements for how the University's information and relevant information systems are to be managed.

The classification model is based on three recognised information security aspects, in accordance with SS-ISO/IEC 27001: *confidentiality*, *accuracy* and *accessibility*. In addition, there is the possibility of adding aspects (e.g. traceability, interruption protection, authenticity, non-deniability, etc.) for which there are special requirements on information security.

SECURITY ASPECT	OBJECTIVE
CONFIDENTIALITY	The information is not to be made available or disclosed to unauthorised persons, systems or processes
ACCURACY	The information is not to be altered or destroyed, without authorisation, by mistake or due to malfunction
ACCESSIBILITY	The information is to be accessible and usable in the expected manner and within the requested time

Areas of application

The concrete areas of application, in which an information classification, according to its instructions, should be the basis for the choice of security level and associated security measures, are:

- Requirements/requirements specification for system development or procurement of systems
- Determining the security design of an information system
- Implementation of risk and threat analyses of a system administration object or single individual information system
- Implementation of information security analyses (self-checks) in an administration object or single individual information system
- Determining management rules of information, e.g. with regard to encryption requirements for emails, rules for and possible labelling of internal and external mail, communication via mobile phone etc.

Security levels

The classification is based on the extent of the consequences that may arise from deficient protection. The need for security (protection) for information is described as one of the levels: **basic level**, **high level** or **special requirements**.

Public information, such as information downloaded from the internet, publicly available text or images, do not require classification. One could say that there is one additional level – “Unclassified” – without any specified need for security.

The need for security levels is described separately for each of the three security aspects, supported by the *Template on information classification* below.

Template on information classification

1 Description of the security levels

1.1 Confidentiality

The need for protection against the information being made available or disclosed to unauthorised persons, systems or processes.

Basic level

General description

Information that requires protection from unintentional or unauthorised access. Information that is deliberately made available to the public.

Example of information

Most of the information at the University (work material, but also public documents) is included in the basic level.

Example of protection

The information is to be protected from unintentional or unauthorised access by requiring a login, locking it away or by means of other protective storage. Public information is to be accessible in a controlled manner.

Possible consequences of deficiencies

Deficiencies in protection can cause discomfort or limited financial loss for individuals, or limited damage to the University or to third parties.

High level

General description

Information that requires strong protection from unintentional or unauthorised access, including information subject to confidentiality.

Example of information

Information protected by confidentiality, highly sensitive information relating to privacy (for example, information about illness).

Example of protection

The information is to be protected through qualified encryption, locking it away in a safe cabinet, or through other equivalent protection.

Possible consequences of deficiencies

Deficiencies in protection can cause significant discomfort or financial loss for individuals, or significant damage to the University or to third parties.

Special requirements (could entail one or several aspects of confidentiality protection)

General description

Information that requires particularly strong protection against unintentional or unauthorised access, including protection against advanced attacks intended to access the information.

Example of information

Protected identities or addresses. Particularly sensitive research information (company secrets, etc.). Information subject to national defence secrecy.

Example of protection

Highly advanced protection against unauthorised or unintentional access, and protection against advanced attacks intended to access the information shall be in place.

Possible consequences of deficiencies

Deficiencies in protection can cause harm to the life or health of individual persons, or significant discomfort or financial loss for a large number of persons, or very serious damage to the University or to third parties.

2.2 Accuracy

The need for protection against the information being altered or destroyed – without authorisation, by mistake or due to malfunction.

Basic level

General description

Information that requires basic protection against alteration or destruction.

Example of information

Most of the information at the University (work material and public documents) is included in the basic level.

Example of protection

The information is to be protected – through backup, careful testing of programs, protected storage, signature on documents etc. – against unintentional or unauthorised alteration or destruction.

Possible consequences of deficiencies

Deficiencies in protection can cause discomfort or limited financial loss for individuals, or limited damage to the University or to third parties.

High level

General description

Information that requires strong protection against alteration or destruction.

Example of information

Decisions and other information that have legal effects, or which are of major significance to the University or individuals. Accounting material, information in accounting and bookkeeping systems, lists of exam results. Research data of major scientific or financial significance.

Example of protection

The information is to be well protected
– by logging changes, digital signatures, manual signatures, careful management routines, etc. – against unintentional or unauthorised alteration or destruction.

Possible consequences of deficiencies

Deficiencies in protection can cause significant discomfort or financial loss for individuals, or significant damage to the University or to third parties.

Special requirements (could entail one or several aspects of accuracy protection)

General description

Information that requires particularly strong protection against alteration or destruction.

Example of information

PhD theses in the original. The Ladok database's tables of persons and their study results. Agreements in the original.

Example of protection

Highly advanced protection against unintentional and unauthorised changes, for example, through the use of certificate-based digital signatures and checksums. Specially designed routines for backup and logging of changes.

Possible consequences of deficiencies

Deficiencies in protection can cause harm to the life or health of individual persons, or significant discomfort or financial loss for a large number of persons, or very serious damage to the University or to third parties.

2.3 Accessibility

The need for protection enabling the information being accessible and usable in the expected manner and within the requested time

Basic level

General description

Information that normally is to be accessible around the clock (or at specially defined times), but where limited interruptions, up to a half a working day, only cause limited damage.

Example of information

Most of the information at the University (work material and public documents of primarily internal interest) is included in the basic level.

Example of protection

The information is preferably to be accessible around the clock. Interruptions in accessibility during office hours should not exceed 4 hours. The accessibility of the information is to be enabled through stable and well-tested IT systems, and working support procedures.

Possible consequences of deficiencies

Deficiencies in protection can cause discomfort or limited financial loss for individuals, or limited damage to the University or to third parties.

High level

General description

Information that is to be accessible around the clock (or at specific times) without interruption. Certain brief interruptions only cause limited damage.

Example of information

The University's external webpages. Information that students need to complete their studies or exams (e.g. information about times and premises). Joint email systems. Information on file servers. Public documents of major interest to the public.

Example of protection

The information is to be accessible around the clock. Interruptions in accessibility should not exceed 0.5 hours. Planned interruptions are to be announced in good time.

Possible consequences of deficiencies

Deficiencies in protection can cause significant discomfort or financial loss for individuals, or significant damage to the University or to third parties.

Special requirements (could entail one or several aspects of accuracy protection)

General description

Information that must be accessible around the clock (or at specific times), without interruption, and where even brief interruptions can cause major damage.

Example of information

Directory and login services (the information in these). DNS, DHCP and other services of major significance for the utilisation of all IT services at the University.

Example of protection

Redundant systems and other measures to allow practically uninterrupted access, despite very serious disturbances (redundant systems in different premises, etc.).

Possible consequences of deficiencies

Deficiencies in protection can cause harm to the life or health of individual persons, or significant discomfort or financial loss for a large number of persons, or very serious damage to the University or to third parties.

INFORMATION CLASSIFICATION TEMPLATE
Version 1.0, 2 February 2017

Information resource (<i>administration object, information system, project etc.</i>)	
Date	
Participant	

Confidentiality

Objective: The information is not to be made available or disclosed to unauthorised persons, systems or processes

Level	In place	Example of information belonging to this level
Basic level		
High level		
Special requirements		
State the special requirements:		

Accuracy

Objective: The information is not to be altered or destroyed, without authorisation, by mistake or due to malfunction

Level	In place	Example of information belonging to this level
Basic level		
High level		
Special requirements		
State the special requirements:		

Accessibility

Objective: The information is to be accessible and usable in the expected manner and within the requested time

Level	In place	Example of information belonging to this level
Basic level		
High level		
Special requirements		
State the special requirements:		

Summary

Security aspect	Basic level	High level	Special requirements
Confidentiality (secrecy)			
Accuracy (privacy)			
Accessibility			

Comments on the assessments

#	Comments



Vice-Chancellor

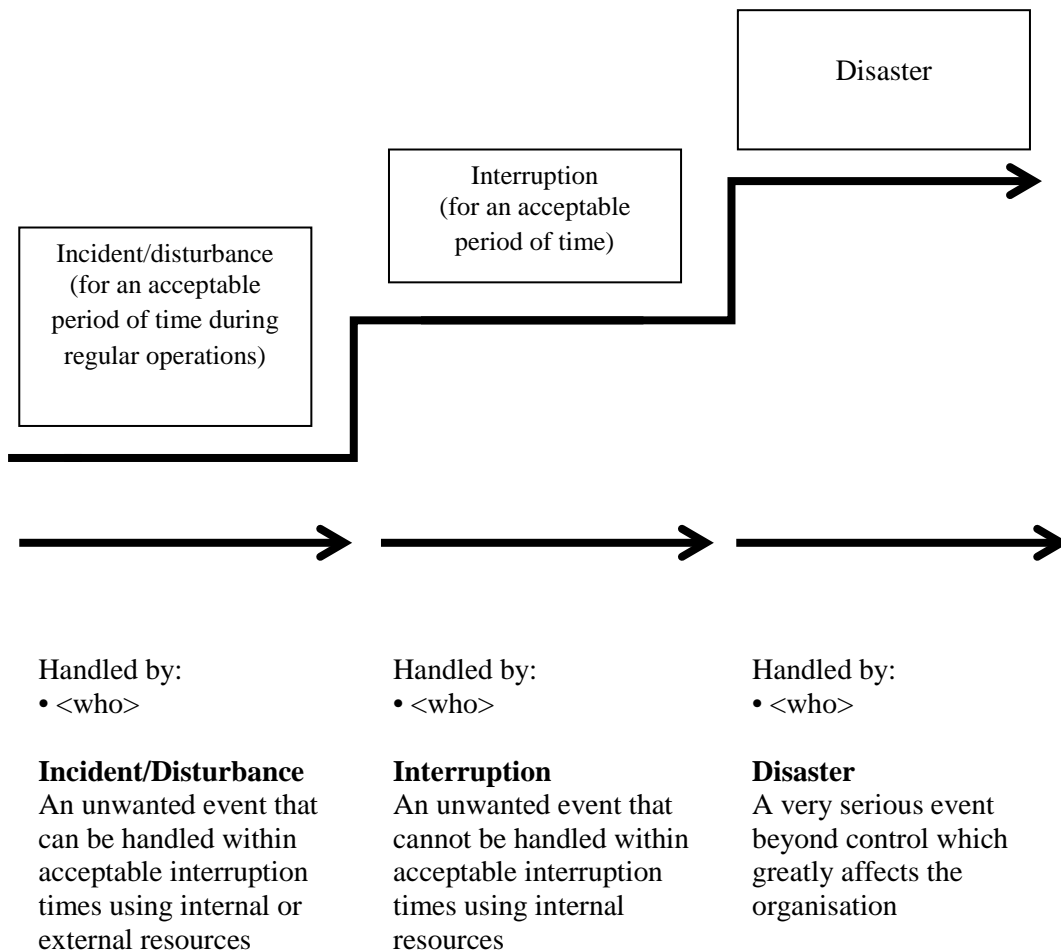
Instructions on information security: Continuity and operation

1. The document's role in information security work

This document is intended for LU's IT organisations or other functions, responsible for the IT operations of information systems at Lund University.

2. Organisation of and responsibilities for security work

The model below describes how service interruptions are handled during different stages of disturbance/interruption.



The management organisation at different stages varies. Generally, this means that the organisation grows gradually as the event escalates.

Support

Describe the staffing and work duties of the support organisation. For example:

The support organisation is staffed daytime during weekdays, and is the first step in the IT service organisation. The support is to:

- *receive reports on all types of events*
- *create a diary with space to include the time and date of the report, who filed the report and, if possible, how the event occurred or was discovered (during implementation)*
- *classify the events – (incident, interruption or disaster?)*
- *handle incidents and disturbances*
- *prepare for the interruption and disaster stage by convening the affected parties*

The support organisation is to have:

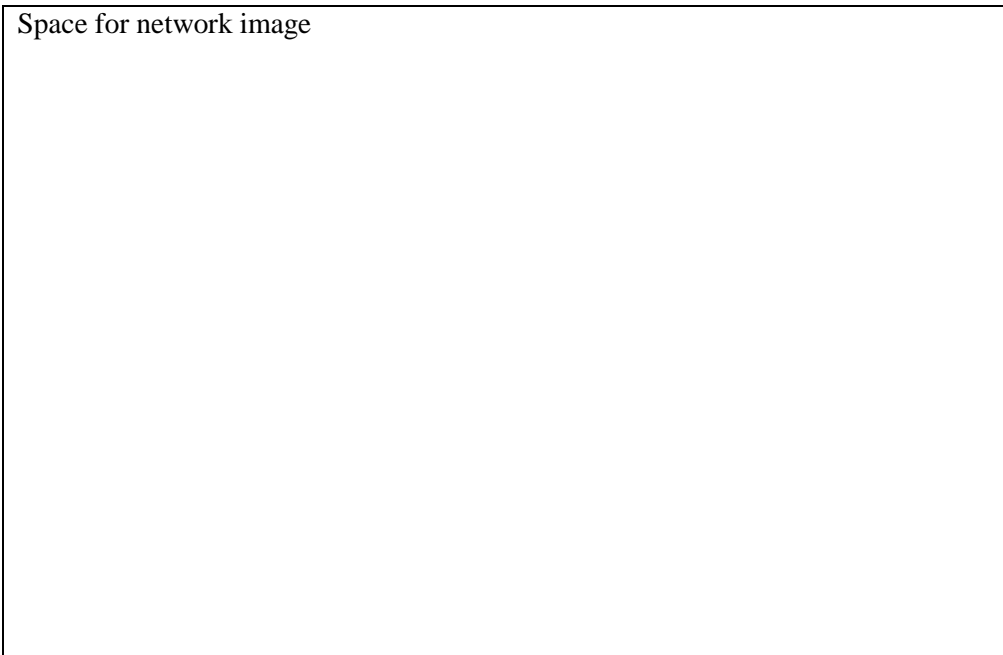
- a list of all the resource persons
- a list of all current agreements with contact persons

The support organisation is also to keep checklists for the most serious threats, such as:

- malware attack
- restore and recovery
- etc.

3. Internal networks of the organisation

Space for network image



4. Network resource requirements

Describe the units in the internal network to be protected in the table below.

The requirements in the table for each unit is based on the

- compiled threat analysis for the applications in the organisation that are part of the internal network
- information stored or transported

The organisation's joint information security instructions for continuity and operation are based on the table.

B=Basic level, HN=High level & MHN=Very high level.
(Examples of resources. Add as many lines as you need.)

Resource	Placement	Information system	Requirement level Accessibility
Application servers	VLAN		B
Backup server	VLAN	Backup server with external storage	HN
Database servers	VLAN		HN

5. Implemented measures

(Examples of measures)

Resource	Implemented measures / Substitute procedure
Clients	<ul style="list-style-type: none"> • The latest security-related updates are installed, both with regard to the operating system and the applications • Antivirus software is installed and updated continuously
Servers	<ul style="list-style-type: none"> • The latest security-related updates are installed both with regard to the operating system and the applications • Antivirus software is installed and updated continuously
Computer hall	<ul style="list-style-type: none"> • Equipment for moisture and temperature alerts are in place • UPS available • Automatic fire alarm equipment • Handheld fire extinguisher available

6. Day-to-day operations

6.1. Resources

6.1.1. Premises and equipment

Describe the physical environment where equipment is located and used. For example:

The server hall:

The server hall acts as the base of the server park's physical location. The premises have appropriate equipment, such as air conditioning, UPSs, elevated anti-static floors, etc.

Lecture halls:

The organisation has a number of lecture halls which usually consist of a thin client as well as projectors, through which the lecturer can connect to the environment that they want so that they can carry out their teaching.

6.1.2. Software/register – Applications

Describe the physical environment where equipment is located and used. For example:

Software managers:

The organisation uses LDC software for most software applications. If the desired software is unavailable, it is purchased/leased with the relevant supplier.

Lund University has Campus agreements with Microsoft, Adobe, Alfasoft (Endnote), among others, which gives all employees the right to use these products in their work.

We also have MSDNAA – an agreement signed with Microsoft – which gives students free access to download a number of Microsoft software to use in their studies.

6.1.3. Labelling and denomination

Describe whether and, if so, how equipment is labelled, as well as how the labelling is documented. For example:

All IT equipment that is disseminated to users is labelled with the computer name, following the department name and the serial number.

Our documentation is stored in Live@Lund (Sharepoint environment).

Parts of the documentation can also be found in Nettools.

Servers and other network equipment that are to act as a service to the organisation's users are also to be labelled according to the standard procedure.

6.1.4. Classification of resources

Describe the practical implementation of information classification of the content of servers

6.1.5. Workplaces

Describe how workplace computers are handled. For example:

The workplace clients consist of standardised hardware from “long-term series”. The hardware consists of desktop/personal laptop computers as well as thin clients.

Software installation is performed using standard images (via “Ghost”) containing current OS and workplace software, such as MS Office, Adobe Acrobat, Endnote and programs as needed.

6.1.6. Relocation and transfer of IT equipment

Describe how the relocation and transfer of all IT equipment to other users is carried out, including methods for destroying discarded storage media.

6.2. Physical protection

6.2.1. Air conditioning

Contact details:

6.2.2. Fire safety protection

Contact details:

6.2.3. Access control

Describe methods and rules for physical access to server halls and other areas where computer or network equipment is located. For example:

Physical access – server hall

- *The server hall is an “independent company” in the passage system, with limited authorisation.*
- *In the event of a lost card: www.lu.se/lucardet*

Physical access – public spaces

- *Access to public spaces is handled in accordance with normal rules.*
- *In the event of a lost card: www.lu.se/lucardet*

6.3. Communication

6.3.1. LAN

Describe LAN configuration. For example:

The organisation’s network is divided into VLAN by function. Servers, printers, clients, etc. are divided into different networks. These networks are separated by a firewall.

The communication takes place with IP v4. All communication equipment is stored in locked areas and is part of CFL. Network management is carried out by the ITS group and resources from LDC.

6.3.2. Remote access/VPN

Is remote access used? How? For what?

Remote access (Remote Desktop Connection, RDC) is used for server management. Client connection outside our client networks use LDC’s VPN service.

6.3.3. Firewall

Are firewalls used? Which? How?

We use the LDC's services for firewalls, which actively logs any failed traffic.

Firewall monitoring is included in the service.

The logs are checked by us in the event of a suspected issue.

6.4. Roles and responsibilities – IT

Describe the roles that exist and who serves in these roles.

6.5. Access rights – user

6.5.1. Accounts

On what grounds are accounts allocated?

How are they created?

How is it documented?

How are they maintained (removed)?

6.6. Logging and traceability

6.6.1. Surveillance

What is surveilled? With the help of which application/s? For example:

- *Our servers are monitored with MS SCOM*
- *We have surveillance of operating systems, DNS, AD, DFS, SQL, email, Sharepoint, the web*
- *Surveillance of hardware via ILO*
- *Certain performance surveillance with SCOM*

6.6.2. Log management

Describe how you ensure that relevant logs are preserved. For example:

Backup software performs a backup of logs.

6.6.3. Log analysis

Describe how and when logs are analysed. For example:

Logs are analysed when systems do poorly or SCOM has reacted to something.

6.7. Backup

6.7.1. Intervals and scope

Describe how backup is performed, what is backed up and for how long these backups are saved. For example:

Documentation of system owners' decision regarding:

- *All servers, including the clients' home directories and profiles are included in the backup*

- *Backup is performed on a daily basis, weekly and once a month*
- *The various backup methods have different periods of protection against overwriting*
- *The backup system is physically separated from other servers*
- *The backup medium consists of a deduplication technique*
- *Verification of backups is always performed*

7. Disturbances/interruptions

7.1. Interruption plan

Describe how you respond in case of interruption. For example:

If there is a power outage, we have battery power for approximately 50 minutes. This is to enable us to shut down all servers.

7.2. Backup power and backup routines

Describe backup routines. For example:

In case of a power outage, the entire server hall will switch to UPS. At the same time, information will be sent to SCOM, which in turn sends an email to the support organisation. A presetting is in place to ensure that nothing will happen in the first 15 minutes. After that time, the systems will begin to shut down. This is performed using <method>.

Systems which are shut down after 15 minutes:

- *<list systems >*

Systems which are shut down after 45 minutes:

- *<list systems >*

7.3. Backup power

Is there backup power? Capacity? Which functions/systems are covered by backup power? Who performs service/maintenance?

7.4. Reboot procedures

What are the reboot procedures like? In what order are the systems to be rebooted? What checks are to be carried out in connection with a reboot? Who is to perform them? How is it to be documented? Who is to be notified?

8. Incident management

8.1. Updating of antivirus software

Describe how to ensure that all relevant machines have updated antivirus protection. For example:

All desktops and servers are updated via antivirus servers as soon as there are new updates. The antivirus server is updated from Symantec whenever new updates are available.

8.2. Preventative measures

Describe what preventive measures you apply to ensure continuous operation. For example:

- *Antivirus software*
- *Firewall*
- *Backups*
- *Profile management: local directories such as “My Documents” directed to server.*

8.3. Documentation of occurred incidents

Describe how incidents, or feared incidents, occur, are handled, documented and reported. For example:

Someone contacts us or we ourselves discover that something is not right on a server.

- *Two people investigate the matter, recording everything that is observed and done.*
- *Find out as much as possible before the server is shut down*
- *Some examples:*
 - *What is the time and dates on the server, and are these different from the actual time?*
 - *IP addresses, hostnames*
 - *Other potentially deviating aspects*
- *Run an image (disk copy) live in the server before it is shut down to be able to review the data more closely at a later date.*
- *Now you can shut down the server and start looking at the image instead.*
- *Check when the antivirus protection software was last updated, as well as Windows Update.*
- *Check user accounts, etc.*
- *Report to LU IRT and/or www.lu.se/alarm*

9. Documentation

Describe how the documentation is kept up-to-date and available to the concerned staff.