

Information Security Policy

for

the University of Copenhagen

This document is designed for all employees and students of the University of Copenhagen, as well as others associated with the University, all of whom will be referred to below as internal users. The document is also a declaration to the outside world that the University has adopted a policy on information security (IS) which is in accordance with recognised standards, in order to safeguard and protect the University's information assets, as well as to contribute to underpinning the University of Copenhagen's positive reputation and standing.

Preamble

The Information Security Policy (IS policy) serves as the over-arching framework for information security at the University of Copenhagen, henceforth often referred to as just 'KU' or 'the University'.

The IS policy underpins KU's Strategic Action Plan 2008-2012, which is available at <http://www.ku.dk/destination2012/>.

KU will at any given time comply with the current Danish standard for information security, as well as Danish legislation and other government guidelines.

As part of overall security management, the Information Security Committee (ISU) will reassess the IS policy at least once per annum on the basis of ongoing monitoring and reporting of incidents.

Revision of the IS policy is approved by the Rector on recommendation from ISU and processing by the General Consultation Committee.

Purpose

Data and information, as well as information systems to process them, are necessary and vital for KU, and information security therefore has vital significance for KU's credibility and its ability to function.

The purpose of the IS policy is to define a framework for the protection of KU's information, and in particular to ensure that critical and sensitive information and information systems retain their confidentiality, integrity and accessibility. KU's management has therefore decided that its level of protection should be determined in accordance with considerations of risk and importance, as well as in compliance with statutory requirements and any agreements already entered into, including the terms of licenses.

The management will inform all of KU's internal users about their responsibility in relation to KU's information and information systems.

Furthermore, the intention of the IS policy is to communicate to everyone that use of information and information systems at KU is subject to recognised standards and guidelines. The pur-

pose of this is to prevent breaches of information security, limit damage in the event of a breach, and facilitate the restoring of information.

Scope

The policy covers KU's information, which is defined as any information that belongs to KU, as well as information that does not belong to KU but for which KU can be held responsible. For example, the policy covers all information about staff, all financial information, all administrative information, research information, production information and system data, as well as information provided to KU by others. Such information may comprise factual information, notes, registrations, reports, planning material, or any other information designed only for internal use.

This policy covers all of KU's information, regardless of the form in which it is stored and communicated.

This policy covers all users without exception – i.e. students, permanent staff and people temporarily associated with KU.

In conjunction with any invitation to submit tenders for parts of, or the whole of, KU's IT operations, safeguards must be put in place in co-operation with the supplier, which ensure that said supplier, its facilities and its staff who have access to KU's information comply with and live up to the standards of KU's information security policy.

Security level

It is KU's policy to protect its information and exclusively allow access to, use of and publication of said information in accordance with KU's guidelines and in compliance with current legislation at any given time.

Based on risk assessments, KU sets a safety level that corresponds to the importance of the information concerned. KU will regularly conduct a balanced risk and consequence assessment, with due deference to financial conditions and the University's purpose.

At least once per annum, or in the event of major changes to the organisation or the information systems, an overall risk assessment is conducted by the management in order to keep up to date with the current risk situation.

The management has decided to develop and administer information security strategies that ensure an information security level that at least corresponds to the basic safeguards in DS 484:2005, and also to ensure that KU's strategies are described in the IS handbook.

The operational responsibility for the day-to-day management of the information security work, cf. Appendix 1, is placed with KU's IT security manager, who makes sure that the activities, standards, guidelines, controls and measures, as described in the security handbook, are implemented and complied with.

It is also highly important that information security is integrated into all relevant business procedures, operating tasks and projects.

Security consciousness

Information security has a bearing on the University's overall information flow, and an IS policy cannot be implemented by the management in isolation. All users have a responsibility to contribute to protecting KU's information against unauthorised access, amendment and destruction, as well as theft. All users shall therefore regularly receive the relevant degree of training in information security.

All internal users of KU's information assets shall follow the IS policy and the guidelines derived from it.

Users must only use KU's information assets in the context of their links with the University, and must protect the information in a manner befitting its sensitivity and/or particularly critical nature.

Breaches of information security

If a user discovers threats to or breaches of information security, this must immediately be reported to the line manager for information security or to the management.

Line managers for information security are listed on KU's IS homepage at informationssikkerhed.ku.dk

Users who breach the IS policy or the guidelines derived from it will be subjected to disciplinary procedures in accordance with KU's current rules and personnel policy.

Amended by ISU 18 December 2008. Processed by the Directors' Co-ordination Committee 19 January 2009, by the Management Team 21 January 2009, by the General Collaboration Committee 18 February 2009 and then approved by the Rector.

Appendix 1: Use in practice

The guidelines and security and control measures at the University of Copenhagen are collated in the IS handbook, which is divided up into the same sections and sub-sections as those used in DS 484:2005.

The security handbook contains a description of the information security areas that are relevant to the University of Copenhagen.

The purpose of the operational responsibility is:

- to guarantee that the IS policy and guidelines derived from it are implemented
- to define the value of the information that is necessary for KU, and to take reasonable precautions to protect that information, including earmarking the necessary funding and resources for that purpose
- to identify system and information owners for all information and information systems
- to classify and protect the information for which KU is responsible
- to prevent and limit risks to a level known to and accepted by KU
- to devise rules for information control and protection, which must be followed by the members of staff who process and use the information
- to establish rules for access to and use of information and make sure that these are maintained and, if necessary, revised on a regular basis
- to define the rules for filing information so that it can always be re-created later, within a known and accepted time scale
- to devise a usable plan to re-establish day-to-day operations if the information or the information systems are destroyed for any reason, so that:
 - the scale of and the consequences of the emergency situation can be minimised
 - the most significant elements of everyday KU operations can be resumed via alternative procedures
 - all relevant effected parties are kept informed to the necessary extent
 - the full operation of the information systems can be resumed within a known and accepted time scale
- to guarantee that any sensitive (in terms of safety) information activity can be attributed to the person who has carried out the activity, and to guarantee implementation of the necessary controls for discovering abuse or attempts at misuse
- to establish rules for the conferment of rights and the separation of functions that will prevent and limit the consequences of errors, accidents and negative actions that are consciously performed by individuals
- to guarantee that KU develops and installs systems with due regard to proper safety measures
- to guarantee that KU's suppliers comply with the safety instructions that are valid for KU's own information, facilities and staff, in co-operation with the University
- to take the necessary precautions to guarantee that the IS policy and guidelines derived from it are complied with
- to guarantee the necessary management reporting of IS status, including activities and incidents.