KPMG P/S
ADVISORY
Dampfærgevej 28
2100 København Ø
Denmark

Telephone +45 70 70 77 60
www.kpmg.dk

University of Copenhagen

Security policy

September 2016

KU IS politik 2016 - English version v2

University of Copenhagen
Security policy
ADVISORY
September 2016

Indhold

University of Copenhagen
Security policy
ADVISORY
September 2016

1 Information security policy

This document defines the University of Copenhagen's general policy on information security.

The policy applies to the entire University of Copenhagen (UCPH), both as an authority, an employer and a research institution.

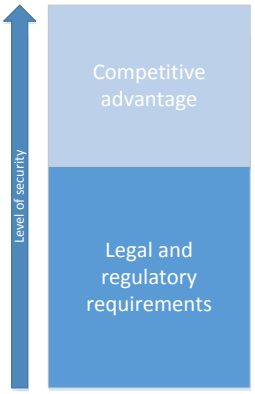
1.1 Why do we wish to protect our information?

First and foremost, we should show basic respect for our own employees and other persons who have entrusted their personal data to UCPH, either directly or indirectly. This trust must not be abused.

Furthermore, it entails a number of consequences for UCPH if information is abused, corrupted or lost, and it is an assessment of these consequences that provides the basis for how strong an information protection we want.

Basically, UCPH must live up to current legislation. This means that a number of security requirements are imposed upon UCPH from outside sources. This is the lower limit for how strong our security must be.

However, if we want UCPH to maintain its status and function as an internationally recognised university and attractive cooperative partner, we must also recognise that information security increasingly is a prerequisite for attracting cooperative partners and research funds and for gaining access to the external information on which we base our research.



At the same time, UCPH has large amounts of information on which we base present and future research; research that is made difficult, impossible or that cannot be documented if information is lost or loses its credibility.

1.2 What does the term "information" cover?

At first, one often associates the word "information" with digital data. But this is only part of it – we also have a wide range of information connected to physical objects. Examples of these are:

— Unique specimens such as for example museum specimens

— Biological material: biobanks, herbariums and living organisms

— Dossiers

— Ice cores and other geological special collections

— Sound, film and pictorial material, possibly of a sensitive nature.

University of Copenhagen
Security policy
ADVISORY
September 2016

In order to secure UCPH's information, we have set out a number of principles for information security, which it is expected that everyone affiliated with UCPH adhere to.

2 Principles

These basic information security principles must be adhered to by everyone:

2.1 Governed by UCPH's strategic requirements

Ownership of policy and guidelines

UCPH's Executive Management has defined the requirement for information security; hereinafter referred to as the desired security level.

It is against this background that the Executive Management has decided on this information security policy and related guidelines, which are maintained by the Information Security Manager and adhered to by everyone at UCPH.

UCPH's requirements

It is UCPH's requirements, including compliance with current legislation and protection against current risks, that determine the security level at UCPH. The purpose is to secure UCPH's ability to maintain its status and function as an internationally recognised university and attractive cooperative partner at the same time as taking a risk level accepted by management into account.

Data classification

All of UCPH's information has value to varying degrees. By classifying the information, one can illustrate the value of each piece of information in a systematic way in order that it can be protected to a necessary and adequate degree, on a uniform basis.

Risk management and assessment

UCPH's informations security is based on risk assessments of specific systems, projects, controls and vulnerabilities.

Information management and processing are to a large extent performed locally, and ongoing risk assessments are consequently a necessary prerequisite for maintaining an overall picture of the information security.

2.2 Implementation of security measures

Security environment

The security environment is the general term for all the measures that protect UCPH's information. Hence it is all the technical and organisational security measures – both centrally and locally – that together must ensure that the security level is maintained.

Because UCPH is a living organisation with work processes and requirements that are constantly changing, it is important to assess risks from time to time in order that the security environment can be adjusted.

2.3 Deviations are documented

Compensatory measures

If a need for information processing arises that cannot be adequately protected by the existing security environment, this results in an increased risk. This risk must be reduced through further measures, called compensatory measures.

Adherence to UCPH's requirement for security

Deviations from the security environment can be approved provided that UCPH's requirement for security is fulfilled partly through compensatory measures and partly through a management acceptance of the remaining risk.

Exemptions

An exemption documents that a specific deviation from the security environment has been accepted and approved. Exemptions are granted based on risk assessments and can require compensatory measures. Exemptions are always temporary.

Circumvention of the security environment

Intended or unintended disregard of the security environment is addressed as security incidents, irrespective of the intentions. The incidents are documented, and ongoing reporting and follow-up must be carried out in order that UCPH's requirement for security is maintained.

2.4 Joint responsibility

Everyone at UCPH has a responsibility

It is understood that everyone at UCPH acts professionally and use their common sense. We at UCPH strive to create a security environment that is transparent and gives us all the possibility to act responsibly in our daily work.

Show awareness and react in case of deviations

At UCPH, you are not only responsible for your own actions; if you become aware that the security level is reduced, it is your responsibility to react and draw attention to the problem.

Responsibility and acceptance

In connection with your access to UCPH's information comes a responsibility. It is important that you relate to – and accept – this responsibility.

Furthermore, as a manager you must ensure that your employees have understood and accepted the responsibility that they are given upon granting of access. This includes access granted to external consultants.

2.5 Work-related need

Granting and administration of access

Access to information at UCPH is based on a documented work-related need that is approved both by the immediate manager and by the entity that owns the information. A work-related need documents the necessary and adequate rights to be granted. The immediate manager must ensure from time to time that the access reflects the current need.

Separation of duty

At UCPH, separation of duty means that you cannot approve or keep secret your own actions. It is a proactive measure against fraud and deception, which at the same time protects you against unwarranted suspicion. In UCPH's security environment, separation of duty is maintained to the extent that it is justified by business needs.

2.6 Digital identity

Digital identity at UCPH

UCPH's IT systems identify you by means of your digital identity and makes your actions personally attributable. Your work-related needs are reflected in the rights that are granted to your digital identity. If another person uses your digital identity, the actions will be carried out in your name. Consequently, a digital identity is personal and must not be transferred or used by others.

2.7 Traceability

Documented history

At UCPH, traceability means knowledge about who carried out a given action and when. This provides the basis for investigation of historical actions to remove unwarranted suspicion and uncover whether irregularities have arisen as a consequence of errors/mistakes or misuse. At the same time, traceability is a prerequisite for necessary periodic follow-up and control.

2.8 Outside of UCPH

The security level applies to everyone

Everyone who processes information for UCPH must adhere to the business's demands when it comes to security. If information is processed outside of UCPH's security environment, for example at an external cooperative partner, this partner must be informed of and adhere to the same demands as are made internally at UCPH.

This also applies when you as an employee transports or uses information outside of UCPH, both logically and physically.

3 Organisation and reporting

At strategic level, UCPH's direction is set out by the Executive Management, i.e. it is defined what UCPH's requirements for information security are.

This is translated by the Information Security Group into general guidelines for how the security requirement can be fulfilled.

Everyone who operates a system which is used to store or process information has to design and implement the solution in such a way that it lives up to the guidelines.

It is also a requirement that as part of the solution it is designed how one can control that the solution lives up to the guidelines.

Finally, a solution requirement is frequent reporting on to what extent the guidelines are adhered to.

The Information Security Group is charged with collecting the reporting, maintaining an overall overview and carrying out periodic management reporting.

The management reporting enables the management to act and prioritise in relation to challenges across the entire UCPH.