Appendix 1
Guidelines on Information Security

Guiding Principles and Rules on Information Security at Karolinska Institutet

Ref 1-516/2013

Version 2.0
Applicable from 01-10-2013

Karolinska Institutet

Appendix 1
Guidelines on information security

Other Appendices

Appendix 2. Description of responsibilities

2.1 University Director
2.2 Chief Security Officer
2.3 Head of Department
2.4 Persons responsible for information
2.5 IT Director
2.6 System Owners

Appendix 3. Instructions

3.1 Conducting risk analyses
3.2 Information classification model – under revision
3.3 Handling of personal data
3.4 Defining requirements for operations outside KI
3.5 Handling information connected with recruitment, employment and termination of employment
3.6 Defining requirements for communication and network security
3.7 Defining requirements for reliability and service level
3.8 Administration of access rights
3.9 Reviewing access rights
3.10 Logging and examining logs
3.11 Defining requirements when acquiring or developing systems
3.12 Defining requirements for system administration
3.13 Handling and reporting of information security incidents
3.14 Continuity planning
3.15 Handling requirements – under revision

Revision log

Version no	Date	Responsible	Changes made compared to previous version
1.0	2013-04-01		
2.0	2013-10-01	Annika Sjöborg	Changed structure of document – split into three parts, more information on how to use the document and some clarifications.

Informationsklass: K1R2T1

Guidelines on information security

(also available in ppt format)

Information security – 6 things to bear in mind!

1. Protect your login details and never pass them on
2. Lock or log out from your computer when you leave it
3. Never send sensitive information by e-mail
4. Do not download files or open attachments in e-mails if you are not sure what they contain
5. Bear in mind the environment you are in when you are handling and speaking about sensitive information
6. Make sure your information is backed up, regardless of what media it is stored on. Contact your local IT-support for advice.

About Information Security

All those who have an active role, i.e. employees, students, contractors/associates and consultants, are responsible for being aware of and observing the current rules on information security within Karolinska Institutet (KI).
The purpose of this document is to provide a description of the information security requirements that those with an active role within KI must be aware of in order to contribute to protecting the organisation's sensitive information.
There is more detailed information in KI's rules on information security and in its appendices.

Handling sensitive information*

When handling sensitive information, you must bear in mind that:

- you only may access sensitive information that is necessary for you to be able to perform your work.
- your access rights are personal and may never be shared with anyone else. You are personally responsible for the activities performed via your login.
- sensitive information on paper must be locked away when not in use
- sensitive information may only be sent in encrypted form when it is sent by e-mail
- sensitive information must never be discussed in a public place or where there is a risk that unauthorised persons may gain access to the information. This also applies for calls made by phone or by mobile phone.

* Information that is considered, or that may become considered, confidentialor iInformation that, for other reasons, should not be spread to unauthorised persons.

IT hardware and portable media

When handling IT hardware and portable media, you must bear in mind that:

- KI's hardware is to be used for work-related purposes
- only hardware that is configured in accordance with the defined standard may be connected to the network
- information always should be saved in designated places (document management system, network disks, etc.), and not on the local hard drive on your computer
- information on computers, mobile phones and on paper must be protected physically, i.e. such items must not be left unattended
- mobile phones and tablets must always be protected against unauthorised access by the use of a PIN code or equivalent
- sensitive information must be encrypted if it is stored on portable IT media

Use of the Internet

The Internet connection is to be used for work-related tasks. Private use is only permitted to a limited extent and as long as it does not affect your work.
It is not permitted to:

- visit websites that contain violence, racism, pornography, criminal activity or other sites that for ethical reasons are judged not to be appropriate*
- download files or programs that are not work-related (incl. copyright material such as movies or music)
- connect a computer to the network while it is simultaneously connected to another network

* Exceptions to this rule may be granted if the work/research requires this. These exceptions must be approved by the immediate manager.

Use of email

The email system is primarily for work-related tasks. Private use is only permitted to a limited extent as long as your work is not affected.

- Sensitive information must always be encrypted when it is sent by email.
- Email accounts may be closed if there is any suspicion of criminal activity or abuse
- Your email address shall only be used in work-related contexts

- It is not permitted to:
  - send or save offensive information such as violence, pornography and discriminatory words or images*
  - send or forward spam or chain mail
  - open, send or forward program files that are not work related
  - automatically forward email to an external, unapproved email address
  - use a private/external email address as contact information on KI's public websites

* Exceptions to this rule may be granted if the work/research requires this. These exceptions must be approved by the immediate manager.

Use of social media*

The use of social media within KI must primarily take place on the basis of the organisation's interests, e.g. to quickly reach various target groups.
You shall also bear in mind that:

- private use of social media during working hours is only permitted to a limited extent, and that KI's email address may not be used for login/communication
- sensitive information must never be communicated through social media
- passwords that are used to log into social media must not be the same as passwords used in KI's internal network

Otherwise, the same rules apply as for the use of email.
For further information on dealing with social media, see
http://internwebben.ki.se/sv/vanliga-fragor-om-sociala-medier

* Social media are interactive communication services on the Internet, such as blogs, Facebook, wikis and comments on articles.

Telecommuting When telecommuting, you must bear in mind that:

- remote connections to KI's network only are permitted through approved communication solutions for remote connection
- only hardware that satisfies KI's security requirements may be connected to KI's internal network (does not apply to access to online web services, e.g. Contempus)
- sensitive information must be stored and handled in a secure way in accordance with current security requirements
- sensitive information always must be encrypted when stored on movable media such as laptops, USB sticks or mobile phones

Access and user ID

With regard to your access and user ID, you must bear in mind that:

- as a user, you are responsible for the handling of information and the activities that take place during the period when you are logged in with your user ID in a system
- your user IDs, passwords and badges are personal and may never be lent to anyone else
- you must immediately submit a report if you suspect that anyone elseis aware of your password or if you have lost your badge.

Logging and examining logs

With regard to logging and examining logs, the following applies:

- all use of the Internet is logged
- for all systems that contain sensitive data, logging takes place of all user activities, i.e. everything we do in the system
- the purpose of the logging is to make it possible to make sure that only authorised persons have had access to certain information
- logs are examined on a regular basis

Incident reporting

Incident reporting is an important element of KI's work with information security. As a user, you must help by:

- as soon as possible report incidents that might affect the information security
- report incidents to the Head of Department or to a person designated by him/her
- also report any suspicions of incidents

Examples of information security incidents are:

- malware (e.g. virus) or malicious software
- information that has fallen into the wrong hands or is being handled incorrectly
- theft of hardware containing information
- hacking or data breach

We all have a responsibility!

In order to maintain a sufficient level of protection for information and the system environment, we must work together and continuously. Adopted security rules must be applied and observed by all those with an active role within KI, i.e. all employees, students, contractors/associates and consultants in the organisation.

Information security is based primarily on common sense and good judgement, in which your knowledge and your actions are decisive. All in all, these are important preconditions that contribute to maintaining confidence in our organisation and guaranteeing the information that we are handling.

Any breach of current security rules can result in loss of access rights to KI's IT systems. This may be decided by the Head of Department in consultation with the Chief Security Officer. More serious cases of abuse or other similar breaches of rules are reported to the Chief Security Officer for further processing. Any suspicions of criminal activity are reported to the police.