Guidelines on Informations Security

2013-10-01

Ref. 1-516/2013

Version 2.0

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. Avoid sending sensitive information by email. If you do, it has to be encrypted!
4. Do not download files or open attachments in emails 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 that your information is backed up, regardless what type of media it is stored on. Contact your local IT support for advice.

About Information Security

- Anyone who has an active role, i.e. employees, students, contractors/associates and consultants, are responsible for being familiar with 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 everybody within KI must be aware of in order to contribute to protecting the organisation's sensitive information.

- There is more detailed information for certain functions/responsible persons 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 may only access sensitive information that you need in order 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 details.
- sensitive information on paper must be locked away when not in use
- sensitive information may only be sent in encrypted form if sent by email
- 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 mobile phone.

IT hardware and protable 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 KI defined standard may be connected to the network
- information saved on the local hard drive on your computer or portable media must always be backed up. When possible, data should be saved in designated places (document management system, network disks, etc.)
- information on computers, mobile phones and on paper must be protected, i.e. such items must not be left unattended
- mobile phones and PDAs 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 provided by KI 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. music or movies)
- 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 for work-related tasks. Private use is only permitted to a limited extent and as long as it does not affect your work.

- Sensitive information must always be encrypted when it is sent by email
- KI email accounts may be closed if there is any suspicion of crime or abuse
- Your email address should only be used in work-related context
- 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
  - → quote 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 is primarily based on the interests of the organisation, e.g. to quickly reach various target groups.

You should also bear in mind that:

- private use of social media during work hours is only permitted to a limited extent, and as long as it does not affect your work.
- KI's email address may not be used for private 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

Telecommuting

When telecommuting, you must bear in mind that:

- remote connections to KI's network are only 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 affect access to online services, e.g. Contempus)
- sensitive information must be stored and handled in a secure way in accordance with current security requirements
- sensitive information must always be encrypted when stored on movable media such as laptops, USB sticks or mobile phones

Access and user ID

Regarding 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 an unauthorised party is aware of your password or if you have lost your badge.

Loggning 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 management

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

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

Examples of information security incidents are:

- incorrect, unauthorized or harmful handling of information, which may cause damage to KI
- information that has fallen into wrong hands
- theft of hardware containing information
- hacking
- malware (e.g. virus) or malicious software

We all have a responsibility!

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

- Information security is primarily based 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 a 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/the IT Director. More serious cases of abuse or other similar breaches of rules should be reported to the Chief Security Officer for further processing. Any suspicions of criminal activity will be reported to the police.