Guidelines for information security at KI

These guidelines will describe the rules and requirements that you, as an affiliate at KI, are responsible to comply with. In order to contribute to KI information security, you'll need to be aware of, and to comply, with this. More detailed information and guidelines can be found in KI's information security management system

Handling of sensitive information

Handling of 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
- Sensitive information on paper must be locked away when not in use, as with unlocked computers, the easiest way for an authorized person to get information from KI is through physical access
- 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 unauthorized persons may gain access to the information. This also applies to phone calls.
- Sensitive information may only be stored and handled in IT-systems that has been approved for the purpose of handling sensitive information.

Processing of personal data

Personal data shall be processed in accordance with, at the time, applicable data protection rules. For an example, GDPR, and the ethical review act for research. When processing personal data, bear in mind that:

- The processing must have a purpose and be based on one of the bases for lawful processing in GDPR.
- Every processing activity regarding personal data must be reported to KI's central record over processing activities. To report, and for instruction on how to report, go to KI's GDPR page.
- Personal data may only be processed in IT-systems that has been approved for the purpose of handling personal data.
- Sensitive data, or data that can impact the personal integrity of a person, shall be processed in accordance with the specific rules on how to handle sensitive personal data

All processing activities must also comply with the principles of processing personal data and KI's guidelines on how to process personal data. For more information, see KI's GDPR page.

Hardware and portable media

When handling 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 security standards may be connected to the network. This includes updated antivirus, firewall and protection against unauthorized access. Sensitive information and sensitive personal data shall not be stored and processed on private devices.
- 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
- Laptops must be protected with a password that meets KI's rules for passwords and mobile phones and tablets the use of biometric authentication (such as fingerprint recognition), PIN code or equivalent

Mobile devices

Information on mobile devices shall be protected from unauthorized access, manipulation and loss. A work phone that is connected to KI's intranet can be used as a stepping stone into our IT-environment and for attacks. Bear in mind that:

- Smartphones and tablets that provided by KI is to be seen as a work tool. These devices, and the information stored on them, is property of KI and KI thereby have the right to access this information.
- Because of the Public access and secrecy act information on mobile devices could, on demand, be disclosed to the public.
- Mobile devices are to be seen as insecure storage locations. Therefore, you shall not store confidential or sensitive information on these if you don't use

security features for these purposes that have been approved by the IT department.
- Applications for mobile devices could contain malicious code. To reduce the risk of getting infected you shall only download applications from known provides, such as App Store or Google Play.
- PIN codes, fingerprints or equivalent protection against unauthorized access must be used on mobile devices. When using PIN codes these shall not be easy to guess, such as 0000, 123 etc.
- Updates from Google or the phone manufacturer must be downloaded promptly.
- Mobile devices shall have features to remote wiping and tracing activated.

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.

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. Contact KI's IT department for help with encryption.
- Email accounts may be locked if there is any suspicion of crime or abuse
- Your email address should 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
- quote a private/external email address as contact information on KI's public websites

Use of social media

The use of social media within KI is primarily based on the organization's interests, 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/en/social-media-faqs.

Teleworking

When teleworking, 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 manner 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.

Logging and audit of 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

Report information security incidents

At KI you shall know what an information security incident is, and how to report these. You shall:

- As soon as possible report incidents that could have an impact on the information security
- As soon as possible report incidents regarding personal data
- Report these incidents in accordance with KI's process for reporting incidents, for now through an email to it-support@ki.se for further analyzes and management.
- You shall also report suspicions of incident.

Example of incidents:

- Incorrect, illegal or harmful handling of information that may have a negative impact on KI
- Information that has come into the wrong hands i.e. unauthorized access to information
- Theft of equipment or physical documents containing sensitive information
- Hacking
- Malicious code (e.g. virus) or malware

To report an incident, send an email to it-support@ki.se.

We all have a responsability!

To maintain an adequate level protection for our information and IT-systems we must work together and continuously. You'll need to comply to our security rules whether you're an employee, student, affialites or a consultant at KI.

Violations of these rules may result in loss of access rights to KI's IT systems. This can be done by a decision of the Head of department in consultation with the Chief Security Offices (CSO). More serious cases of abuse or other similar breaches are reported to the CSO for further processing. Suspicions of criminal activity will be reported to the police.

Karolinska Institutet