Appendix 2
Description of responsibilities

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 2
Description of responsibilities

Content

Other Appendices

Appendix 1. Guidelines on information security

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.

2.1 University Director

By delegation from the Vice-Chancellor, the University Director has ultimate responsibility for KI's organisation in administrative, legal and financial respects. Described below are the areas of responsibility for KI's University Director in respect of information security:

- Is responsible for information security at an organisational level and is ultimately responsible for ensuring that there are current, communicated guidelines, rules and instructions in respect of the work with information security within KI.
- Is responsible for organisation-wide work with information security, including work in the areas of continuity planning, risk management and incident management.
- Is responsible for reporting, on an annual basis, to the consistory on KI's work with information security.

2.2 Chief Security Officer

Described below are the areas of responsibility for KI's Chief Security Officer in respect of information security:

- Is responsible for coordinating organisation-wide work with information security, including work in the areas of continuity planning, risk management and incident management.
- Is responsible for making sure that the general work with information security is carried out as effectively and appropriately as possible.
- Is responsible for drawing up general action plans and for planning and coordinating work with information security at KI in accordance with the overall information security process.
- Is responsible for managing KI's management system for information security and for making sure that associated rules and instructions are at all times current, updated and communicated.
- Is responsible for defining requirements for the organisation in respect of information security. For example, overall IT security and physical security.
- Is responsible for reporting the following to KI's University Director on an annual basis:
  - Results of reviews of protective measures carried out in accordance with KI's rules and instructions.
  - Risk analyses carried out in respect of information security within KI.
  - Improvement measures carried out in respect of information security.
  - Summary and analysis of information security incidents that has occurred during the year.
  - Compliance with guidelines, rules and instructions on information security.
- Is responsible for representing KI in relation to other authorities and organisations on issues relating to information security.

2.3 Head of Department

As part of the responsibility for operational activities within each department, as defined in the Vice-Chancellor's delegation to Heads of Department within KI, responsibility for information security is included in each Head of Department's area of responsibility as follows:

- Is overall responsible for information security within the department and for regularly following up and reporting compliance with information security requirements within the department to KI's Chief Security Officer.
- Is responsible for the information generated by his/her own department. For further information on areas of responsibility connected to the role of those responsible for certain information, see *Description of responsibilities: Responsible for information.*
- Is responsible for ensuring that all information assets within the department have designated persons responsible for information and that the assets have been classified. For more information, see *KI's information classification model*.
- Is responsible for ensuring that time and resources are made available for work with information security within the department.
- Is responsible for ensuring that department-wide risk analyses are conducted on a regular basis. For further information, see *Instructions on conducting risk analyses*.
- Is responsible for ensuring that continuity planning takes place and is coordinated at a departmental level. For more information see *Instructions on continuity planning*.
- Is responsible for making sure that all with an active role within the department are given sufficient training in information security and that they observe defined information security rules.
- Is responsible for ensuring that activities are carried out to make sure that those with an active role have correct access rights in relation to their role/work. This is done by observing current instructions on the granting of access rights and by actively participating in regular reviews of access rights. For further information, see *Instructions on administration of access rights* and *Instructions on reviewing access rights*.
- Is responsible for observing information security in connection with recruitment, employment and termination of employment. For further information, see *Instructions on handling information in connection with recruitment, employment and termination of employment.*
- Is responsible for receiving and initially dealing with information security incidents classified as Classes 1 and 2. For further information, see *Instructions on the handling and reporting of information security incidents*.

2.4 Persons responsible for information

Within Karolinska Institutet there are designated persons responsible for certain information, who are responsible for the following:

- That information is classified in accordance with KI's information classification model. For more information, see *KI's information classification model*.
- That risk analyses in respect of the specific information and associated information assets are conducted on a regular basis. For further information, see *Instructions on conducting risk analyses*.
- That access rights to the specific information and associated information assets are correct, that regular reviews of access rights are conducted and that any necessary action is taken as a consequence of the results of the reviews (for example that people who no longer need access to the information in a particular system are deleted, etc.). This work must be carried out in collaboration with the System Owners of the systems that handle and provide the information in question. For further information, see *Instructions on administration of access rights* and *Instructions on reviewing access rights*.
- That logging and follow-up on logs of user activities connected with the information are carried out to an appropriate extent. This work must be carried out in collaboration with the System Owners of the systems that handle and provide the information. For more information see *Instructions on logging and examining logs*.
- To define requirements for relevant System Owners, i.e. for all systems where information is handled, in respect of the choice of protective measures for the information in question.
- That personal data are handled in accordance with the Swedish Personal Data Act, which means, for example, that the handling of personal data must be reported to KI's Personal Data Representative.
- That verification is performed, in accordance with both current legislation (the Swedish Public Access to Information and Secrecy Act 2009:400) and KI's information classification model, in respect of whether or not information may be released. The result of this verification must be documented and archived.
- To define requirements in terms of how information that is issued to another party outside KI is to be handled.
- To decide on how information is to be handled and stored, in both digital and physical form, if it deviates from KI's information classification model. If a person responsible for information decides that the information may be handled in a way that deviates from KI's information classification model, this decision must be documented and archived. For decisions relating to handling or storage outside KI, a documented risk analysis must be conducted first, see *Instructions on conducting risk analyses.*

2.5 IT Director

Described below are the areas of responsibility for KI's IT Director in the area of information security:

- Is responsible for guaranteeing compliance in respect of the information security requirements defined for the IT systems, environments and components for which the IT Department is responsible.
- Is responsible for drawing up detailed instructions for IT activities based on KI's rules and instructions in respect of information security. These instructions must be kept up to date and be observed.
- Is responsible for KI's IT infrastructure and its security. For further information, see *Instructions on defining requirements for communication and network security*.
- Is responsible for and coordinating general work on IT security within KI.
- Is responsible for making sure that IT personnel (internal and external) observe the current rules on information security.
- Is responsible for making sure that IT personnel receive the necessary training in respect of information security.
- Is responsible for making sure that suppliers hired in the IT field satisfy KI's requirements for information security.
- Is responsible for making decisions, in collaboration with the relevant System Owners of central systems, on the allocation of personal administrator rights. For further information see *Instructions on administration of access rights*.

2.6 System Owners

Described below are the areas of responsibility for KI's System Owners in respect of information security:

- Is responsible for general information security in respect of the specific system.
- Is responsible for defining requirements in respect of the system's reliability. For further information, see *Instructions on defining requirements for reliability and service level*.
- Is responsible for ensuring that risk analyses of the system are conducted on a regular basis. For further information, see *Instructions on conducting risk analyses*.
- Is responsible for defining and following up on the system's protective measures and for making sure that they are in accordance with the requirements in respect of information security.
- Is responsible for setting up collaboration with persons responsible for information in respect of the information assets that are handled in the system.
- Is responsible for appointing a system administrator and for defining requirements for him/her in respect of work on information security. For further information, see *Instructions on defining requirements for system administration*.

- Is responsible for making sure that requirements in respect of system development and system modification are observed. For further information, see *Instructions on defining requirements when acquiring or developing systems* and *Instructions on defining requirements for reliability*.
- Is responsible for defining requirements for information security and protective measures when systems are operated outside KI's organisation. For further information, see *Instructions on defining requirements for operations outside KI*.
- Is responsible for ensuring that there are defined instructions and an organisation for the administration of access rights to the system and that these are used. For further information see *Instructions on administration of access rights*.
- Is responsible for ensuring that regular reviews of access rights to the system are conducted, and that there are instructions describing how these reviews are to be conducted. For further information, see *Instructions on reviewing access rights*.
- Is responsible for collaborating with the IT Manager to decide on and to grant personal administrator rights for central systems. For further information see *Instructions on administration of access rights*.
- Is responsible for ensuring that the logging function works in the system in accordance with the requirements defined by the relevant person responsible for the information in the system in question. Is also responsible for ensuring that there are system-specific instructions for examining logs of user activities in the system, and that regular examinations of logs are conducted in accordance with the requirements defined by the person responsible for the information. For more information see *Instructions on logging and examining logs*.