Appendix 3
Instructions

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 3
Instructions

Content

Other Appendices

Appendix 1. Guidelines on information security

Appendix 2. Description of responsibilities

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.

3.1 Conducting risk analyses

In accordance with the *Rules and regulations on internal management and control* at KI, ref. 1795/2009-010, risk analyses must be conducted on a regular basis at various levels and in various areas within Karolinska Institutet's organisation. There are various methods and models for conducting risk analyses. Within KI there is an adopted risk analysis method, which should be used if possible. As an alternative method, the Swedish Civil Contingencies Agency's (MSB's) "*Risk analysis*[1]*"* may be used. Whichever method is used, the following activities must always be carried out when conducting a risk analysis:

1. **The scope and delimitation of the analysis must be defined**
   The scope of the risk analysis to be conducted is specified by defining and delaminating the area or the process to be analysed. The risk analysis method must be chosen and people with good knowledge of the relevant area/process must be identified and invited to take part in the analysis. These people must also be given the opportunity to prepare and obtain the necessary information/facts to enable them to perform the task in an effective, appropriate way.

2. **Threats must be identified**
   For each sub-area or stage in the process to be analysed, the threats that exist must be identified, grouped and documented. The threats must be documented to a sufficient level of detail so that even an external party can understand what is meant.

3. **Consequences and probability must be assessed**
   The consequences of identified threats being realised, and the probability that they will be realised, must be identified and analysed, and the results documented. The scope of the risk, i.e. the consequence and probability of a threat being realised, should be assessed on the basis of a defined method that also makes it possible to compare risks and their scope.

4. **Suggested action must be drawn up**
   There may be a number of different causes behind each risk identified, and suggestions on how to deal with these must therefore be drawn up. The consequences of the suggestions must be analysed before any decision is made on action. Action may be taken, for example, to prevent or reduce the probability of the underlying causes occurring, or the consequences of their occurring being minimised.

5. **The risk analysis must be documented**
   A report must be compiled on the basis of the completed risk analysis. The report should contain, in addition to the actual result of the analysis and the description of the risks identified, information about all of the implementation stages in the risk analysis. The report should also contain any possible suggested action and recommendations to the person who is to make a decision on the matter. These suggestions will form the basis of planning on-going work on managing the risk.

6. **An action plan must be produced and followed up**

[1] See the MSB's Information Security Framework, http://www.informationssäkerhet.se/Ramverket/, which contains explanations, methods and templates.

A prioritised action plan, specifying which measures are to be taken, who is responsible for them and by when they are to be completed, must be produced and followed up. If there are risks that the organisation considers do not require action, this acceptance of remaining risks must also be documented.

3.2 Karolinska Institutet's (KI's) information classification model – Under revision

All information within KI must be classified on the basis of the following aspects:

- **Confidentiality** – that information is not made available or revealed to unauthorised persons.
- **Integrity** – guaranteeing reliability and completeness in respect of information.
- **Availability** – that information is accessible at the request of an authorised person.

The combination of the different classes (Cx, Ix, Ax) must be specified in the designated place in electronic and paper documents where the information is contained, and it must be clear from system documentation or equivalent which information class(es) each system handles.
When a document arrives or is created at Karolinska Institutet, it must thus be given information classification. Despite the principles of information classification set out below, KI must always hear a request for omission in an individual case. The following principles for classifying information never take priority over the individual review under the Swedish Public Access to Information and Secrecy Act, but classification may need to be abandoned in individual cases.
Certain information may also be of such a nature that it moves between the different classes over time (e.g. research information may have a high confidentiality class before it has been formally published, but once it has been published it has low confidentiality class), and it must therefore be ensured that information is ranked correctly at any given time. The person responsible for the information is responsible for ensuring that this is done.

Information class	Confidentiality	Integrity	Availability
4. Serious a) causes a serious restriction in KI's ability to perform its undertaking to an extent and for a period that means that the organisation is unable to perform one or more of its primary tasks; b) results in extensive damage to the organisation's or another party's assets; c) results in major financial losses for KI or another party, or d) has a seriously negative impact on an individual person's rights, life or health.	An information asset that contains sensitive information that may cause **serious damage** if it falls into the wrong hands. Generally applicable to: 1. An information asset that is or may become the subject of confidentiality under the Swedish Public Access to Information and Secrecy Act (e.g. information about individual people's illnesses or abuse, on-going cases involving the expulsion of students from higher education). 2. An information asset that may be the subject of an application requirement under special legislation (e.g. patient data, details of illness together with personal ID no.). 3. An information asset that constitute the organisation's own or another organisation's business secrets (e.g. crude research data relating to an individual person, unpublished research data, passwords, IT security settings). 4. An information asset that is not a public document and that may contain information that is sensitive for an individual or individual company/organisation (e.g.	Information that, if it is not correct and complete, can cause **serious damage**. Generally applicable to: 1. An information asset with particularly high requirements for correctness (e.g. personal data and metadata such as research data). 2. IT systems or information assets for critical processes in the organisation (e.g. ……).	IT system or information asset that is a part of or supports continuous activity in which disruption may cause **serious damage.** Generally applicable to: 1. IT systems or information assets that are extremely critical for the organisation (e.g. ……).

	research information from people in the criminal register). 5. Information about animal experiments with a considerable level of severity for the animals. 6. Information that identifies persons who handle animals used in animal experiments. 7. Information about the physical storage of animals used in experiments (e.g. building plans, information about animal transport).		
Information class	Confidentiality	Integrity	Availability
3. Significant a) causes a significant reduction in the ability to perform KI's operational undertaking to an extent and for a period that there is a tangible reduction in the effective performance of the organisation's primary undertaking; b) results in significant damage to the organisation's or another party's assets; c) results in significant financial losses for KI or another party, or d) has a significant negative impact on an individual person's rights or health.	An information asset that contains sensitive information that may cause **significant damage** if it falls into the wrong hands. Generally applicable to: 1. Information that must always be subject to a confidentiality test before being issued (e.g. diagnoses of illnesses of deceased persons identified via serial number, working documents from other authorities). 2. Personal data in general or that is considered sensitive under the Swedish Personal Data Act (e.g. where details of illness are specified but identification is via serial number rather than personal ID no., individual student matters relating to personal problems). 3. Data of an internal nature, with no other restrictions, to which only in-house personnel should have access (e.g. descriptions of methods in respect of research, information that identifies the manipulation of crude data, i.e. research fraud, information about sensitive meetings such as recruitments and donors, working documents and notes containing sensitive data).	Information that, if it is not correct and complete, can cause **significant damage**. Generally applicable to: 1. An information asset that is covered by legislation in which a requirement for correctness is specified (e.g. the Swedish Personal Data Act or special legislation). 2. IT system or information asset that is part of an authority exercise (e.g. system that stores certificates....). 3. Information or IT system in which there is a requirement for traceability or non-repudiation.	IT system or information asset that is a part of or supports continuous activity in which disruption may cause **significant damage.** Generally applicable to: 1. IT system or information asset that is a part of or provides support for an authority exercise and/or core activity. 2. E-services for the public or other stakeholders.
Information class	Confidentiality	Integrity	Availability
2. Moderate a) causes a reduction in the ability to perform KI's operational undertaking to an extent and for a period that there is a clear reduction in the effective performance of the organisation's primary undertaking; b) results in minor damage to the organisation's or another party's assets; c) results in minor financial losses for KI or another party, or d) has a limited negative impact on	An information asset that contains sensitive information that may cause **moderate damage** if it falls into the wrong hands. Generally applicable to: 1. Information received from other parties (e.g. job applications). 2. Unidentifiable patient data, crude data from clinical trials (not traceable to an individual) and source code. 3. Information asset that does not constitute a public document and only contains general information (e.g. work material that does not contain any sensitive information or any information that may otherwise be traced to an individual company, product or person).	Information that, if it is not correct and complete, can cause **moderate damage**.	IT system or information asset where organisational dependence is relatively low and where disruption may cause **moderate damage**.

an individual person's rights or health.	4. Information governed by organisation-specific legislation. 5. Information of an internal nature that, with no other restrictions, only in-house personnel should be able to access (e.g. research plans, strategic plans for the organisation, controlling documents, evaluations and assessments of personnel and students, memos and communication plans). 6. Information on which kinds of animals KI uses in animal experiments.		
Information class	Confidentiality	Integrity	Availability
1. None/negligible	An information asset that only contains information that is publicly available data or information that, if it comes into the possession of unauthorised persons, causes **no damage**. Information that is intended for or can be distributed to an indeterminate group of recipients without any risk of negative consequences. Generally applicable to, for example: 1. Completed internal guidelines, process descriptions, instructions, course material and results of exams, manuals and rules of procedure, etc. that do not contain data that may be subject to confidentiality under the Swedish Public Access to Information and Secrecy Act. 2. Completed, published research reports, public presentations, external newsletters and other communication material. 3. Metadata. 4. Successful applications for funding, ethical permits and associated research applications. 5. Personal data relating to employees and associated persons. 6. Information about finance, equipment, technology, chemicals, etc. used within KI.	Information that, if it is not correct and complete, can only cause **little or no damage**.	IT system or information asset where organisational dependence is low and where disruption may only cause **little or no damage.**

3.3 Handling of personal data

The handling of personal data within Karolinska Institutet (KI) is regulated by the Swedish Personal Data Act (1998:204) and the Swedish Act (2003:460) concerning the ethical review of research involving humans. Personal data must always be handled in accordance with current legislation, and these instructions provide support in defining the minimum level of protective measures for personal data that must be observed within KI.

Personal data

Personal data may only be collected and processed for special, expressly defined and justified purposes, and they may not be stored for longer than is necessary. The basic principle is that personal data may only be processed if the person registered, i.e. the person to whom personal data relate, has given consent to such processing or if it is required in order for KI to be able to perform its legal obligations. Sensitive personal data, for example information about health or sex life, and information about infringements of the law, may only be processed if this has been approved in accordance with the Swedish Act (2003:460) concerning the ethical review of research involving humans. Before any form of processing of the personal data described above takes place, it must therefore be guaranteed that the relevant consents and approvals have been obtained. Approvals and consents must be saved for at least as long as the processing of personal data in question continues and in accordance with current legislation on archiving.

Information to the registered person

In connection with the collection of personal data, the registered person must receive: information about the data processing (reason and purpose), which person(s) shall receive the personal data, KI's obligation to provide information to the registered person about the data processing, how the registered person may apply for information about the data processing from KI and how the registered person can apply for the correction of any incorrect data. As KI is obliged, once a calendar year and free of charge, to provide notification of personal data relating to the person applying to find out about these data, all processing of personal data must be managed and stored in such a way as to enable KI to provide information within one month of the application on: which data on the applicant are being processed, from where these data have been obtained, the purpose of the data processing and to which recipients the data have been issued. Notification of the processing of personal data for an individual person may only be issued in response to a written, undersigned application from the person in question and on the condition that the issuing of the data is not in breach of the Swedish Public Access to Information and Secrecy Act (2009:400). This information may only be sent to the applicant's address as contained in the Civil Register.

Issuing of personal data

In order to process requests for information by registered persons, authorities and other bodies, there must be instructions for processing the issuing of personal data. These instructions must specify who is entitled to make a decision to issue data. Before data are issued, there must always be a review in accordance with the Swedish Public Access to Information and Secrecy Act (2009:400). If it is considered that data can be issued, this must be done on detachable electronic storage media, which includes portable hard disks, USB sticks, CDs, etc. The information must, however, be encrypted and handled in a secure way in order to prevent unauthorised persons from accessing it. The person issuing the information must always make sure that the right person is receiving the information.

Storage of personal data
Sensitive personal data that are stored on laptops and on detachable storage media must be encrypted and handled in such a way that unauthorised persons cannot access the data.

Preservation, excision and destruction of personal data
Personal data must be preserved, excised and destroyed in accordance with current legislation, and there must be documented instructions on how this is to be handled within KI.

Unauthorised access to personal data
There must be procedures and instructions describing how to deal with any suspicion of unauthorised access to personal data. These instructions must as a minimum include a procedure describing how the matter is to be dealt with and if necessary forwarded to more senior bodies (e.g. if the police have to be notified).

3.4 Defining requirements for operations outside KI
When Karolinska Institutet KI buys services or outsources the operation of IT systems outside KI, the same rules on information security must apply as when operation is carried out under its own auspices. In addition to this, the following rules must also apply when operation takes place outside KI:

- Information security requirements must be defined on the basis of a risk analysis and regulated in an agreement between the parties. The System Owner is responsible for defining requirements in respect of the specific system, but coordination should take place when several systems are operated by the same supplier.
- When system acquisition, development or maintenance is included in the external party's undertaking, the security requirements in *Instructions on defining requirements when acquiring or developing systems* must be observed.
- There must be regular follow-up on agreed security requirements. This must be achieved by specifying in the agreement that KI has the right to conduct an audit and an examination of the service provided and of how well the supplier is fulfilling current and relevant information security requirements.
- If the information in the systems contains personal data, the roles of the parties as being the Controller of personal data and the Personal data representative must be regulated in the agreement. The agreement must specify that the Personal data representative may only process personal data in accordance with instructions issued by the Controller of personal data. Furthermore, the Personal data representative must also implement appropriate, adequate technical and organisational measures to protect the personal data.
- Risks resulting from dependence on one particular supplier must be minimised.

Cloud services

The operation of services that contain sensitive information or that need to be integrated with other services must not be procured as a cloud service without a careful risk analysis first having been conducted and documented. Any necessary action must be taken in the light of the analysis results, and as a minimum the following must be guaranteed:

- Guarantees of availability must be included in the agreement with the supplier. Availability must satisfy the organisation's requirements.
- If there are strict availability requirements, there must be a redundant Internet connection.
- The agreement should include a penalty clause.
- The agreement must specify which organisation(s) has/have access to the information.
- The number of people who have access to the information must be limited.
- The agreement must specify expressly that the supplier may ***not*** use KI's information for its own or another party's use apart from what has been specifically agreed.
- If the information will be processed outside Sweden, the legal situation must be analysed and steps must be taken to make sure that the security requirements for personal data, for example, can be guaranteed.
- The service must include export functions, so that KI can easily change supplier when the agreement ends or otherwise as required.
- The agreement must specify KI's opportunities to conduct an audit so that follow-up on agreed security requirements is possible.

Instructions on handling information in connection with recruitment, employment and termination of employment
When information in respect of Karolinska Institutet's employees is handled, there are a number of areas in which information security must be considered. Described below are requirements to guarantee information security within each sub-process.

Recruitment

- The job applicant's formal qualifications (e.g. education, degree, references, etc.) must be checked.
- The job applicant's identity must be checked to make sure that the person really is the person he/she claims to be.
- When recruiting for particularly sensitive jobs, additional register checks should be performed of the person recommended for the position.

Employment and terms of employment

- In connection with commencement of employment, the employee must be informed of his/her obligation to meet the requirements of KI's information security guidelines and regulations, as well as the associated instructions.
- All employees must be made aware continuously during their period of employment of their obligations under the item above, and must also be informed of current rules on information security and applicable legal requirements, such as the Swedish Public Access to Information and Secrecy Act (2009:400).
- It must be made clear which information is owned by the employer and which may not be destroyed or copied upon termination of employment.

- It must be made clear to employees that any breach of current guidelines, rules and instructions for information security may be treated as negligence, which is a breach of the employment contract and may result in action being taken under labour law.

Termination of employment

- Activities must be implemented to make sure that responsibilities are handed over and that access rights ceases upon termination of employment. Steps must also be taken to make sure that keys, badges and other items of equipment are returned.

Consultants and other external personnel

- When a consultant or other external contractor is hired, it must be determined to what extent he/she is a member of the organisation in the same way as an employee and thus is covered by the Swedish Public Access to Information and Secrecy Act. Otherwise the duty of confidentiality must be regulated in civil law, i.e. in an agreement.
- Consultants and other external personnel must be made aware of their obligations to satisfy the requirements defined in KI's guidelines, rules and instructions on information security.
- Access rights (both logical and physical) that are granted to consultants and other external personnel must match the period of the assignment. Activities must take place to make sure that the access rights cease in connection with the end of the assignment.

3.6 Defining requirements for communication and network security

Karolinska Institutet Chief Security Officer is responsible for the general definition of requirements for security in respect of KI's networks and infrastructure. The level of the requirements defined must be coordinated with the information owners' requirements for availability and protective measures. These instructions should be viewed purely as a means of support regarding which areas should be included in the definition of requirements and the minimum level to be observed within KI.

The network environment

The network environment and its components must be documented and monitored from a security perspective. There must be system diagrams showing all components in the network, and all connection points with other networks must be clearly labelled. Each component must be documented with a network name, brand, model, software and configuration. There must also be one or more logical system diagrams of all system relationships. Technical solutions such as cabling, active network components and communication protocols must be chosen on the basis of KI's requirements for information security.

Wireless networks

When information is transmitted by means of wireless networks, risks occur, including the risk of eavesdropping, and communication via wireless networks must therefore be encrypted. Detailed instructions must be drawn up for the design, configuration and use

of wireless networks. The risk of disruption of sensitive electronic equipment must always be borne in mind when using wireless networks.

External networks

Connections to external networks (outside KI's network) and the Internet must be regulated by specific instructions. Internet connections and computers used by those other than KI's employees (e.g. guest lecturers or visitors) must be logically separated from KI's network (so-called guest network).

Hardware in the network

It is not permitted to install or run software that is not work-related on KI's hardware that is connected to the internal network. All hardware (workstations, laptops, PDAs, tablet PCs, mobile phones, etc.) connected to the network must satisfy KI's current security rules. The use of software on KI's hardware must not be in breach of current copyright legislation. Hardware that is connected to KI's network may not be simultaneously connected to other fixed or wireless networks. All hardware that is connected to KI's network must be protected and configured in accordance with defined, documented standard configurations. Synchronisation of email, calendar, etc. is only permitted on hardware on which approved security solutions are installed.

Phones and smartphones

The use of mobile phones must be regulated through instructions in respect of the use of email and other internal resources.
Wireless telephones in general are not encrypted and are therefore not suitable for sharing sensitive information. This is also true to some extent of text messages and voice calls from mobile phones. When communicating sensitive data over the phone, measures must always be taken to make sure that the right person is receiving the data.

3.7 Defining requirements for reliability and service level

The owner of a specific IT resource (systems/applications, networks, technical platforms, etc.) is responsible for defining requirements in respect of its reliability. The level of requirements defined should be based on a completed risk analysis and with due reference to the information classification of the system or information asset. These instructions define the minimum level that must be observed within Karolinska Institutet and also provide support when defining which areas, by way of example but not exclusively, should be included in the definition of requirements.

Operation and operating documentation

Operation of KI's IT resources must take place in accordance with good practice and documented, implemented processes. There must be documented, continuously updated, operating procedures and operating instructions, and all operations must take place in accordance with these. The documented operating documentation must be updated as required and revised at least once a year, or otherwise as required. Where possible, evidence that the procedures/instructions are being observed must be documented and archived.

Copies of operating documentation must be stored apart from the originals, and archiving of documentation must take place in accordance with established procedures.

Security patching

Security patching in respect of operating systems and programs must be managed in a controlled, prompt way. To make sure that operations are not adversely affected, security patches must be tested and analysed before they are installed in the production environment. If the analysis indicates that the security patch generates risks to the stability of the production environment, there must be a documented explanation of the reason why the security patch is not implemented.

There must be detailed instructions for the handling of urgent security patches, i.e. patches that have to be installed so promptly that there is no time to test them. The instructions should guarantee that tests are conducted after installation, and that action is taken on the basis of the test results.

Change management

All changes made in KI's IT systems must be carefully planned and analysed, and all changes, as well as testing and transfers of changes to the production environment, must be formally approved by an authorised person. These approvals must be documented and archived. The principle of duality must be applied, i.e. development, testing and migration to production must not be performed by one single person and must take place in separate environments. The development and test environment may not contain sensitive information unless special safety measures approved by the System Owner have been taken.

There must be detailed instructions on how changes are to be managed and tested, as well as plans for being able as required to return to the status before the change commenced.

There must also be detailed instructions on urgent changes that have to be initiated immediately, when there is no time to follow the normal change process. Such changes might be, for example, disruption in the production environment. Urgent changes must be documented and followed up subsequently in accordance with detailed instructions on urgent change management.

Capacity planning

The purpose of capacity planning is to predict and prevent capacity and performance problems in KI's IT environment. To make this possible, there must be regular measurement of and follow-up on IT capacity. There must always be capacity planning for business-critical systems within KI.

Malware protection

IT hardware that risks being exposed to malware must be protected by means of appropriate software that must be capable of identifying, deleting and protecting against known types of malware. Users must not be able to uninstall or close down the software (antivirus function); this may only be done by authorised administrators. Updating of the program's definition files and checking of hardware must take place automatically. Scanning of servers and clients for malware must be performed on a daily basis. Files infected by malware must be automatically rendered harmless and events relating to malware must be logged, flagged up and followed up. If malware is discovered, this must be reported as an incident, see *Instructions on the handling and reporting of information security incidents.*

Backing up and restoring data

Backing up of information and software must be performed regularly in such a way that individual files can be restored. The frequency and scope of the backup routine vary, but should be based on the availability requirements defined in the information classification, see *KI's information classification model*. The System Owner is responsible, after consultation with the person responsible for the information, for documenting these requirements and making sure that appropriate security mechanisms are in place on the basis of the information's classification.

Backups must be clearly labelled and protected against overwriting and physical destruction, and must be stored apart from the originals and in premises that satisfy the requirements described in chapter 6, *Physical security*, in *Rules on information security.*

Restoration tests must be conducted on a regular basis to make sure that the backups can be used if required. The test results must be documented.

System documentation

There must be complete, continuously updated system documentation for all IT systems within KI. System documentation must be produced in accordance with good practice and documented, implemented processes. Copies of system documentation must be stored apart from the originals, and archiving of documentation must take place in accordance with established procedures. The parts of system documentation that deal with sensitive information, such as security functions, must be stored in such a way that only authorised personnel can access them.

3.8 Administration of access rights

There must be detailed instructions and an organisation for the administration of access rights for access to Karolinska Institutet's (KI's) networks and systems. This is to make sure that only approved access rights are set up in the systems. The System Owner, or the equivalent role in cases where information is not stored in a specific system (but is, for example, in a folder structure in a shared storage area), is responsible for the instructions and organisation for each system/environment.

The following applies for the administration of access rights:

- A needs and risk analysis must be performed for the setup of access rights in the system or another electronic storage area. This is so that rights can be assigned in a correct way. The analyses must be performed and evaluated in consultation with those responsible for certain information.
- The access rights assigned to a user in a system, or other electronic storage area, must not be any higher than is required for the person to perform his/her current work.
- Access rights to a system, or other storage area, may only be used to perform the work that the user has been instructed to do by KI.
- If there are several owners of information that is processed in one single system, these owners must jointly agree on the work method and instructions for the administration of access rights.
- User IDs must be unique and must be used in combination with personal passwords.

- Privileged access rights, known as administrator rights, must be personal and limited to as few people as possible. These may only be issued following a written decision by each System Owner, or equivalent role in cases where information is not stored in a specific system. For central IT systems, a formal, written decision is also required from the IT Manager.
- Privileged access rights, known as administrator rights, for technical IT hardware must be personal and limited to as few people as possible, and access rights may only be issued following a written decision by each the person responsible for the information.
- Strong authentication (so-called two-factor authentication) is required for access to information that has been classified at the highest level in respect of confidentiality[2].
- Passwords must be kept confidential and changed regularly, as a general rule at least every 90 days. If there is system support to guarantee the complexity of passwords, this must be used.

Instructions on administration of access rights

Instructions on controls over the ordering, changing and removal of access rights must be defined for each system or other electronic storage area. The instructions must as a minimum contain the following information:

- How the ordering of additions, removals and changes of access rights is to proceed.
- Which templates or forms are to be filled in and how they are to be used.
- How the specific access rights being ordered are to be specified and that it must be possible to link actual tasks to the various rights being ordered.
- Which criteria and tasks the user must have for an application for access rights to the system, or other electronic area, to be made.
- Who (roles) may order access rights.
- Who (roles) may decide whether a user is to be granted access rights.
- Where the order is to be sent and who (roles) sets up the access rights in the system/other storage area or orders the rights from an IT provider, if relevant.
- How the delivery of access rights and a temporary password is to proceed and how it is guaranteed that the right user receives this information.
- How traceability is guaranteed, i.e. how ordering and approval are to be saved and archived.

[2] Two-factor authentication involves checking identity using two different kinds of information, usually something that people have and something that they know. For example, like an ATM card, where the card itself is something people have and the PIN code is something that they know.

3.9 Reviewing access rights

There must be regular follow-up on existing access rights in Karolinska Institutet's systems and IT environments in order to make sure that they are compatible with users' needs and tasks, and that unauthorised people do not have access to sensitive information. These reviews must be performed at various frequencies, on the basis of the information's/system's information classification, as follows:

Information class:	***Frequency:***
C4 and/or I4	Quarterly
C3 and/or I3	Quarterly
C2 and/or I2	Half-yearly
C1 and/or I1	Annually

Authorisations for particularly privileged access rights, known as administrator rights, must always be reviewed quarterly.

In addition to the frequencies described above, there must also be reviews of all access rights in connection with major organisational or system-related changes.

Documentation

When reviews are conducted, it is important that the documentation is saved, not only to make it possible to follow up on the handling of access rights, but also so that auditors and other supervisory bodies can be shown that the reviews have actually been conducted. The following points provide guidance on which kinds of documentation must be saved as a minimum:

- Base data (list of users from the system) on which the review was based.
- Approval/confirmation in respect of all access rights granted for the system.
- Base data for ordering in respect of changes and removals that the review has generated.
- New base data (list of users from the system) showing that changes from the review have been implemented.

General guidelines on reviewing access rights

NB: The following guidelines are general, simplified and produced to suit most systems, or other electronic storage locations, within KI. The intention is that the guidelines shall provide support in the production of local instructions to guarantee that there are regular, appropriate reviews of access rights.

Regular reviews of access rights should at least include the following activities:

1. The person responsible for certain information, or the System Owner if the task in question has been delegated to him/her, initiates the review by asking the relevant administrator to order/produce a list of the relevant system's users and their access rights.

2. The list of rights is then sent to relevant managers, Heads of Department, administrative manager and any other interested parties (e.g. the person responsible for the information), who are thus involved in the review by reviewing all accounts

(both user accounts and system accounts) in the system based on the following aspects:

a. Who owns the account?
b. Does the person need an account with reference to his/her tasks at work?
c. Is this the right level of access rights on the basis of the person's work and organisational affinity?

3. The administrator of the review compiles the information from the organisation's examination and then draws up a list of the changes and/or deletions of access rights that are to be implemented.

4. The administrator implements the changes or orders them from the IT provider.

5. The administrator orders/produces a new list of the system's access rights and makes sure that the changes ordered have actually been implemented.

6. The administrator concludes the review by saving the documentation that the review has generated in the designated location.

3.10 Logging and examining logs

There must be logging of all systems and electronic storage locations (e.g. when research data are not stored in a specific system, but for example in a folder structure in a shared storage area) where business-critical information is stored. This is to make sure that relevant user activities and information security events are registered and traceable. The the person responsible for the information is responsible for making sure that satisfactory logging and examination of logs take place in respect of the handling of information. The System Owner, or the equivalent role in cases where information is not stored in a specific system (but is, for example, in a folder structure in a shared storage area), is responsible for ensuring that actual examinations are conducted.

Logging

The following applies in respect of logging:

- Monitoring and logging must comply with current, relevant legal requirements. The logs must as a minimum contain information about the following:
  - all events in the system, or in another electronic storage location, initiated by a user or another system,
  - which user initiated the event and the time,
  - all unsuccessful login attempts in the system, and the IP address from where the login attempt was made,
  - system alarms or faults, and
  - changes, or attempted changes, in the system's security settings and security measures.
- Users must be informed that their activities in networks and systems, etc. are logged and the purpose of follow-up on these logs. This information can be issued, for example, in each system's user instructions or as an automatic message in con-

nection with login.

- All log files must be protected against unauthorised access and manipulation, and subject to relevant backup routines in accordance with defined instructions. Logs must be saved in accordance with current legislation and the requirements of the person responsible for the information
- To guarantee the value of the logs as evidence, the system clocks of logging systems must be synchronised with a designated normal clock.

Examination of logs

There must be regular examinations of logs for systems that have high classification in terms of confidentiality (C3 and C4) and correctness (I3 and I4). The examinations must be conducted on the basis of defined instructions as follows:

- The instructions must describe what is being logged, how often the logs are to be examined, who is to conduct the examination and what is considered to constitute a breach and how any breaches are to be handled and reported. Decisions on how often the logs, either in full or only certain parts, are to be examined should be based on the risks that exist, with consideration given to, for example, the value and sensitivity of the information in question. Activities of system administrators and operators should, however, be examined at least on a monthly basis.
- If possible, the logs must be analysed with the aid of automated tools. If this is not possible, sufficient manual checks should be performed instead.
- Access to logs and log analysis tools must be limited and regulated through individual access allocation.
- Base data from completed log examinations must be saved, and access to these regulated through individual access allocation.

3.11 Defining requirements when acquiring or developing systems

When developing or acquiring information systems, the person responsible for the information must make sure that the following activities are carried out:

Before development or acquisition

- A risk analysis must be performed in order to define the information security requirements of the system. These requirements must then be documented as part of the specification of requirements.
- In connection with the risk analysis, there must also be an assessment of how the intended system solution complies with laws and regulations, for example the Swedish Personal Data Act (1998:204).

Procurement of supplier for development or acquisition

- When procuring systems, documented requirements of the suppliers' work on information security must be included in the tender documentation.
- KI's requirement regarding information security must be defined and agreed with the selected supplier.
- In connection with system development, an assessment must be performed of

which software, information and rights that are to be owned by KI after completion of the assignment. An agreement with the selected supplier must be drawn up in accordance with this assessment.

During development or acquisition

- During development, accepted system development models must be used in order to guarantee traceability at all stages of development.
- Tests must be conducted in a separate test environment in order to guarantee the integrity of the system's output data. Anonymous test data must always be used and actual personal data must never be used in a test context. The integrity of output data must be evaluated during the test phase using plausibility checks.
- Steps must be taken to make sure that security requirements identified for the system have been implemented in accordance with what was defined in the specification of requirements.
- Before the system can be migrated to the production environment, it must undergo an acceptance test/validation, which the buyer must approve.
- A System Owner must be appointed for the system.

Migration to production environment of developed or acquired system

- The buyer's operational approval, which must form the basis of a decision on the migration to production environment of the system, must include follow-up on the predefined information security requirements.
- In connection with development or acquisition, complete system, user and operating documentation must be produced. Operating documentation must also include a general description of the re-initiation procedures required for the system's shutdown plan. All documentation must be produced and available to the persons concerned no later than when the system is migrated to the production environment.

3.12 Defining requirements for system administration

The System Owner is responsible himself/herself, or through a designated administrator, for the administration of the system and the security requirements relating to administration. The System Owner is responsible for ensuring that as a minimum, but not exclusively, the following requirements are satisfied within the framework of system administration. Additional requirements relating to operation are also contained in *Instructions on defining requirements for reliability and service level*.

- There must be a documented system administration plan, containing instructions on administration, operation and maintenance, for the purpose of ensuring that the system is managed correctly on the basis of an information security perspective.
- There must be current, updated system documentation, which must be available to all concerned, authorised persons as required.
- There must be a disruption plan for the system, and the plan must be linked to the business continuity plans for the areas of the organisation that the system supports.
- The system's users must be informed about the system's protective measures, and users must receive the necessary security training before they are granted access to the system.

- All information security incidents identified under the administration must be reported in accordance with the current instructions. For further information on reporting incidents, see *Instructions on the handling and reporting of information security incidents*.
- Functional faults and defects relating to the system must be continuously analysed and reported to the System Owner.
- When changes are made in the system, KI's information security requirements in respect of change management must always be observed.

In addition to the practical handling of the requirements described above, the system administrator must support the System Owner and the person responsible for the information in respect of:

- handling administration and examination of access rights, see *Instructions on administration of access rights* and *Instructions on examining access rights* for further information
- risk analyses for the system and the production of proposed action and improvements based on these, see *Instructions on conducting risk analyses* for further information.

3.13 Handling and reporting of information security incidents

The main purpose of these instructions is to:

- define how the reporting of information security incidents (incidents) is to proceed
- define how incidents are to be classified
- describe how incidents in different classes are to be dealt with

Reporting of incidents

Information security incidents are events that have, or may in the future have, a negative impact on the security of KI's information assets. Incidents that occur in connection with information processing in the organisation, i.e. have an impact on information in respect of confidentiality, integrity or availability, must be reported as soon as possible by the person or persons who have discovered the incident. Reports shall be made primarily to the Head of Department or to the Information Security Coordinator appointed by him/her for the department/unit, and to the immediate manager if this is considered necessary.

Reported incidents must be evaluated with reference to the following four classes:

Incident management

The recipient of reported incidents is the Head of Department or the Information Security Coordinator appointed by him/her. These persons must perform a prompt initial analysis of the potential impact of the incident in order to assess how the incident is to be classified, and whether it needs to be further escalated in the organisation.

Reported incidents must be handled in order of priority with reference to the classification of the incident. Handling of incidents must include:

- Documented information about the incident, including: time, what happened, circumstances, etc.
- Any evidence must be obtained, for example by examining logs.
- KI's IT Department and other relevant providers of IT services must be informed if this is considered necessary. There must be a formal way of reporting incidents to these suppliers.
- In the event of an incident that also has a physical impact, the Security Manager must also be informed.
- Experience from incidents dealt with must be reused in order to guarantee effective, appropriate handling in the future.

Reporting

Incidents must be reported depending on their classification in accordance with the description of procedures on the previous page. Every year the Chief Security Officer must ensure that a summary report is produced of all incidents relating to information security. An analysis must also be conducted and suggestions made for any necessary improvements in order to avoid similar incidents in the future if possible. Experiences from the reporting and handling of incidents should be used when risk analyses are performed and as base data for updating the rules on information security.

3.14 Continuity planning

There must be continuity planning for all departments and critical processes within Karolinska Institutet (KI), and this must be documented in a continuity plan. The following areas must be considered:

1. ***Definition of areas/scope and strategy***
   The continuity plan must clearly state which operational processes it covers and the strategy selected to restore the processes. There may be different strategies, depending on the type of event that has a consequence on the availability of the operational process, as well as which process the plan is designed to cover. Analyses of risks and consequences must be conducted and form the basis of the strategy selected.

2. ***Analyses of risks and consequences***
   Risk analyses, which consider potential vulnerabilities and threats to the organisation and its key processes, must be conducted on a regular basis (for further information, see *Instructions on conducting risk analyses*). Work on the risk analysis also obtains information that is necessary for, among other things, the ability to draw up a relevant continuity plan and to carry out preventive work. In continuity planning, the risk analysis must also include an analysis of consequences, in which the focus must be on the consequences of inadequate access to critical information. This identifies the organisation's need for, and requirement

for availability of, information in order to be able to maintain business-critical processes.

3. ***Recovery times***
   On the basis of the results of the analysis of consequences, critical recovery times for significant main and sub-processes must be defined. The definition of recovery times means that the maximum time that the process in question is permitted to be unavailable must be defined. This time has in turn an effect on the design of the continuity solutions, rectification activities and contingency procedures that have to be documented in the continuity plan.

4. ***Continuity solutions***
   The defined recovery times form the basis of which continuity solutions are to be selected and how contingency procedures are to be designed. The solutions to achieve continuity in the organisation must be designed so that they are practical and financially feasible on the basis of the strategy selected. The design of the contingency procedures must be sufficiently detailed for it to form the basis of the continuity plan.

5. ***Organisation to develop, introduce and maintain the plan***
   Roles and responsibilities to develop and work continuously on continuity plans must be defined and communicated. Work on and responsibility for this can ideally be divided in relation to the various sub-processes that must be covered by continuity planning. It is, however, important that one person is designated to be responsible for the administration and maintenance of the overall continuity plan.

6. ***Review, testing and exercise***
   Continuity plans need to be maintained, and as an element of this work the plans must be regularly reviewed and updated. Regular exercises of the plans must also be conducted in order to test that they are current, appropriate and actually work when needed. These exercises also serve to provide training for employees, and other parties concerned, in the continuity plans' contingency procedures.

Information class: K1R2T1

3.15 Handling requirements - Under revision

Confidentiality

Information class	Confidentiality	Requirements	Protective measure
4 Definition of serious damage: d) causes a serious restriction in KI's ability to perform its undertaking to an extent and for a period that means that the organisation is unable to perform one or more of its primary tasks. e) results in extensive damage to the organisation's or another party's assets; f) results in major financial losses for KI or another party, or d) has a seriously negative impact on an individual person's rights, life or health.	An information asset that contains sensitive information that may cause **serious damage** if it falls into the wrong hands. Generally applicable to: 1. An information asset that is or may become the subject of confidentiality under the Swedish Public Access to Information and Secrecy Act (e.g. information about individual people's illnesses or abuse, on-going cases involving the expulsion of students from higher education). 2. An information asset that may be the subject of an application requirement under special legislation (e.g. patient data, details of illness together with personal ID no.). 3. An information asset that constitute the organisation's own or another organisation's business secrets (e.g. crude research data relating to an individual person, unpublished research data, passwords, IT security settings). 4. An information asset that is not a public document and that may contain information that is sensitive for an individual or individual company/organisation (e.g. research information from people in the criminal register). 5. Information about animal experiments with a considerable level of severity for the animals. 6. Information that identifies persons who handle animals used in animal experiments. 7. Information about the physical storage of animals used in experiments (e.g. building plans, information about animal transport).	**Create:** Specify information class "C4" in header or designated place. **Store:** Locked in security cabinet, if it is a paper document. Printouts must never be left unattended. Not permitted to store away from normal workplace. Storage on hard disk/PC/smartphone, etc. requires authorisation check and strong encryption. Storage on CD/USB/other portable media not permitted. **Discuss:** Not permitted over the phone, either internally or externally. **Distribute:** May under no circumstances be distributed internally/externally without special security measures. If the information is sent externally, only approved courier firms may be used, and receipt must be acknowledged by an authorised person. Digital transmission only via an encrypted connection. Fax transmission is not permitted. **Email:** Internally: must be encrypted. Verify the recipient. Externally: not permitted. External contract partner: only via encrypted connection, verify recipient. **Discard:** Paper printouts must be destroyed in a shredder. Digital information must be overwritten using a special program.	Limited, needs-based access with strong authentication.

3 Definition of significant damage: d) causes a significant reduction in the ability to perform KI's operational undertaking to an extent and for a period that there is a tangible reduction in the effective performance of the organisation's primary undertaking; e) results in significant damage to the organisation's or another party's assets; f) results in significant financial losses for KI or another party, or d) has a significant negative impact on an individual person's rights or health.	An information asset that contains sensitive information that may cause **significant damage** if it falls into the wrong hands. Generally applicable to: 1. Information that must always be subject to a confidentiality test before being issued (e.g. diagnoses of illnesses of deceased persons identified via serial number, working documents from other authorities). 2. Personal data in general or that is considered sensitive under the Swedish Personal Data Act (e.g. where details of illness are specified but identification is via serial number rather than personal ID no., individual student matters relating to personal problems). 3. Data of an internal nature, with no other restrictions, to which only in-house personnel should have access (e.g. descriptions of methods in respect of research, information that identifies the manipulation of crude data, i.e. research fraud, information about sensitive meetings such as recruitments and donors, working documents and notes containing sensitive data).	**Create:** Specify information class "C3" in header or designated place. **Store:** At normal workplace in sealed storage facility that offers protection against theft. If it is stored at home/temporary workplace, the information must not be left unattended, otherwise locked. While travelling, the information must be kept in locked hand baggage. If possible, should be locked in hotel's safety deposit box. Storage on hard disk/PC requires authorisation check. Storage on CD/USB/other portable media requires strong encryption. **Discuss:** Permitted on the phone internally within KI. Not permitted via external phone. **Distribute:** To authorised personnel within KI. If the information is sent by internal post: sealed package. If the information is sent externally, only approved courier firms may be used, and receipt must be acknowledged by an authorised person. Fax: The recipient is phoned and reception monitored. Strong encryption must be used for digital transmission that does not use an encrypted connection. **Email:** Internally: encryption recommended. Verify the recipient. Externally: not permitted. External contract party: must be encrypted and the recipient verified. **Discard:** Paper printouts must be discarded in sealed containers. The contents are incinerated or destroyed in some other way. Digital information must be sent to the "Recycle Bin" on the computer desktop, and the "Recycle Bin" must then be	Limited, needs-based access.

		emptied immediately.	
2 Definition of moderate damage: a) causes a reduction in the ability to perform KI's operational undertaking to an extent and for a period that there is a clear reduction in the effective performance of the organisation's primary undertaking; b) results in minor damage to the organisation's or another party's assets; c) results in minor financial losses for KI or another party, or d) has a limited negative impact on an individual person's rights or health.	An information asset that contains sensitive information that may cause **moderate damage** if it falls into the wrong hands. Generally applicable to: 1. Information received from other parties (e.g. job applications). 2. Unidentifiable patient data, crude data from clinical trials (not traceable to an individual) and source code. 3. Information asset that does not constitute a public document and only contains general information (e.g. work material that does not contain any sensitive information or any information that may otherwise be traced to an individual company, product or person). 4. Information governed by organisation-specific legislation. 5. Information of an internal nature that, with no other restrictions, only in-house personnel should be able to access (e.g. research plans, strategic plans for the organisation, controlling documents, evaluations and assessments of personnel and students, memos and communication plans). 6. Information on which kinds of animal KI uses in animal experiments.	**Create:** Specify information class "C2" in header or designated place. **Store:** No restrictions if the information is stored at the normal workplace. If the information is stored at home/temporary workplace, the information must not be left unattended, otherwise locked. If the information is being processed while travelling, it must be stored in hand baggage or a suitcase. **Discuss:** Permitted by phone internally within KI and externally with an authorised party. **Distribute:** May be distributed internally within KI. **Email:** Internally: no restrictions. Externally: must be encrypted. External contract party: should be encrypted. **Discard:** Paper printouts must be discarded in sealed containers. The contents are incinerated or destroyed in some other way. Digital information must be placed in the "Recycle Bin" on the computer desktop.	Authorisation check required for access.
1 None/negligible	An information asset that only contains information that is publicly available data or information that, if it comes into the possession of unauthorised persons, causes **no damage**. Information that is intended for or can be distributed to an indeterminate group of recipients without any risk of negative consequences. Generally applicable to, for example: 1. Completed internal guidelines, process descrip-	**Create:** No restrictions. **Store:** No restrictions. **Discuss:** No restrictions for information in either paper or digital form.	No special measures.

	tions, instructions, course material and results of exams, manuals and rules of procedure, etc. that do not contain data that may be subject to confidentiality under the Swedish Public Access to Information and Secrecy Act. 2. Completed, published research reports, public presentations, external newsletters and other communication material. 3. Metadata. 4. Successful applications for funding, ethical permits and associated research applications. 5. Personal data relating to employees and associated persons. 6. Information about finance, equipment, technology, chemicals, etc. used within KI.	**Distribute:** No restrictions in either paper or digital form. **Email:** No restrictions. **Discard:** No restrictions.	

Integrity

Information class	Integrity	Requirements	Protective measure
4 Definition of serious damage: g) causes a serious restriction in KI's ability to perform its undertaking to an extent and for a period that means that the organisation is unable to perform one or more of its primary tasks. h) results in extensive damage to the organisation's or another party's assets; i) results in major financial losses for KI or another party, or d) has a seriously negative impact on an individual person's rights, life or health.	Information that, if it is not correct and complete, can cause **serious damage**. Generally applicable to: 1. An information asset with particularly high requirements for correctness (e.g. personal data and metadata such as research data). 2. IT systems or information assets for critical processes in the organisation (e.g. ……) .	Limited, needs-based access with strong authentication. Authorisation check and logging of activities in systems must be performed and followed up. There must be version management of documents and changes must be traceable. Duality for input and output data, i.e. the cooperation of at least two people is required to enter data into the system and to extract data from it. Steps must also be taken to make sure that logging is enabled for the system in order to guarantee traceability in activities carried out. System processes that update information must be actively verified in respect of their impact on the information. System changes must take place in accordance with the adopted process, and implementation of these system changes must be preceded by a satisfaction test to confirm that they only involve the intended system changes. Data integrity must be tested on a regular basis.	
3 Definition of significant damage: g) causes a significant reduction in the ability to perform KI's operational undertaking to an extent and for a period that there is a tangible reduction in the effective performance of the organisation's primary undertaking; h) results in significant damage to the organisation's or another party's assets;	Information that, if it is not correct and complete, can cause **significant damage**. Generally applicable to: 1. An information asset that is covered by legislation in which a requirement for correctness is specified (e.g. the Swedish Personal Data Act or special legislation). 2. IT system or information asset that is part of an authority exercise (e.g. system that stores certificates....). 3. Information or IT system in which there is a requirement for traceability or non-repudiation.	Limited, needs-based access. Authorisation check and logging of activities in systems must be performed and followed up. There must be version management of documents and changes must be traceable. System processes that update information must be actively verified in	

Information class	Integrity	Requirements	Protective measure
i) results in significant financial losses for KI or another party, or d) has a significant negative impact on an individual person's rights or health.		respect of their impact on the information. System changes must take place in accordance with the adopted process, and implementation of these system changes must be preceded by a satisfaction test to confirm that they only involve the intended system changes.	
2 Definition of moderate damage: a) causes a reduction in the ability to perform KI's operational undertaking to an extent and for a period that there is a clear reduction in the effective performance of the organisation's primary undertaking; b) results in minor damage to the organisation's or another party's assets; c) results in minor financial losses for KI or another party, or d) has a limited negative impact on an individual person's rights or health.	Information that, if it is not correct and complete, can cause **moderate damage**.	Authorisation check must be required for access to systems. System changes must take place in accordance with the adopted process.	
1 None/negligible	Incorrect information can only cause **little or no damage**.	No special measures.	

Availability

Information class	Availability	Requirements	Protective measure
4 Definition of serious damage: j) causes a serious restriction in KI's ability to perform its undertaking to an extent and for a period that means that the organisation is unable to perform one or more of its primary tasks. k) results in extensive damage to the organisation's or another party's assets; l) results in major financial losses for KI or another party, or d) has a seriously negative impact on an individual person's rights, life or health.	IT system or information asset that is a part of or supports continuous activity in which disruption may cause **serious damage.** Generally applicable to: 1. IT systems or information assets that are extremely critical for the organisation (e.g. ……).	In the event of a disaster, it must be possible to restore the information within 24 hours. The maximum loss may be of the last four hours' information created.	
3 Definition of significant damage: j) causes a significant reduction in the ability to perform KI's operational undertaking to an extent and for a period that there is a tangible reduction in the effective performance of the organisation's primary undertaking; k) results in significant damage to the organisation's or another party's assets; l) results in significant financial losses for KI or another party, or d) has a significant negative impact on an individual person's rights or health.	IT system or information asset that is a part of or supports continuous activity in which disruption may cause **significant damage.** Generally applicable to: 1. IT system or information asset that is a part of or provides support for an authority exercise and/or core activity. 2. E-services for the public or other stakeholders.	In the event of a disaster, it must be possible to restore the information within 1-7 days. The maximum loss may be of the last eight hours' (one working day's) information created.	
2 Definition of moderate damage: a) causes a reduction in the ability to perform KI's operational undertaking to an extent and for a period that there is a clear reduction in the effective performance of the organisation's primary undertaking; b) results in minor damage to the organisation's or another party's assets; c) results in minor financial losses for KI or another party, or d) has a limited negative impact on an individual person's rights or health.	IT system or information assets where organisational dependence is relatively low and where disruption may cause **moderate damage**.	In the event of a disaster, it must be possible to restore the information within 7-14 days. The maximum loss may be of the last eight hours' (one working day's) information created.	
1 None/negligible	IT system or information asset where organisational dependence is low and where disruption may only cause **little or no damage.**	No requirements.	