Guiding Principles and Rules on Information Security at Karolinska Institutet

(excl. appendices)

Ref. 1-516/2013

Version 2.0
Applicable from 01-10-2013

Karolinska Institutet

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.

Published by:
Karolinska Institutet
University Administration
Version: 2.0, 01-10-2013
For further information, please contact the Chief Security Officer.

Karolinska Institutet

Decision
2012-10-09

Ref.: 6255/12-060
Page: 1/1

Management system for information security at Karolinska Institutet – LIS

Karolinska Institutet's (KI) mission is to contribute to improving people's health by means of research and education. In this work, various kinds of information represent significant prerequisites and assets. Everyone working within KI must therefore work actively, effectively and continuously with information security, i.e. how different kinds of information are handled in different contexts.

To support a systematic work on information security within KI, a management system has been developed consisting of, among other things, guidelines, rules and instructions, which are hereby confirmed in accordance with the appendices.

The decision in this matter was made by the undersigned University Director following a presentation by Deputy University Director Marie Tell.

Bengt Norrving

Marie Tell

Guiding Principles and Rules on Information Security at Karolinska Institutet

Ref. 1-516/2013

Confirmed by the University Director on 09-10-2012 for application from 01-04-2013.

Revised version 2.0, 01-10-2013

CONTENTS

Reading tips

For best possible understanding of these Rules and guidelines, please read the complete document. Some chapters, however, are targeted on specific categories of staff, see below:

Category of staff	Relevant chapters
All categories at KI	1, 2, 4
IT-staff (central/local)	6, 7, 8, 9, 10, 11
System owners	3, 7, 8, 9, 11
Department chairs and chief administrators	3, 5, 6, 7, 10, 11, 12

(You should also read the applicable appendices for each relevant chapter)

Guiding Principles on Information Security within Karolinska Institutet

Karolinska Institutet's (KI) mission is to contribute to improving people's health by means of research and education.

KI's work is founded on principles of high quality and an ethical approach, and on the basis that education and research must collaborate in a mutual sharing of knowledge and experience.

In this work, various kinds of information represent significant prerequisites and assets. Everyone working within KI must work actively, effectively and continuously with information security, i.e. how different kinds of information are handled.

The objective of KI's work on information security is to guarantee:

- *Confidentiality* – that sensitive information is only accessible for authorised persons
- *Integrity* – that information is reliable, correct and complete
- *Availability* – that information is available on the basis of the organisation's needs

Another important aspect that must be considered when handling KI's information is *traceability*, i.e. that it is possible to specify who has had access to and potentially changed information.

KI's security solutions and associated procedures and processes must be based on how critical and sensitive the information in question is. This approach achieves a level of protection for the information that is adapted to the risk.

These are all important prerequisites that contribute to guaranteeing confidence in the activities that are carried out under KI's auspices, as well as being an important element of general work on risk management, internal management and control.

These guiding principles and the associated rules and instructions cover all of KI's activities, which means everyone with an active role, i.e. all employees, students, contractors/associates and consultants in the organisation, as well as premises, equipment, processes, systems and information.

Information security covers all kinds of information, regardless of whether the information is in digital form, on paper or verbal. It is based primarily on common sense and good judgement, in which each individual's knowledge and actions are crucial.

Rules on Information Security

1 An introduction to information security

This information is for everyone associated to KI's organisation

The aim of these rules is to introduce a basic level of information security within Karolinska Institutet (KI). KI must make sure that everyone is aware of the importance of their own contribution to maintain suitable protection and ethical, correct handling of the organisation's information.

These rules on information security, which took effect on 01-04-13, constitute Karolinska Institutet's (KI's) basic regulations for handling the organisation's information. The implementation of these rules and required actions will be made gradually.

There will be no revision of compliance until implementation of different aspects of the rules has taken place.

As an organisation, KI is continuously exposed to various security risks, for example fire, theft and intentional or unintentional damage, unauthorised access to information and illegal handling of data. If these risks become a reality, this can result in problems such as a loss of confidence and compromised integrity, financial damages or other kinds of losses, and harm to KI's reputation. It can also result in damage to an individual or another party's organisation.

Information security is about protecting all kinds of information, regardless of whether the information is in digital form, on paper or verbal. This means, for example, information assets such as research data, personal data, staff registers and IT systems. Sensitive information has to be protected in an appropriate way from unauthorised dissemination (for example the issuing of information in breach of current confidentiality legislation), incorrect changes or unavailability. In other words, work on information security aims to make sure that information:

- is not issued to unauthorised persons – *Confidentiality*
- is always reliable, correct and complete – *Integrity*
- is available when needed in day-to-day activities – *Availability*

The combination of rules and associated instructions form a framework for KI's total protection of information assets within the organisation. To achieve success with these information security initiatives, it is necessary for everyone to understand their responsibility and to strive to comply with these rules.

The rules are based on current laws and regulations, including the regulations on information security issued by the *Swedish Civil Contingencies Agency* (MSB), (MSBFS 2009:10 Föreskrifter om statliga myndigheters informationssäkerhet) and the ISO standard for information security (SS-ISO/IEC 27002: 2005). The aim of these rules on information security, which describe what must be done, is among other things to specify and define precisely the guidelines on information security for KI's activities. For a number of the areas described in the rules there is an additional level of detail, which is described in the form of instructions. These are intended to provide a more detailed description of how various activities relating to information security are to be carried out.

2 Information security organisation

This information is for everyone in KI's organisation

Protecting information in an appropriate way requires that work on information security is organised in a structured, effective way. Information security must be a natural element of day-to-day work. A clearly defined organisation covering responsibility for and work with information security is a prerequisite for KI to achieve success in this task.

Basic security

The University Director has drawn up the organisation's guidelines on information security and has, as part of his assignment, the ultimate responsibility for information security within KI.

The Chief Security Officer has, on behalf of the University Director, the task of making sure that general work on information security is carried out in a way that is as effective and as appropriate to the organisation as possible. The Chief Security Officer, supported by an *Information Security Coordinator*, organises the coordination of work on information security within KI, manages guidelines, rules and general instructions on information security, and makes sure that compliance at operational level is followed up regularly and reported to the University Director.

Heads of Department within KI are responsible for information security within their own areas of responsibility as an element of their delegated operational responsibility. *Managers* and *supervisors* at all levels must make sure that their employees receive sufficient training, continuous information about information security and comply with defined rules on security. The Head of Department is responsible for the right conditions being in place locally for work on information security and must regularly follow up and report on compliance within his/her area of responsibility to KI's Chief Security Officer.

It is suggested that the Head of Department appoint a *local Contact Person* to support him/her in carrying out work on information security within his/her own organisation and to support employees in their day-to-day work on information security. The actual tasks of the local Contact person at operational level may vary between different areas. This depends on the scope of responsibilities that the role is assigned by the Head of Department.

Everyone associated to KI, i.e. employees, students, contractors/associates and consultants in the organisation, is responsible for protecting the organisation's information when handling it. It is therefore important that everyone is familiar with and observes these rules and underlying instructions on information security. For further information about the responsibilities of those with active roles, see Appendix 1 *Guidelines on information security*.

There are several roles within KI that have a specified responsibility relating to the organisation's work on information security. In addition to the roles described above, persons responsible for certain information, System Owners and the IT Director have a specified responsibility with regard to KI's information security. For further

information on roles and responsibilities in the area of information security at KI, see Appendix 2, *descriptions of responsibilities* for each role.

There is also a Personal Data Representative within KI with responsibility for making sure that personal data are handled in accordance with the Swedish Personal Data Act (PuL).

3 Risk management

This information is aimed at managers and system owners
The information and systems used within KI are important for running the organisation, and they must therefore be appropriately protected. In order to determine the right way for KI to protect information and systems, related risks must be identified and analysed. Risk analyses must be a natural element of KI's work methods and contribute to making it possible to run the organisation in an appropriate and effective way.

Basic security

In order to make sure that information is handled in a secure way, threats relating to information must be continuously identified, analysed and managed using suitable protective measures. To determine which protective measures are suitable for each information asset, risk analyses must be conducted continuously.

Risk analyses make it possible for holders of roles with responsibility for information to identify primary risks. These are then assessed on the basis of the probability that the threat will be realized together with potential consequences. The analysis provides base data for a decision on which protective measures are required in order to make sure that the risks, i.e. the consequence and probability that a threat is realised, are managed and minimised in an appropriate way. All protective measures must be documented in such a way that it is possible to check compliance.

Risk analyses must be based on aspects of confidentiality, integrity and availability of the information analysed. See also Appendix 3.1, *Instructions on conducting risk analyses*, which provides guidelines on the most important steps in a risk analysis.

Within KI, risk analyses must be a natural element of handling information and must be conducted at several different levels; at governing organisational level, at institutional level, in respect of specific systems or information assets, etc. Risk analyses must be conducted in connection with changes in the organisation, processes and information systems. Risk analyses must be conducted annually for all business-critical[1] systems. In connection with this, analyses must also be conducted if there are new or changed internal or external requirements that affect the system in question. A person must be appointed for all risks identified with responsibility for making sure that the risks are handled in an appropriate way. There must be follow-up to ensure that identified risks are resolved or handled in some other way within a reasonable time. The results of conducted risk analyses should be reported to the Chief Security Officer.

[1] Business-critical information means information that is classified in the two highest classes in any of the aspects confidentiality, integrity and availability. (For further information, see Chapter 4, Handling assets).

4 Handling assets

This information is aimed at those responsible for certain information
At Karolinska Institutet there are important assets that are necessary for the organization, e.g. information assets in the form of research and educational data. These assets must be handled in such a way as to make sure that they are protected against unauthorised access, incorrect changes and that they are available when needed.

Basic security

For all information assets within KI a person must be appointed responsible.. There must be a register of information assets and who is responsible for each of them. All information assets within KI must also be classified and labelled in order to specify how significant the asset is to the organisation. There must be documented, detailed instructions and a structured work method describing how classification is to be carried out. Classification of the information asset must be reviewed regularly as a natural element of continuous work on security. Information assets within KI must be classified and labelled in accordance with KI's information classification model, see Appendix 3.2, *KI's information classification model.* This is valid for information in both physical and electronic form.

Handling of various kinds of information must take place as follows:

Personal data	Personal data must be handled in accordance with the Swedish Personal Data Act (1998:204). There is further information about this in Appendix 3.3, *Instructions on the handling of personal data*.
Protected personal data	Protected personal data must be handled in accordance with Chapter 22 of the Swedish Public Access to Information and Secrecy Act (2009:400).
Issuing of information	There must be instructions for the issuing of information, stating who is entitled to make decisions on issuing information. A confidentiality test must always be conducted before information is issued. Please see http://internwebben.ki.se/en/storing-and-issuing-public-documents
External handling of information	When KI's information is handled by a third party, for example external suppliers, requirements in respect of information security must be specified in a contract between the supplier and KI. For further information, see Appendix 3.4, *Instructions on defining requirements for operations outside KI*.
External access to information	When accessing KI's information from an environment outside KI's control, specific requirements must be defined for authentication and encryption.

5 Staff resources and information security

This information is aimed at managers, personnel staff and others, that grant access to internal information

Everyone with an active role within Karolinska Institutet must understand his/her responsibility to protect KI's information. Everyone concerned therefore needs to be given continuous information about and training in current information security requirements. The purpose of this is to enable KI to continuously maintain an appropriate level of protection for information.

Basic security

Steps must be taken to make sure that everyone with an active role understands his/her responsibility in respect of information security within KI. The purpose is to ensure that all information within KI is handled in accordance with current rules. Responsibility for information security must be clearly set out in connection with commencement of employment and in a job description. For others with an active role, responsibility for information security must be specified in connection with their being granted access to KI's internal information. For further information about the specific information security requirements that exist in respect of handling by staff, see Appendix 3.5, *Instructions on handling information in connection with recruitment, employment and termination of employment.*

Responsibility for information security within KI must be clearly defined. Chapter 2 *Information security organisation* describes the responsibility for work on information security within the organisation. The detailed responsibility for information security is described in each *description of responsibility, Appendix 2*. Those with an active role must be made aware of their responsibility in respect of information security, which is described partly in the *Guidelines on information security, Appendix 1*. In addition to this information, there may be local rules that need to be considered.

All those who have an active role within KI must be given the training in information security that is required in order that they are able to perform their work in accordance with defined guidelines, rules and instructions. The scope of training must be adapted to the responsibility and the levels of authority that apply for the assignment. Everyone who is granted access to KI's information must have completed a basic information security course. Responsibility for this rests with the relevant manager. Training and ongoing training in the field of information security must be a continuous process within KI.

One important kind of information in this context is that which relates to those with an active role within KI. Correct handling of this information must be clearly set out in the form of instructions, procedures and checklists within the framework of the HR function's work.

6 Physical security

This information is aimed at those with responsibility for security and IT-security.
All information that is handled under the auspices of Karolinska Institutet must be physically protected, regardless of whether it is stored digitally or on paper. To make sure that the information is protected, regardless of whether it is being handled in KI's own premises or elsewhere, it is important that everyone assumes responsibility for physically protecting it. KI also wants to make sure that only those people who actually need to have access to KI's premises are given it.

Basic security

The security level of physical protection must be based on completed risk analyses and be in proportion to the risks identified. The basic rule must be that sensitive information must never be left unprotected. Hardware that is sensitive or that processes sensitive information must be located such that the opportunity for unauthorised access is minimised and the creation of appropriate protective measures is facilitated.

Information written on paper must be protected in an appropriate way in accordance with the information classification level that has been agreed for the information in question.

IT hardware that in any way processes information centrally must be housed in a secure area with suitable access controls, to which only authorised persons are granted access. "Secure areas" means areas that have been specially designed in order to meet stricter requirements for the protective shell and fire safety than normal premises, and have access to uninterruptible supplies of electricity and cooling. For these secure areas, the following security measures must be implemented as a minimum:

- Access controls must include an alarm, staffed reception areas and/or computerised access control systems with individual passes and codes.
- Fire protection such as evacuation alarm and fire extinguishing equipment, must be present as appropriate. Combustible material must not be stored in secure areas.
- There must be an air-conditioning system to compensate for the surplus heat generated by the equipment.

Electronic equipment must be protected against power cuts and other disruption. Power supplies for business-critical[2] equipment and systems must be uninterruptible and connected to a backup power source. Tests must be conducted regularly to make sure that the transition to backup power works.

Protection of portable storage media and IT hardware

Business information that is handled outside KI's premises must be protected by means of adapted protective measures to counteract the risk of loss of or unauthorised access to information. This includes, among other things, laptops, mobile phones, USB sticks, paper documents, etc.

[2] Business-critical information means information that is classified in the two highest classes in any of the aspects confidentiality, integrity and availability. (For further information, see Chapter 4, Handling assets).

Storage media that contain sensitive information or licensed software must be physically destroyed or overwritten in a secure way in connection with disposal or reuse. It is not sufficient to use standard function to delete data. (Note: for physical security in respect of normal premises, please refer to the Security Unit's rules/instructions.)

7 Managing communication and operations

This information is aimed at those with responsibility for security and IT-security and to those responsible for certain information and also to system owners
Within Karolinska Institutet's organisation there is dependence on various IT systems and the information handled there, and it is therefore extremely important that these systems are available as required. At the same time, the information communicated and transmitted in KI's network must be protected so that unauthorised parties are unable to access it.

Basic security

Communication

When information is transmitted by means of data communication or telecommunication, there is a risk that the information transmitted may be accessed or modified. Each person responsible for information is responsible for analysing the need for necessary protective measures relating to the risk of information being accessed or modified, and for documenting these in a suitable way. The person responsible for information must communicate their needs to KI's Chief Security Officer, who is responsible for defining requirements in respect of the network. Further information is available in Appendix3.6, *Instructions on defining requirements for communication and network security*.

KI's network must be designed so that there are defined interfaces, both physical and logical, with other networks. Connections may only be made with other networks once the security aspects have been analysed and necessary protective measures implemented by each network's owner.

Information with a high confidentiality class (K3 and K4) under the current information classification model must never be transferred in such a way that unauthorised parties might access the information. This means that as a rule, transmissions via open networks must be encrypted.

All IT hardware that is connected to KI's network must be configured in accordance with the defined standard and there must be instructions for the handling of such hardware. Other computers that need to be connected to the Internet must be separated from KI's internal network and must be connected via a so-called guest network.

Operations

Production, development, test and educational environments at KI must be kept apart. The security rules for production environments must also apply where relevant to development and test environments.
The owner of a specific IT resource (system/application, network, technical platform, etc.) is responsible for defining requirements in respect of its reliability, which covers the following areas: security updates, change management, capacity planning, protection against malware, backup routines and restoration of data, and system and

operating documentation. There is further information about this in Appendix 3.7, *Instructions on defining requirements for reliability and service level*.

When KI buys services or outsources the operation of IT resources outside its own organisation, the same rules on information security must apply as when operation is carried out under its own auspices. Information security requirements must be defined on the basis of a documented risk analysis, and the requirements must be regulated in an agreement between the parties. The owner of each specific IT resource is responsible for defining requirements and following up on them, but there should be coordination in cases where the supplier is dealing with several of KI's IT resources. There is further information in Appendix 3.4, *Instructions on defining requirements for operations outside Karolinska Institutet.*

8 Management of access to information

Information for system owners
Access to information is important to conduct the daily operation atKarolinska Institutet.. At the same time, it is important that information is only accessible for those people who have an actual, authorised need for it. Sensitive information must be protected against unauthorised access and incorrect changes. It must therefore be guaranteed that access to information is only granted to authorised persons.

Basic security

There are many individuals, not only employees, students, contractors/associates and consultants in the organisation, but also to some extent suppliers, who have access to KI's information and information systems. Therefore, there must be methods and procedures in place to control all access to information, systems, networks and services. It is also important that everyone who has access to KI's information systems considers the information security aspects and understands his/her personal obligations when using systems and handling information.

Access to information within KI must be controlled by means of the administrative and technical protective measures described below.

Administration of access rights

To make sure that only authorised users of information has access to certain information (in both digital and physical form), access rights must be approved by an authorised person before they are granted to a user. The scope of access must be limited on each occasion to the user's current needs on the basis of his/her work and organisational affinity. Detailed instructions on how the ordering, registration, modification and deregistration of access rights are to be implemented must be defined and documented. See also Appendix 3.8, *Instructions on administration of access rights.*

Granted access rights must be reviewed on a regular basis and action taken to make sure that only users who are authorised at any given time have access to each information asset/system. For further information, see Appendix 3.9, *Instructions on reviewing access rights*.

Access control

All users must be identified and verified by means of a user name and password before they gain access to an information system. Strong authentication is required for access to information that has been classified at the highest level in respect of confidentiality. All users must have a unique identity and all user accounts must be traceable to a physical person.

Logging and monitoring

In order to make sure that all user activities are traceable, there must be logging of activities in all business-critical systems[3]. Detailed instructions and work methods for reviewing logs and how to deal with any breaches must be defined and documented. See Appendix 3.10, *Instructions on logging and examining logs.*

9 Acquisition, development and maintenance of systems

Information for system owners, system developers and procurement staff
Karolinska Institutet's systems and the information handled there are crucially important for the organisation. To make sure that business-critical[3] information is handled securely, it is important that the systems have the right functional and technical features. The security requirements must therefore be reflected in the systems and dealt with as early as in the planning of purchases or development of systems.

Basic security

Building security into systems while they are being developed is more cost-efficient and secure than adding security afterwards. When preparing to develop or procure a system, it is important to make sure that the various aspects of information security – confidentiality, integrity, availability and traceability – are considered. This is in order to ensure that security is an integral part of the system, which requires a structured approach and for the requirements in respect of information security to be clearly defined. A formal development method or a formal acquisition process that take this into consideration must therefore be used.

Comprehensive knowledge of the organisation's requirements (including requirements for the confidentiality, integrity, availability and traceability of the information) is important if the system is to be able to fulfil its purpose. The organisation's security requirements and legal requirements must therefore be formally confirmed and dealt with as a part of the development and acquisition process. All system development and acquisition of systems must be preceded by a risk analysis. The development or acquisition process must be approved by an appropriate body and consider as a minimum the following:

- mandatory authority requirements,
- internal rules in respect of information security,
- operationally stable, tried and tested solutions.

[3] Business-critical information means information that is classified in the two highest classes in any of the aspects confidentiality, integrity and availability. (For further information, see Chapter 4, Handling assets).

A strict, well-defined work procedure is required when new systems or developed system components are implemented from the development and test environment into the production environment. Only formally accepted, approved systems or system components may be implemented in the production environment. For further information, see Appendix 3.11, *Instructions on defining requirements when acquiring or developing systems.*

In order to maintain secure, reliable access to information, the administration, operation and maintenance of IT systems must be carried out in a structured, systematic way in accordance with a formalised, adopted model for system administration. The System Owner of each IT system is responsible for defining requirements in respect of system administration. For further information, see Appendix 3.12, *Instructions on defining requirements for system administration*.

10 Handling information security incidents

Information for those responsible for security and IT-security
An incident is an event that can have a negative effect on Karolinska Institutet's organisation. Information security incidents might be, for example, the loss of or unauthorised access to information, the theft of IT hardware or a virus outbreak, etc. To reduce the risk of an incident, it is important that everyone knows how to respond and whom to contact in order to report deviating events or information security incidents that have occurred.

Basic security

To make sure that any information security incidents (incidents) have a minimal impact on KI's organisation, there must be a formalised process for reporting and dealing with incidents. This process must guarantee that incidents and weaknesses relating to the handling of information are reported in such a way that appropriate action can be taken in both the short term and the long term.

Information security incidents are events that have, or may in future have, a negative impact on the security of KI's information assets. An incident can be caused by either an intentional or an unintentional action. The common denominator is that information security is threatened by, for example, unauthorised access to information, the illegal handling of data, an operational shutdown or a lack of access to information. Examples of incidents can include the unauthorised or unethical use of information, hacking or malware (virus). Additional examples are the loss of information in paper form or the loss of a computer or other storage media.

All those with an active role must be aware of what is classified as an incident and where and how these are to be reported. For detailed information about reporting incidents, see Appendix 3.13, *Instructions on the handling and reporting of information security incidents.*

Reported incidents must be classified in accordance with a defined model on the basis of the potential impact on information, individuals and the organisation. Incidents must be handled in order of priority with reference to the classification of the incident.

All reported incidents must be analysed, when they have been dealt with, in terms of their cause and effect. This is because there may be a connection between different incidents that is not immediately evident. A number of smaller incidents may, when viewed together, highlight major deficiencies in security that are difficult to identify without a comprehensive analysis. Identified deficiencies in security are defined as incidents and must be reported and dealt with as described above.

In the event of incidents that are considered to have the capacity for a major impact on KI's organisation, KI's Security Manager must be notified immediately so that KI's general crisis and emergency plan can be initiated, if this is considered necessary.

11 Continuity planning

Information for those responsible for security and IT-security
Access to Karolinska Institutet's information is a basic prerequisite for running the organisation. In the event of any disruption in access to information and system support, there must be plans and procedures in place to make sure that the organisation nevertheless can continue to operate.

Basic security

The main objective of continuity planning for KI's organisation is to make sure than any disruption in access to information and system support does not have serious consequences for the organisation. It must be guaranteed that potential risk, disruption and threats to the organisation's continuous operation have been evaluated and that appropriate measures have been taken. These measures must be clearly structured and organised in order that access to information and system support can be restored within a critical time as defined by the organisation. All parties concerned must know how, when and which measures to be taken when an incident in the form of a shutdown occurs. The focus on this part of continuity planning is on handling information and systems. The elements of continuity planning that relate to disaster and contingency situations must be included in KI's disaster planning.

Everyone with an active role within KI plays an important part in the business continuity planning.

The *University Director* is responsible for KI's overall continuity plan.

Heads of Department are ultimately responsible for making sure that analyses are conducted of each department and its operational processes, including important sub-components, as well as creating backup procedures to run the organisation in the event of an incident. This must be described in a continuity plan, which must also contain information about measures to return to normal operation.

The *Information Officer*, with the aid of the *System Owner*, is responsible for making sure that there is an established risk assessment and risk management process in place for systems in which information is handled, and that a continuity plan is developed and maintained for necessary areas.

The *Chief Security Officer* is responsible for defining requirements and for requesting continuity plans in respect of the infrastructure and its services, and for ensuring that these plans satisfy the organisation's defined requirements for restoration times.

Those *with an active role* must be aware of their responsibility in accordance with the current continuity plan within their own various areas of responsibility, which must be defined and agreed together with the Head of Department and the person's immediate manager. The level and scope of continuity planning must depend on the department's need for and dependence on each process or system to maintain its ongoing operations.

All operations and all IT systems are probably not equally critical for the organisation to run, and it is therefore quite possible to decide that certain systems should not be covered by a continuity plan and that resources and actions, in the event of an urgent situation, should instead focus primarily on more business-critical[4] activities and systems. These non-prioritised systems will then be dealt with only when the critical systems have been restored.

To achieve good continuity, a combination of preventive and corrective protective measures is required. During work to draw up continuity plans, a number of measures are often identified to reduce the risk of disaster situations, disruption and unplanned discontinuations from happening in the first place. In KI's operational activities that are extremely sensitive to disruptions, such preventive measures should be given a high priority. For further information, see Appendix 3.14, *Instructions on continuity planning*.

Continuity plans must be updated continuously and tested regularly, at least once a year, to make sure that they work, are appropriate and still reflect the current situation. Testing of the plans also serves as a training and communication initiative for the functions and roles concerned.

12 Compliance

Information for everyone at KI
Continuous control of compliance with current information security requirements is a prerequisite for maintaining a good level of information security within Karolinska Institutet. Understanding the importance of and complying with these requirements is absolutely crucial for handling KI's information and ultimately for the confidence in KI's organisation.

Internal follow-up on compliance will be adapted gradually, when the various parts of this information security framework are implemented.

Basic security

A correct understanding of defined requirements and conditions for all of KI's information security is required by all those with an active role if they are to observe information security in a good, effective way. Security requirements and protective measures need to be continuously evaluated in order to make sure that the level of

[4] Business-critical information means information that is classified in the two highest classes in any of the aspects confidentiality, integrity and availability. (For further information, see Chapter 4, Handling assets).

protection over time is correct in relation to identified risks. It is also important to make sure that defined security principles are being complied with and observed.

All *Heads of Department or equivalent* are responsible for making sure that the organisation is being run in accordance with these rules and instructions, and for reporting regularly on the organisation's compliance with the information security requirements to the Chief Security Officer.

A breach of current security rules can mean that those with an active role can lose their access rights to KI's IT systems. Decisions on this may be made by the Head of Department in consultation with the Chief Security Officer. More serious cases of abuse or other similar breaches of rules must be reported to the Chief Security Officer for further processing. Any suspicions of criminal activity will be reported to the police.

Information security relating to important operational processes, systems and the IT environment should be subjected to regular, independent audits. The results of these audits must be reported to the University Director and the management group/consistory. There must be a clear process for dealing with any deviations.

The design, operation and use of information systems may be subject to statutory, internally and externally regulated and contractual security requirements. It is the responsibility of every one in charge to make sure that current rules, regulations and laws are observed in the organisation. Advice on specific legal requirements must be sought from KI's legal advisors.

KI's Chief Security Officer is responsible for the information security framework, which must be reviewed every year and updated as required.
The purpose of this is to make sure that the rules cover any new risks and threats that have to be dealt with. It shall also ensure that suggested security solutions continue to be adequate and up to date.

The Chief Security Officer must compile a report every year for the University Director in respect of the organisation's work on information security.

Appendices

Appendix 1. Guidelines on information security

Appendix 2. Description of responsibilities

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

Appendix 3. Instructions

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