# Security Handbook

*Approved by the Information Security Committee and valid as of September 15, 2018.*

## Table of Contents

## 5 Information security policies

### 5.1 Guidelines for managing information security

### 5.1.1 Information Security Policies

**Publishing security policies**

Information security policies must be published and communicated to all relevant stakeholders, including all staff members.

### 5.1.2 Survey of Information Security Policies

**Revising security policies**

Security policies must be revised once a year as a minimum. The information security committee addresses this topic in May and sends proposals for new information security policies to the Rector for final approval.

**Definition of IT security**

Information security is defined as the sum of measures implemented to ensure confidentiality, accessibility and integrity. Such measures include technical, procedural, legal and regular control.

**Approval of security policies**

Information security policies, including any changes, must be approved in June each year by the Rector.

## 6 Organisation of information security

### 6.1 Internal organisation

### 6.1.1 Roles and responsibility areas for information security

**Security responsibilities for IT functions**

All critical IT functions which require special knowledge, skills or experience must be identified, and an operations manager must be appointed.

Security system owners responsible for business critical systems must be identified and be made aware of this responsibility. These owners must have the responsibility and authority to ensure adequate protection.

**Ownership**

All information assets must have a designated owner, who is responsible for classifying the individual asset and ensuring that protection is done according to the classification.

**Security Organisation**

The Executive Management will set up an information security committee (cf. terms of reference)

**Coordination of information security**

The Information Security Committee (ISU) is responsible for coordinating the overall information security. (http://www.informationssikkerhed.aau.dk/)

**The role of the management**

In order to ensure secure AAU information activities, placement of responsibility is necessary.

The management must support the AAU's information security by establishing clear guidelines, demonstrating visible commitment and ensure the accurate placement of responsibility.

The unit manager allocates resources for information security activities.

### 6.1.2 Functional separation

**Protection of business critical systems**

Functional separation should be implemented if the law requires this or if the unit management estimates this to be necessary to reduce the risk of unauthorized or accidental use, modification or misuse of AAU's confidential and critical information.

### 6.1.3 Contact with authorities

In the event of security breaches, a procedure must be in place for the handling of proof material and any contact with relevant authorities, including The Danish Data Protection Agency and The Danish Centre for Cyber Security.

### 6.1.4 Contact with special interest groups

The IT Department must keep informed about new vulnerabilities and threats as regards the platforms being used. This is done by establishing internal and external contacts for information and knowledge sharing and skill development

### 6.1.5 Information security in project management

**The project model must contain the following considerations regarding information security:**

The requirement specification must include the requirements for information security.

Identification of necessary security measures must be carried out using risk assessments etc.

Information security should be an integral part of project management.

## 6.2 Mobile equipment and remote workplaces

### 6.2.1 Policy for mobile equipment

**Access to mobile devices**

Users of AAU's mobile devices are responsible for protecting the data processed on them and the devices themselves. Access to information on mobile devices must be protected by access control. Mobile devices must not be left unlocked or unattended in unlocked rooms.

### 6.2.2 Remote workplaces

**Access from remote workplaces**

An encrypted connection must be used when a risk analysis dictates this.

Access is only granted to users authenticated by user name and password and possibly either a personal digital key or a physical token. (2factor)

**Protection of remote workplaces**

Remote workplaces and their communication links must be protected as regards the information and business systems for which they are used.

## 7 Staff security

### 7.1 Before appointment

### 7.1.1 Screening

**Background checks of employees**

The HR Department must ensure that the necessary background check is carried out of staff who are responsible for critical work areas.

**Verification of references**

The appointing authority is responsible for the necessary review and verification of the information provided by members of staff and applicants before appointments are made.

**Background checks of members of staff may include:**

A personal reference.

The applicant's curriculum vitae.

Educational and professional qualifications.

Identity checks (should always be conducted).

**Background checks of consultants**

Unit managers must ensure that the necessary background checks of consultants are carried out.

### 7.1.2 Employment terms and conditions

**Employment agreement**

The first time a person is registered as a user of AAU's IT assets, they must be informed about the rules that apply to the use of AAU's IT assets ("Rules concerning the responsible use of IT at Aalborg University" and an "IT code of conduct for staff and students" can be found on the website https://www.informationssikkerhed.aau.dk/english/)

An email for the user will be automatically generated, including a link to https://www.informationssikkerhed.aau.dk/english/

**The employment agreement should include and elaborate:**

The legal responsibility and rights of the employee.

The employee's responsibilities in connection with information processing.

Information about AAU’s treatment of personal data regarding the employee, cf. the Danish Data Protection Act, part 8.

Accountability when working outside of AAU’s premises or outside of normal working hours, e.g. when working from home.

A description of the action that will be taken if an employee ignores the employer’s security requirements.

### 7.2 During appointment

#### 7.2.1 Managerial responsibilities

The information security at AAU depends largely on the employees. Employees must therefore be trained in information security in relation to their job function and receive necessary information.

**The management is responsible for ensuring that all employees:**

remain sufficiently informed about their roles and responsibilities relating to security before they are assigned access to AAU's systems and data,

are made familiar with the necessary guidelines, enabling them to comply with AAU's information security policy,

achieve a level of awareness of issues relating to information security which is consistent with their roles and responsibilities at AAU,

remain within the guidelines and rules applying to their position, including AAU's information security policy and concrete working methods.

gets knowledge about how information is classified.

#### 7.2.2 Awareness of and training in information security

**Training in security policy**

All new employees receive a link to AAU’s information security policy on their first work day at the latest.

All employees must read the information concerning AAU’s information security policy.

All employees currently receive instructions of how to comply with and study AAU’s Information Security Policy.

Unit managers are responsible for providing new IT users with an introduction to AAU's IT code of conduct etc. Before users are given access to IT assets, they must be adequately instructed in log-on and log-off procedures, the use of applications etc.

**Security training for IT staff**

All IT staff must be trained specifically in aspects of security in order to minimise the risk of security incidents.

When employed, IT staff must be made aware of the information security handbook and its annexes and supplementary guidelines.

#### 7.2.3 Sanctions

The management must establish a formal procedure for employees who violate AAU’s policies, rules or guidelines for information security.

It is management's responsibility that sanctions for the violation of AAU's information security policies, rules or guidelines are implemented in accordance with the legislation in force.

Violation of the information security policy are sanctioned in the same manner as other violation of AAU's policies and rules (reprimand, warning, dismissal, withdrawal of the right to use AAU's networks, eviction and in certain cases reporting to the police.)

### 7.3 Termination of or changes in employment

#### 7.3.1 Termination of or changes in employment

**Information on private equipment, termination of employment**

The employee must hand over all information and assets provided by AAU upon termination of employment. The employee must also delete the company's information from private equipment at the end of the employment. HR must, in cooperation with IT, create and maintain a procedure for withdrawing privileges in relation to changes in the employment relationship, resignation or dismissal of staff.

## 8 Management of assets

### 8.1 Responsibility for assets

#### 8.1.1 List of assets

An overview of AAU's critical and sensitive information assets must be available, which at the same time deals with legal requirements regarding records of personal data

#### 8.1.2 Ownership of assets

**Security responsibility for information assets**

The unit head must appoint a security officer. The security officer is responsible for maintaining a list of information assets. The list must specify the data and system owner of each asset.

**Preparation of an overall risk assessment**

The necessary information security measures are determined on the basis of risk analyses.

The unit management is responsible for preparing risk assessments of the unit's critical IT assets. The assessment should elucidate any threats that might exist, the probability that threat incidents might occur and the possible consequences.

Risk assessments must be updated at least every two years and must be carried out by the individual unit in cooperation with the information security manager.

All the material in combination represents AAU's overall risk assessment.

**Risk analysis**

The unit manager is responsible for preparing and documenting a risk analysis of all critical systems.

#### 8.1.3 Accepted use of assets

**Accepted use of information assets**

An "IT code of conduct for staff and students" has been prepared. This code describes procedures and general guidelines for IT user conduct (visit https://www.informationssikkerhed.aau.dk/english for more information)

### 8.1.4 Return of assets

All users must return all AAU assets in their possession when their agreement with AAU terminates.

## 8.2 Classification of information

### 8.2.1 Classification of information

All employees should be aware of how information is classified. To ensure the confidentiality of information, a classification model has been prepared after 4 levels:

0. Public: Information that is available to the public or where disclosure does not harm AAU.
1. Internal: Information that only users, with a purely work-related need, must and can access, but where a breach of confidentiality will have a low harmful effect for AAU, private individuals or business partner(s).
2. Confidential: Information that only users, with a purely work-related need, must and can access, and where a breach of confidentiality will have a medium harmful effect for AAU, private individuals or business partner(s).
3. Sensitive: Information that only users, with a purely work-related need, must and can access, and where a breach of confidentiality will have a high harmful effect for AAU, private individuals or business partner(s).

Regardless of the level of classification, access control can be implemented for information at several levels.

**Definitions of roles related to the classification, processing and use of data:**

- **Data owner:** The person responsible for the classification of data as well as ensuring that protection is done according to the classification.
- **Administrator:** Person or organization who, on the basis of the data owner's classification and instructions, manages access to data.
- **Data Processor:** Person or organization that processes data on behalf of the data owner and according to his instructions.
- **User:** Person or organization using data.

### 8.2.2 Labelling of information

**Responsibility for classification**

The owner of the asset is responsible for the classification of this. (A, B or C-active)

**Responsibility for access rights**

The asset owner is responsible for establishing and continually reassessing access rights.

**Classification labelling**

AAU's information must be identified and classified in accordance with the rules of classification.

#### 8.2.3 Management of assets

**Control of classified information**

The Information Security Committee is responsible for defining a fixed set of adequate and appropriate security control measures to protect the individual information categories.

### 8.3 Media management

#### 8.3.1 Management of portable media

**Storage and registration of data media**

The information owner must ensure that the media or the information on the media are classified, and that users are instructed to store the media in accordance with the rules applying to the classification.

**Use of data media**

The selected data media must be able to protect the information in accordance with its classification.

**Use of portable media for confidential data**

Data media must be protected against loss and misuse, cf. the basic rules for mobile devices.

Sensitive (personal data) information must be encrypted when stored or transported on portable media, such as USB memory sticks, tablets, mobile phones, DVDs or floppy disks.

#### 8.3.2 Disposal of media

**Disposal and reuse of media**

All data media, for example hard disks, floppy disks, CDs, DVDs, tapes and memory devices must be security deleted or destroyed before disposal if they contain data that are not classified as "Public".

#### 8.3.3 Physical media during transport

All data media, such as hard drives, floppy disks, CDs, DVDs, tapes, and memory devices containing confidential or sensitive data must be encrypted. The current encryption requirement is at least 256 bits of AES encryption.

## 9 Access management

### 9.1 Business requirements for access management

Password requirements should be determined by the sensitivity and classification of the data and the systems to which access is given. Ideally, a layered security policy model should be established, implying that the closer an employee gets to 'the gold', the stricter the access control will be.  For instance, if access is granted to the Internet only, i.e. to publicly available data and systems, it is not necessary to have the same rules regarding username/password as when access is granted to confidential and sensitive information and systems internally at AAU.  However, at present, AAU is not able to implement such a model, therefore the policy below will apply at AAU for the time being.  The rules should be regarded as minimum requirements, and individual systems and data owners are allowed to introduce a stricter policy in case a risk assessment requires this.

#### 9.1.1 Policy for access management

**Limited access to information**

Access for users and support staff to the functions and information of user systems must be limited in accordance with the established business-related requirements and the classification of information.

**Withdrawal of privileges when employment is terminated**

An updated procedure must be in place regarding the withdrawal of privileges in case employment is terminated by resignation or dismissal.

The unit management is responsible for informing IT asset owners of any changes in the work tasks of employees (including dismissal or resignation), in order that privileges can be adjusted/withdrawn.

### 9.1.2 Access to networks and network services

**Network monitoring**

The network group is responsible for continuously monitoring the use and safety of AAU's network infrastructure.

It is recommended that automatic monitoring systems are used.

**Guidelines for the use of network services**

Users should only have access to the services they are authorised to use.

**Access to wireless networks**

Students, staff and guests have the option of using the wireless network at Aalborg University. Read more at https://www.en.its.aau.dk/instructions/wifi/

**Separation of networks**

In order to improve the operational reliability of critical servers, separate server networks with a strict filtering policy should be established.

Separate networks should be established for equipment in different "risk groups", e.g. private computers, university computers, printers.

**Management of network access**

Only authorised users and devices may have access to the network at AAU.

**Authentication when accessing the network**

Access to the internal network from other locations than AAU premises must be protected in accordance with the applicable risk assessment.

## 9.2 Administration of user access

### 9.2.1 User registration and de-registration

**Identification and authentication of users**

All users must have a unique identity for personal use.

An appropriate authentication technique must be used for the verification of user identity.

The user identity must be traceable to the person who is responsible for a particular activity.

Shared user identities must be avoided where possible.

### 9.2.2 Assigning user access

**Allocation of user rights**
The data owner is responsible for ensuring that the individual user is given precisely the user privileges that the user's work tasks warrant.

**Guidelines for access control**
Administrator is responsible for the ongoing registration, management and monitoring of the allocation and use of privileges according to the data owner's classification of information.

**Access restriction for information**
Applications must ensure that access to information takes place according to a well-defined access policy.

### 9.2.3 Managing privileged access rights

**Administrator protection**

Passwords must be used at all times for access with system administrator privileges.

**Extended access rights**

Extended access rights may be granted only to a limited extent and only on the basis of work-related needs.

Extended access rights must be registered.

Extended access rights must not be put into effect until the requisite authorisation has been obtained.

Whenever possible, automated system engineering processes must be used in order to limit the need for granting extended rights.

Whenever possible, individual user programmes must be organised so as to curb the need for intervention with extended rights.

Special user identities must be used for the extended rights for the sake of monitoring and follow-up.

**Change of administrative passwords**

Administrative passwords must be changed in case of suspicion that outsiders have come to know these, or when administrators leave the unit.

**Change of administrator password in case of resignation**

When a person who knows the administrative passwords resigns, such passwords must be changed immediately.

### 9.2.4 Managing secret authentication information about users

**Storing passwords**

Passwords should never be stored electronically in plain text.

### 9.2.5 Review of user access rights

**Review of user profiles**

All user profiles must be reviewed at least once a year to identify inactive profiles or other content which should be removed or modified.

**9.2.6 Withdrawal or adjustment of access rights**

**User profiles**

Guests and external consultants may only be created as users with time limited access. Under normal circumstances, the time limitation must not exceed 12 months prior to renewed approval.

Users are only granted access to AAU's IT assets on the basis of work or study related needs.

Return of assets when resigning

The employee must return all AAU assets when terminating their employment.

**Resignation**

When employment periods or temporary contracts expire, all associated rights must be assessed and adjusted, if necessary.  ID cards etc. must be returned, and IT equipment must be called in.

**Relocation of employees**

Assigned access rights and privileges must be reviewed in when employees resign or are relocated. Unit managers are responsible for establishing procedures for this.

**Registration of users**

Users must have a unique user name and user ID.

The system owner must authorise user access.

Access rights must be adjusted to 'need to have' in accordance with work function and the organization needs.

It must be verified that the rights level is consistent with AAU's general security guidelines.

The service supplier must use a similar or the same authorisation procedure as AAU.

The system owner must maintain user records of the system.

AAU must maintain records of how users or user rights are removed or changed upon the termination or modification of the job functions of users.

Access rights must not infringe on any requirements of function segregation.

The procedures must apply to the entire period during which access rights are applicable, i.e. from the registration of a user to the formal cancellation of a user who no longer has a work or study related need for access.

Every effort must be made to ensure that the user has the same identification in all the IT systems to which the user has access.

Shared ID for a group of employees should be avoided to the widest extent possible.

### 9.3 User responsibilities

#### 9.3.1 Using secret authentication information

**Selecting secure passwords**

Users must follow good security practices when selecting and using passwords. Passwords should be chosen which are easy to remember and difficult to guess.

**Requirements for the change of password**

Passwords must be changed whenever it is suspected that others have come to know these.

Passwords must be changed at least every six months. (March 2015)

For data that is protected by more qualified access control (where the access control implies more than just username/password),the  frequency of password change can be changed by agreement with the information security committee (via the information security manager).

**Requirements for password length**

User passwords must contain at least 8 characters and at least 3 different types of characters (e.g. uppercase and lowercase letters and numbers).

Passwords for administrators must contain at least 10 characters and at least 4 different types of characters (uppercase letters, lowercase letters, numbers, or special characters)

**Reuse of passwords**

Users must not use the same password on the AAU systems as they use on external systems.

**Passwords are strictly personal**

Passwords are strictly personal and must not be shared with others.

However, students may use the following web solution options to retrieve their AAU emails: gmail.com, hotmail.com, outlook.com.

**Guidelines for passwords**

In connection with user creation of passwords or the resetting of passwords, a secure temporary password must be assigned to the user; this must be changed immediately after it was used for the first time.

Prior to assigning a new temporary password, a procedure must be established and maintained as to how a user's identity is established.

Temporary passwords must be unique, must not be reused and must meet the general requirements for passwords.

**Protection of critical data**

Following installation of a new system, the standard passwords for this must be changed.

### 9.4 Managing system and application access

#### 9.4.1 Limited access to information

#### 9.4.2 Procedures for secure log-on

**Secure log-on**

System access must be protected by a secure log-on procedure.

#### 9.4.3 System for the administration of passwords

**Systems for password management**

To the extent possible, IT systems must ensure that the requirements for passwords are met, and that passwords are not reused within an established history, e.g. the 20 most recently used.

**Implementation of a system for password management**

A password management system for critical systems that enforce the password rules of the university must be implemented.

#### 9.4.4 Using privileged system programs

**Using system tools**

All use of system tools must be logged.

The IT Department must ensure that the use of system tools (e.g. utilities that can affect or bypass systems or unit security) is limited to a minimum number of trusted and authorised users.

#### 9.4.5 Management of access to program source codes

**Access control for source text**

Source text for applications in a development process must be protected by access control systems to ensure integrity.

**Controlled access to the source code**

The source code for development projects must be protected against unauthorised access. Changes must be controlled to ensure integrity.

Any printouts of source codes must be stored safely.

## 10 Cryptography

### 10.1 Cryptographic controls

#### 10.1.1 Policy on the use of cryptography

**Encryption of files**

It should be considered to protect files including data classified as "Secret" using cryptography.

**Approval of encryption products**

Only cryptography using recognised encryption methods may be used.

**The use of encryption in connection with the storage of data**

Confidential information should always be encrypted when stored on portable equipment such as laptops, handheld computers, etc. (Please note a separate policy for mobile devices has been published.)

### 10.1.2 Administration of keys

**Management of keys**

The procedure for key management should describe how the generation, distribution, storage and destruction of keys are managed.

## 11 Physical protection and environmental protection

Physical security includes doors, windows, alarms, video surveillance - and theft protection of the University's physical assets, such as IT equipment. In addition, there are access control systems which are also an element of physical security and which to some extent ensure that only persons with legal purpose have access to the University's area at the times when the system is switched on.

## 11.1 Secure areas

### 11.1.1 Physical perimeter protection

**Intruder alarms**

Most AAU areas have established shell security, and agreements are in place with a security company concerning surveillance and on-call service/emergency response in case of an alarm.

### 11.1.2 Physical access control

Physical protection and access rules form part of AAU’s security policy. Access control systems are elements of physical protection which ensure that only individuals with a legitimate purpose gain access to AAU’s premises.

**Access Card**

Access control cards are personal. They must be stored securely and may not be transferred to third parties.

### 11.1.3 Protection of offices, premises and facilities

**Protection of offices, premises and equipment**

Offices and other rooms where sensitive data are stored must be lockable.

**Information about secure areas**

Information about the secure areas and their function may only be given if a work-related need exists.

### 11.1.4 Protection against external and environmental threats

**Fire protection**

Server rooms must not be used as storage rooms for flammable materials.

It is recommended that automatic fire-fighting equipment is established in or beside engine rooms.

Automatic fire-fighting and fire-alarm equipment must always be established in rooms containing IT and other assets amounting to more than DKK 700,000, year 2018 price level.

**Environmental protection of server rooms**

Server rooms, wiring closets and corresponding areas must be secured adequately against environmental events such as fire, flooding, explosion etc.

### 11.1.5 Work in secure areas

**Locking of premises and buildings**

All doors and windows with access to/from the buildings must be closed and locked when work is terminated. Doors to secured areas in the buildings must also be locked.

### 11.1.6 Areas for loading and unloading

**Areas for loading and unloading**

Deliveries must be recorded according to the goods reception procedure.

## 11.2 Equipment

### 11.2.1 Placement and protection of equipment

**Locking of wiring closets and other technical rooms**

All wiring closets and technical rooms must remain locked.

**Access to server rooms and main wiring closets**

Access to server rooms and main wiring closets is described in the annex concerning "Access to technical rooms”

**Lending of access cards and/or keys**

Access to secured areas can be temporarily assigned to craftspeople, technicians and others, providing all rules concerning access are complied with.

**Access for service suppliers**

Service suppliers may only get access to secure areas when this is imperative and their access is monitored.

### 11.2.2 Supporting supplies (supply security)

**Back-up power units**

The risk assessment available for critical IT assets must include an assessment regarding the use of back-up power units (UPS).

**Supply security**

Data communication must be secured through the establishment of redundancy and strategic placement of the equipment and lines, in order to avoid the "single point of failure".

### 11.2.3 Securing cables

**Securing cables**

Data communication cables must be protected against unauthorised interference and damage. Care must be taken to ensure that ground cables are registered with relevant stakeholders.

Fixed cables and equipment must always be labelled clearly and unambiguously.

Documentation must be updated when cabling is changed.

### 11.2.4 Maintenance of equipment

**Maintenance of equipment and installations**

System owners should maintain equipment in accordance with the supplier's instructions.

Only qualified suppliers may carry out repair and maintenance work.

When equipment is repaired or maintained in locations outside of the AAU, such repair activity must comply with the appropriate security requirements.

Critical/sensitive information must be deleted from equipment that is repaired or maintained outside of the AAU.

System managers are responsible for maintaining a log of all errors and omissions as well as repair work and preventive maintenance.

### 11.2.5 Removal of assets

**Removal of assets from AAU**

Unit managements determine the rules applying to authorised removal of IT assets.

### 11.2.6 Securing equipment and assets outside of the organisation

**Supervision of mobile devices**

Mobile devices must not be left unattended in unlocked rooms.

Portable equipment must be configured in accordance with the AAU rules in force regarding mobile devices.

### 11.2.7 Secure disposal or reuse of equipment

**Disposal or reuse of equipment**

All IT equipment containing storage media such as fixed hard drives in workstations, servers and photocopiers must be checked before removal to ensure that all data (not classified as public) as well as licensed and personal user programs have been deleted.

### 11.2.8 Unsupervised user equipment

**Placement of equipment**

Portable computers etc. left unsupervised in an office (e.g. after working hours) must be placed in a locked cupboard or the like to ensure that it is not immediately visible from the outside.

Equipment must be placed or protected so as to minimise the risk of damage and unauthorised access.

Equipment used to treat critical/sensitive information must be placed so as to insure that  information cannot be extracted by any unauthorised person.

### 11.2.9 Policy regarding tidy desks and blank screens

**Storage of physical documents**

Documents with personally identifiable information must be stored in a locked cabinet or drawer after working hours.

Desktops (physical) should be cleared of confidential documents when the work day ends, at the latest.

**Use of password-protected screen saver**

Users must activate the password-protected screen lock when abandoning their workstation.

The system must activate the password-protected screen lock on computers after 15 minutes of inactivity, as a maximum.

**Printing**

Print queues etc. with sensitive content must be secured against unauthorised access. Users must ensure that sensitive printouts are retrieved as soon as possible.

## 12 Operational reliability

### 12.1 Operating procedures and areas of responsibility

### 12.1.1 Documented operating procedures

**Protection of server systems**

All servers must be secured and approved before release to production.

**Documentation**

The unit management must ensure the existence of clearly defined operational procedures for all critical IT assets in production.

**Operational responsibility**

The IT Department is responsible for the operation and administration of IT systems and their security. This includes compliance with security policies, rules and procedures.

**Operational procedures**

Operational procedures must be documented, updated and made accessible for operational staff and others with a work-related need.

**Registration of operating status**

Major disruptions and irregularities in the operation of systems and the reasons for these must be recorded.

**Protection of diagnostic and configuration ports**

Physical and logical access to diagnostic and configuration ports must be controlled.

Access to remote diagnostics and maintenance (including special diagnostic ports, console switches, out-of-band management etc.) must be secured against unauthorised use.

Procedures for the access of external suppliers to remote diagnostics must be outlined by the owner of the IT assets.

Any use of diagnostic ports should be logged.

### 12.1.2 Change management

#### Change management

The IT Department has decided to establish change management with inspiration from ITIL; the rules below are examples of this.

When changes are made, a review must be carried out of security measures and integrity controls in order to ensure that these are not reduced as a result of the implementation.

Prior to the implementation of changes, approval must be obtained from the system owner.

The system documentation must be updated at each change.

Obsolete system documentation must be filed or destroyed.

Version management must be maintained for all system changes.

A log of all changes must be maintained.

To the extent possible, a test of the operational functionality must be conducted before changes are implemented.

#### Planning, testing and approval of changes

Changes must be planned and possibly tested before they are made operational.

The consequences of the changes must be assessed prior to implementation.

Changes must follow a formalised procedure prior to implementation.

#### Guidelines for changes

Changes must only be carried out when a justified need exists.

The IT Department is responsible for ensuring that unambiguous identification and registration of significant changes takes place.

Information about implemented changes must be communicated to stakeholders.

The IT Department is responsible for the existence of an emergency procedure to reduce the effect of failed changes.

### 12.1.3 Capacity management

#### Capacity planning

The dimensioning of IT systems must be adjusted according to capacity requirements.  Strain must be monitored to ensure that upgrading and adjustment take place currently. This applies in particular to business critical systems.

**Capacity monitoring**

All server systems must be monitored in order to ensure sufficient capacity, reliable operation and accessibility. Major deviations from the normal capacity must be recorded and handled as incidents.

### 12.1.4 The separation of development testing and operating environments

**Protection of application development environments**

Development environments must be secured against threats such as unauthorised access, changes and loss. Data must be secured according to their classification.

**Access to production data**

The access of system administrators to confidential information must be curbed.

**The separation of development, testing and operating**

Development and test environments should be separated from the operating environment, physically or in terms of system engineering.

## 12.2 Protection against malware

### 12.2.1 Controlling against malware

**Requirements for antivirus on computers**

All computers must use an up-to-date antivirus program, or be protected in a similar way by other methods. This also applies to personal computers, which are connected on the AAU network. Protective measures against Spyware and other Malware must be used wherever necessary.

## 12.3 Backup

### 12.3.1 Backup of information

**Backup of data in server systems**

A backup procedure/guide must be prepared for the backup of all essential data, programmes and parameter configurations.

The IT Department is responsible for the safe storage and backup of data on server equipment.

The IT Department is responsible for the storage and backup of all business-critical information on server systems.

Backup must be accurate, complete and include documented restore procedures.

The volume and frequency of backup must reflect the current business and IT needs.

Backup data must be protected by appropriate logical and physical access control.

Backed up data must be tested regularly to ensure that data can be restored correctly.

Backup data must be stored off-site in order to ensure redundancy in the event of a disaster.

**Monitoring of backup procedures**

The ability to recover data from backup systems must be tested at regular intervals. Moreover, data recovery must be tested following system and process changes which may affect backup routines.

**Emergency plans for backup**

All critical systems must have an emergency plan for backup to ensure that the risk of data loss is minimised.

**Storing backups in an external location**

Data media for the recovery of critical systems must be kept in a secure storage place located at an appropriate distance from the production data.

## 12.4 Logging and monitoring

### 12.4.1 Incident logging

**Incident logging**

All production systems must log information about access and attempts at access in order to be able to track any unauthorised activity.

Logs must be reviewed regularly, preferably using automated tools.

All security incidents must be logged and retained for a fixed period of time to enable follow-up on access controls and possibly investigation of errors and abuse.

The IT Department is responsible for configuring the systems in such a way that relevant information is logged and saved for later use if needed.

**Storage of follow-up log**

AAU’s rules for logging must comply with the Danish legislation in force.

**Monitoring Internet use**

AAU reserves the right to filter, log and limit the use of networks, including the Internet, to the extent necessary in order to ensure smooth operations.

### 12.4.2 Protection of log information

**Protection of log information**

Log files may contain information which must not be publicly accessible.

Log facilities and log information must be protected against manipulation and technical errors.

All log records must be protected from unauthorised access through the use of access control systems, physical separation or network segmentation.

Log records must be immediately transferred to a centralised log server or to a safe media, which is not easily modifiable.

Only individuals whose work requires this may obtain access to the logs.

### 12.4.3 Administrator and operator log

**Monitoring of service supplier**

The IT Department must regularly monitor service providers, review the agreed reports and logs and perform actual revisions in order to ensure that the agreement is complied with, and that security incidents and issues are adequately handled.

**Administrator log**

Logging must be carried out of all actions performed by individuals with administrator rights in connection with critical system components in operation (including network equipment).

### 12.4.4 Time synchronisation

**Time synchronisation**

It required that all equipment (servers, personal computers, network equipment) that delivers a log according to the rules on logging synchronise their clocks to NTP.

## 12.5 Control of operation software

### 12.5.1 Software installation on operation systems

The maintenance and updating of IT systems is necessary in order to maintain an adequate level of security for AAU. The operation of IT systems includes elements of the monitoring of system health as well as the updating and backup of data. Most contemporary IT systems are dependent on networks, and this is why the administration, construction, security and maintenance of networks are vital for AAU. The threat caused by unauthorised access makes it necessary to have clear rules for the use of AAU’s networks and the monitoring of the infrastructure.

## 12.6 Vulnerability management

### 12.6.1 Management of technical vulnerabilities

**Changes for operating systems and application program packages**

The IT Department must continuously assess the accessible security patches, e.g. patches or hot-fixes for operating systems and applications in use. Deployment and installation of critical security patches on relevant systems must be carried out as soon as possible and normally within a week of the assessment and the positive functionality and compatibility test.

**Major operating system updates, e.g. "service packs"**

When major updates such as "service packs" are made accessible by suppliers, the IT Department must assess whether to install these.

Updates in critical systems must be tested thoroughly regarding compatibility with commonly used applications before the updates are installed in the production environment.

**Software updates in general**

The IT Department must keep informed of program patches for programs used at the AAU and must install these as soon as possible on all computers, e.g. servers and workstations, when it is estimated that the patches have a positive influence on the overall security level.

The IT Department must carry out installation of all major patches, when it is assessed that these have a positive influence on the overall security level.

System owners are responsible for ensuring that regular updates of the software in use are carried out.

**Changes in critical systems**

All changes in critical systems must be carried out in accordance with the approved procedure. All procedures must include an alternative plan for restoring the critical system. The conditions for the activation of the alternative plan must also appear from the procedure.

## 12.7 Considerations regarding the audit of information systems

### 12.7.1 Controls regarding the audit of information systems

**Security in connection with audits**

Auditing requirements and auditing procedures regarding systems in operation must be carefully planned and agreed upon with the parties involved in order to minimise the risk of disruption of AAU's business activities.

The planned auditing activities may only include reading access to systems and data.

If the audit necessitates more than reading access, this must only be permitted on copies of the affected files, which must be deleted after use.

All access in the event of auditing must be logged.

The individuals performing the audit must be independent of the audited area.

**Protection of auditing tools**

Access to auditing tools must be limited in order to prevent abuse.

# 13 Communication security

## Management of network security

### 13.1.1 Network management

**Installation of network equipment**

Installation of network equipment must be coordinated through the network group.

**Setting up wireless access points**

Wireless networks may only be set up in agreement with the central network group.

**Connecting equipment to the network**

The IT Department must draw up and publish rules for the connection of equipment to the local network.

**Incoming network connections**

It is recommended to split the local network in zones, maintaining a well-defined filter policy between the zones. The filter policy must ensure that access will only be opened to necessary services and resources (servers, PC's etc.). Filtering can be carried out centrally or locally.

**Securing networks**

The network group carries the overall responsibility for protecting AAU's network.

**Using the wireless local network**

Students and employees at Aalborg University are recommended to use the wireless network AAU-1 x. Read more about wireless networks at https://www.en.its.aau.dk/instructions/wifi/

**Installation of wireless equipment**

A wireless network (access points) must only be set up on campus following prior agreement with the IT Department's network group.

**Access to the network**

Access to AAU's network may only take place through approved security solutions.

**Access to data in AAU networks**

Access to data in AAU's network must take place through the security-approved solutions and in accordance with the classification of the data.

**Storage of confidential information on private equipment**

Handling or storage of personally identifiable or confidential information on equipment that does not belong to the AAU must adhere to the rules described for data classification.

### 13.1.2 Securing network services

**Using encryption in connection with data exchange**

Emails and data containing confidential information must always be encrypted during transmission to recipients outside of the AAU.

**Internet-based services**

It is allowed to use Internet services that do not involve increased security risks.

**Remote control and administration**

Connections for remote administration to be used for maintenance and support tasks must only be activated when necessary and at the request of the user and/or system owner.

## 13.2 Information transfer

### 13.2.1 Policies and procedures for information transfer

**Forwarding of confidential information and notifications**

Information that is not classified as "Public" must not be forwarded to third parties in any form without the approval of the information owner.

Subject access requests should be referred to the Management Secretariat (represented by the Rector/AAU Director)

**Encryption of administrative network connections**

Network connections used for the administration of IT equipment must be encrypted, if possible.

**Procedures for information exchange**

The individual unit manager is responsible for ensuring that guidelines and procedures are available for any critical form of information exchange, physical as well as electronic.

**Printouts**

Users must collect printouts with sensitive content as soon as possible. (It is recommended to use the Follow-You print system for printouts that others should not see)

**13.2.2 Agreements regarding information transfer**

**Agreements regarding information exchange**

When information and software are exchanged between AAU and a third party, AAU's rules concerning data classifications must be complied with.

**13.2.3 Electronic messages**

**Electronic exchange of mail and documents**

If emails are used for binding external agreements, they should be signed using a digital signature (employee certificate, which can be ordered via support@its.aau.dk)

**Authentication**

Users should be aware that communication via social services on the Internet can be unsecure, and users will rarely or never be certain who they are communicating with.

**Attachments**

The IT Department can choose to block file types deemed dangerous or inappropriate.

**Phishing and fraud**

Users should be aware of "phishing" and "social engineering", which may mean, for instance, that they receive apparently genuine emails which are trying to con personal or confidential information from users or to get users to perform unwanted actions.

**Confidential mail**

Emails with confidential or secret content sent to external recipients must be encrypted using a recognised method.

**Employees' private use of email**

Employees may use the email systems for personal use to a limited extent if this has no effect on the operation and security of the AAU in general.

Private emails should be saved in a folder with the word 'private' included in the folder's name.

**AAU’s information on social networks**

Only public information may be shared on an external social network.

**Private use of the Internet access**

AAU's Internet access may be used for private purposes, provided that the security policy is complied with, and that the work-related use is not hampered in any way.

**Processing personal data:**

The processing of personal data is described in a separate annex.

The procedure for the unintended publication of information on the Internet is described in a separate annex.

**Storage and deletion of emails**

Emails that contain personally identifiable information must be processed in accordance with the Danish Data Protection Act.

**Integrity of messages**

If the integrity of a message needs to be verified, it may be required that an employee certificate or a similar solution is used for signing such messages.

**Spam mail protection**

The AAU filters out emails that meet the AAU’s criteria concerning spam mails.

### 13.2.4 Confidentiality and non-disclosure agreements

**Content of non-disclosure agreements**

The information security manual contains a non-disclosure agreement template.

**Third party non-disclosure agreement**

The unit manager must ensure that a third party who has access to systems and data is subject to the requirements concerning confidentiality.

# 14 Acquisition, development and maintenance of systems

## 14.1 Security requirements for information systems

### 14.1.1 Analysis and specification of information security requirements

**Security in application development**

Security must be included as an integral part of all development projects.

**Acquisition procedures**

The unit manager must ensure that new acquisitions do not conflict with existing requirements in adopted policies.

Acquisitions which may cause an increased risk of security incidents are subject to the acceptance of the management.

### 14.1.2 Securing application services on public networks

**Securing applications on public networks**

Secure authentication and authorisation processes must be used to secure service transactions across public networks

Data integrity and confidentiality must be secured when using application services across public networks For example:

Securing integrity (such as hashing)

Cryptographic solutions (such as SSL, SFTP, HTTPS, secure API's or web services)

### 14.1.3 Protection of commerce applications and services

**Online transactions**

Systems offering external users the possibility of direct updating in AAU's databases must be subject to special security measures in order to prevent transmission errors, misdirection, manipulation and unauthorised access and repetition of transactions already undertaken.

**Electronic commerce**

Information concerning electronic commerce through public networks must be protected against fraud, contract disputes, unauthorised access and changes.

In order to secure its e-commerce, AAU must launch a variety of different security measures. On a general level, a set of trade terms should always be accessible, understood and accepted by the customer. These should state how authenticity is determined, who sets prices, and what requirements apply regarding confidentiality, integrity and non-repudiation. The protection should apply to the exchange of information as well as the systems used to store or process data.

## 14.2 Security in development and auxiliary processes

### 14.2.1 Secure development policy

**Validation of input**

Data that are sent into the systems must be validated for correctness.

Periodic review of key data must confirm their validity and integrity.

It is tested whether data seem plausible before they are sent into the systems.

Logs must be generated of the activities that send data into the system.

Data validation must protect IT activity against input errors. Input data such as date formats and personal identification numbers must be validated to ensure that they meet the formal format requirements.

**Database integrity**

It must be assessed whether the data update procedures used secure data integrity.

### 14.2.2 Procedures for the management of system changes

### 14.2.3 Technical review of applications following modifications of operating platforms

#### Review of systems following modifications

Before changing operating environments, critical business systems need to be reviewed and tested to ensure that it does not have unintended derivative effects on AAU's daily operations. For externally accessible systems and especially critical systems, it must always be considered from a risk assessment whether an actual penetration test via external independent third party must be performed.

### 14.2.4 Restriction of changes in software packages

#### Changes in standard systems

Changes in externally supplied systems must be restricted to the necessary changes, and such changes must be carefully controlled.

Built-in security measures, for example logging and access and integrity control, should be reviewed to ensure that they are not compromised.

It must be assessed to what extent the AAU will be responsible for the future maintenance of the software.

### 14.2.5 Principles for the development of secure systems

#### Security requirements for information processing systems

AAU's requirement specification for both new and existing systems must include information security which must be aligned with the system's risk assessment.

#### Security in system planning

When scheduling systems, security issues must always be included in the considerations.

IT security requirements must be taken into account in the design, testing, implementation and upgrading of IT systems, as well as in systems changes.

#### Specification of security requirements

All new assets/systems must be classified (A, B or C-asset), and critical assets must be risk assessed.

#### Control of internal data processing

Validation and adaptation controls must be incorporated into the IT asset in order to detect inconsistencies and ensure data integrity. The level of control depends on the classification of the IT asset and must be described in the requirements specification.

### 14.2.6 Secure development environment

#### Securing development environments

In the risk assessment of system development, the following should be considered:

The volume of sensitive data

Legal requirements

Separation of development, testing and production environments

Policies for access control and audit trail

Secure exchange of data between development, testing and production

Secure storage of backup

Audit trail of changes in environments

The security requirements should identify all relevant security aspects, such as the protection of data stored, transported or used

The analysis of security requirements must also take the following into account:

Requirements for access assignment and approval processes

Support for role-based access

Requirements from other system interfaces

Requirements for logging

Compatibility with other systems and security solutions

**14.2.7 Outsourced development**

**System development carried out by external supplier**

AAU requires access to monitoring the development process.

AAU requires acceptance testing.

AAU requires documented continuous quality assurance.

The selection of supplier must be considered carefully in order to ensure stable development and maintenance.

Functional requirements must be prepared for the IT system, including the specification of input data and operational validation and network management.

The circumstances regarding ownership or right of the use of the IT system and data must appear in the agreement made with the supplier.

It must be considered whether it would be appropriate to make a maintenance agreement with the supplier.

**External audit of outsourcing partners**

Outsourcing partners must ensure external audits at least once a year and must be able to present the audit report on demand.

**14.2.8 System security test**

### 14.2.9 System approval test

**Approval of new or modified systems**

The IT Department must establish an approval procedure for new systems as well as for new versions and updates of existing systems and for the tests to be carried out before the new systems, versions and updates can put into operation.

## 14.3 Test data

### 14.3.1 Securing test data

**Securing test data**

Data for testing must be selected, controlled and protected carefully and in accordance with their classification.

The copying of data from an operation environment to a test environment must be approved by the owner.

The copying and use of data from the operation environment to a test environment must be logged in order to ensure the audit trail.

# 15 Supplier relationships

## 15.1 Information security in supplier relationships

### 15.1.1 Information security policy regarding supplier relationships

**Information to external partners**

Third parties must be made aware of the desired security level, possibly by access to the policies in force.

**Assessment and approval of outsourcing supplier**

The supplier must document a satisfactory security level.

### 15.1.2 Handling of security in supplier agreements

**Outsourcing partners**

Prior to the conclusion of agreements, the partner’s security level must be clarified and approved by the systems and data owners.  Therefore, a so-called ISAE 3402/3401 statement or other relevant security level documentation must be presented by the outsourcing partners.

**Security when cooperating with partners**

Risks when using external service suppliers must be identified, and security measures must be agreed upon and included in the contract.

Whenever AAU’s systems and processes are integrated with those of a third party, security risks must be assessed and documented.

**Security assessment of a third party**

Prior to the establishment of any cooperation, risk assessment of the third party must be executed.

**Handling of security in supplier agreement procedures**

Relevant security requirements must be identified and agreed upon with suppliers who have access to, treat, store or deliver IT infrastructure to the information assets of the organisation.

The requirements include (but are not limited to):

A description of the relevant information assets

Adaption of the classification systems of the organisation and the suppliers

Identification of legal requirements such as rules regarding data protection, copyright, intellectual property right and compliance with industrial requirements (PCI DSS, ISO 27001)

Policies regarding acceptable use

Incident management and BCM requirements

Security requirements for logical and physical access

Auditing rights

The supplier's obligation to comply with organisational security policies.

Awareness and training programmes.

Supply chain for information and communication technology

**Network security, outsourcing supplier**

The supplier must ensure an appropriate structure of network, firewall, segmentation, encryption etc.

**15.2 Management of supplier services**

**15.2.1 Monitoring and review of supplier services**

**Monitoring and audit, cloud solution**

The supplier must document an adequate level of security, for example by means of an audit report, internal audit, ISO 27001 certification, outsourcing statement or equivalent.

The supplier must be able to report to which extent the service targets agreed upon have been met.

**15.2.2 Management of changes in supplier services**

**Change management with the service supplier**

It must be ensured that the change management of the service supplier's services complies with that of the AAU.

**16 Management of information security breaches**

**16.1.1 Management of information security breaches and improvements**

**16.1.1 Responsibilities and procedures**

**Information about security incidents**

AAU must inform the parties concerned of any security incidents. The unit manager of the main area in question, or the information security manager, should approve such information before it is circulated externally.

**Responsibility and business procedures for security events**

The unit manager is responsible for defining the business procedures which will ensure the speedy, efficient and methodical handling of security breaches.

**Accessibility incidents**

Incidents that affect accessibility must be resolved in accordance with the operation agreements in force (SLA). Operating incidents that cannot be resolved within the agreed time must result in the procedures for incident handling to be implemented. The affected users and system owners must be informed.

### 16.1.2 Reporting information security incidents

**Reporting of suspected security incidents**

In the case of finding, or having suspicions of, breaches of information security measures, this must be reported immediately to the immediate manager and to ITS via the security incident form. Exceptionally direct to ITS support (support@its.aau.dk or tel: 9940 2020). Both AAU and external service providers are required to report any observed security incident or suspicion. There should be easy access to reporting these incidents. All security incidents must be documented in the applicable support tool and filed in accordance with applicable legislation, which currently is 5 years.

### 16.1.3 Reporting information security weaknesses

**Reporting program errors**

Users who observe program errors which have not previously been experienced must report this to support@its.aau.dk or Tel.:+45 9940 2020

### 16.1.4 Assessment of and decision concerning information security incidents

**Assessment of past incidents**

The information security committee must review incidents of the past period at regular intervals and must on this basis recommend whether information security systems need to be improved or specified.  This may result in proposals to update rules or procedures or to update the risk assessment.

**Follow-up on reported security incidents**

ITS Support is responsible for collecting data for statistics of reported security incidents.

### 16.1.5 Management of information security breaches

ITS, in collaboration with CISO, shall ensure that procedures are in place for handling information breaches, including troubleshooting, controlled recovery after a breach and communication to internal and external persons, organizations or authorities.

### 16.1.6 Experience from information security breaches

**Control of and follow-up on security breaches**

Security breaches and unauthorised access to systems, information and data must be recorded.

### 16.1.7 Collecting evidence

**Collecting evidence**

If a security breach has legal consequences, adequate evidence material must be collected, stored and presented. This applies whether the security breach was performed by a person or a company. Securing evidence is a very difficult issues, and in each individual case, this should be coordinated with experts in the field. Using a wrong method can often result in the court rejecting the evidence.

**Liaison with relevant authorities**

The unit manager is responsible for maintaining contact with external partners regarding information security issues.

## 17 Information security aspects in emergency, contingency and restoration management

### 17.1 Information security continuity

### 17.1.1 Planning information security continuity

**Emergency procedures for critical processes and systems**

For all business-critical processes and systems, there must be an updated emergency procedure (emergency plan) that can be put into operation and which is continuously tested. It must be clearly defined who is responsible for activating emergency plans.

**Framework for contingency plans**

Based on business impact assessments, a contingency plan is prepared for the most business-critical systems in order to minimize the consequences for the information security of accidents and errors in AAU. The contingency plan must include and address all business critical systems.

The management must establish a uniform framework for AAU's contingency plan to ensure that it is coherent and meets all safety requirements, as well as determining the priority of testing and maintenance. The contingency plan must reflect the possibility that the physical locations may be inaccessible or destroyed.

### 17.1.2 Implementation of information security continuity

**Contingency plan**

A contingency plan must be available for all business-critical systems

**Activating the contingency plan**

It must be clearly defined who is responsible for activating contingency plans.

Employees who are involved in the contingency plan, must be informed of this responsibility.

All employees must be informed of the existence of the contingency plans.

### 17.1.3 Verify, review and evaluate information security continuity

**Contingency plan training**

Each unit is responsible for making sure that their employees receive adequate training in the contingency procedures agreed upon, including crisis management.

**Testing and maintaining contingency plans**

Contingency plans must be tested and updated regularly to ensure that they are up-to-date and effective.

**The testing of contingency plans must include:**

A desktop test of the different scenarios.

Simulations (in order to train the participants in the management of their roles after the episode).

Technical restoration (ensuring that technical systems can be effectively restored).

Restoration in other premises than the original (implementing parallel operation in other premises).

**Updating emergency plans**

At least once a year, emergency plans must be reviewed with a view to updating.

**17.2 Redundancy**

**17.2.1 Accessibility of information processing facilities**

AAU continuously reviews the business requirements for the availability of information systems in order to incorporate sufficient redundancy into the information systems.

## 18 Consistency

### 18.1 Consistency with legal and contractual requirements

**18.1.1 Identification of the legislation and contractual requirements in force**

**Storage and processing of personal data**

The AAU has released a separate policy for the processing of personal data. Read the details in the annex describing this.

**Control of compliance with the legislation regarding personal data**

The unit manager is responsible for ensuring that the Danish Data Protection Act is complied with in their unit.

**Traceability**

The processing of personal information must be logged automatically to ensure that it is possible for an auditor to check who has been working with the information and at which times.

**18.1.2 Intellectual property rights**

**Guidelines for copyright**

The management has the overall responsibility for making sure that the AAU pays adequate attention to ensuring non-violation of the copyrights of third parties.

Each user is responsible for always complying with the legislation in force regarding copyrights.

Documentation must be maintained of the ownership of licenses, original material and manuals.

It must be continuously checked that software license agreements are complied with; this includes compliance with restrictions regarding number of users, servers or copies.

It must be continuously checked that only authorised systems with authorised licenses are installed in AAU's equipment.

**Administration of software licenses**

Registration of software licenses takes place through the IT Department. The unit manager of each main area bears the overall responsibility for ensuring that a sufficient number of licenses are available within their main area.

The use of software licenses must be coordinated with the IT department or the person responsible for managing the unit’s licenses.

Employees must not commit the AAU by accepting software license terms which have not been accepted by the individual unit.

Each unit must record locally which licensed programs are available in the unit’s IT systems. Licence registers must be continually updated.

### 18.1.3 Protection of records

**Storage of system documentation**

System documentation must be stored for as long as the system is being used for development, testing or operation.

**Protection of system documentation**

System owners must keep system documentation in adequately secure storage.

Access rights to system documentation must be kept at a minimum and must be approved by the system owner.

**Data regulated by law**

AAU must protect data regulated by law against modification, deletion and unauthorised access.

**Storage and processing of data**

Business-critical data must always be stored and handled in such a way that the data integrity cannot be called into question.

### 18.1.4 Privacy and protection of personal information

Privacy and personal data must be protected in accordance with applicable law. Rules for the storage, shipping, transfer, disclosure and deletion of personal data communicated to all employees, affiliates and students of AAU involved in the processing of personal data must be implemented.

### 18.1.5 Regulation of cryptography

### Regulation in the area of cryptography

AAU must comply with the national rules regarding encryption. This also applies to employees taking portable and mobile equipment when visiting other countries.

### Regulatory compliance

All IT systems must comply with the relevant legal requirements.

## 18.2 Review of information security

### 18.2.1 Independent review of information security

### Revising security policies

The internal audit must check that the security policy is incorporated into the organisation and that it is being complied with. The check-up must take place at least once a year.

### Follow-up on the implementation of the security policy

At least once a year, a systematic follow-up process must take place of the compliance with the security policy in force.

Each unit leader must continuously ensure that security policies are adhered to within their own area of responsibility.

### 18.2.2 Compliance with security policies and security standards

### 18.2.3 Testing technical compliance

### Security test of internal IT systems

At least once a year, in-depth security tests must be conducted of the security level in internal network equipment and servers.

### Security test of external IT systems

At least once a year, a security test must be conducted of control procedures and network connections in order to identify and avoid unauthorised access attempts.