AAU's Security Handbook

The Security Handbook describes information security in various areas at AAU. The content has been approved by the Information Security Committee and is valid as of 15 December 2018.

Last edited 11.10.2023

1. Information Security Policies

1.1 Information Security Management Guidelines −

1.1.1 INFORMATION SECURITY POLICIES

PUBLICATION OF SECURITY POLICY
AAU's information security policy must be published and communicated to all relevant stakeholders, including all employees.

1.1.2 REVIEW OF INFORMATION SECURITY POLICIES

REVIEW OF SECURITY POLICY
The information security policy must be reviewed at least once a year. The Information Security Committee will review this topic in the second quarter and send a proposal for a new information policy to the Vice-Chancellor for final approval.

DEFINITION OF INFORMATION SECURITY
Information security is defined as the overall measures to ensure the confidentiality, availability and integrity of AAU's information. Measures include technical, procedural, legal and regulatory controls.

APPROVAL OF SECURITY POLICY
The information security policy, including any changes, must be approved by the Rector every year in June.

2. Organising Information Security

2.1 Internal Organisation −

2.1.1 ROLES AND RESPONSIBILITIES FOR INFORMATION SECURITY

SECURITY RESPONSIBILITIES FOR IT FUNCTIONS

All critical IT functions that require specialised knowledge, skill or experience must be identified and a responsible owner must be appointed. Security responsible system owners for business-critical systems must be identified and made aware of this responsibility. These owners must be given the responsibility and authority to ensure adequate protection.

OWNERSHIP

All information assets must have a designated owner (data owner) who is responsible for classifying each asset and ensuring that protection is provided in accordance with the classification.

SECURITY ORGANISATION

The Executive Board establishes an information security committee. (see terms of reference)

COORDINATION OF INFORMATION SECURITY

The Information Security Committee (ISU) is responsible for coordinating overall information security.

THE ROLE OF MANAGEMENT

Placement of responsibility is necessary to secure AAU's information assets.

Management must support the organisation's information security by setting clear guidelines, demonstrating visible commitment, allocating resources, defining roles and following up on information security work.

2.1.2 SEGREGATION OF DUTIES

SECURING BUSINESS-CRITICAL SYSTEMS

Segregation of duties must be implemented if required by law or if unit management deems it necessary to reduce the risk of unauthorised or unintentional use, modification or misuse of AAU's confidential and critical information.

2.1.3 CONTACT WITH AUTHORITIES

In the event of a security breach, a procedure must be established for communication and reporting to relevant authorities, including the Danish Data Protection Agency and the Centre for Cyber Security.

2.1.4 CONTACT WITH SPECIAL INTEREST GROUPS

The IT department (ITS) must keep abreast of new threats to the platforms and networks used. This is done by establishing internal and external contacts for information and knowledge sharing and upskilling.

2.1.5 INFORMATION SECURITY IN PROJECT MANAGEMENT

Information security must be an integral part of project management, where requirement specifications include requirements for information security - including protection of personal data - and where necessary security measures are identified on the basis of risk assessments.

2.2 Mobile Devices and Remote Workstations –

2.2.1 MOBILE DEVICE POLICY

ACCESS TO MOBILE DEVICES

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

2.2.2 REMOTE WORKPLACES

ACCESS FROM REMOTE WORKSTATIONS

Employees at AAU have the option to work from home or on the move. An encrypted connection must be used where a risk assessment dictates this. Access is only granted to users who are authenticated with a username and password and possibly either a personal digital key or 2-factor validation.

SECURING HOME OFFICES

Home workstations and their communication links must be protected in relation to the information and business systems they are used for.

3. Personnel Safety

3.1 Pre-employment –

3.1.1 SCREENING

BACKGROUND CHECKS OF EMPLOYEES

The HR department must ensure that the necessary background checks are carried out on employees with responsibility for critical or sensitive information.

VERIFICATION OF REFERENCES

The appointing authority is responsible for the necessary review and verification of information provided by employees and applicants prior to employment.

Background checks of employees may include, for example:

- Personal references.
- The applicant's CV.
- Education, certifications and professional qualifications.
- Identity checks (must always be done)

BACKGROUND CHECK OF CONSULTANTS

The unit manager must ensure that the necessary background checks of consultants are carried out.

3.1.2 TERMS AND CONDITIONS OF EMPLOYMENT

When a person is first created as a user of AAU's information assets, they must be informed of the rules that apply to the use of AAU's assets (see section 4 Asset management).

An email is automatically generated to the user with a link to www.informationssikkerhed.aau.dk.

The employment agreement should contain and elaborate:

- The legal responsibilities and rights of the employee.
- The employee's responsibilities in connection with information processing.
- Information about AAU's processing of personal data about the employee.
- Responsibilities when working outside AAU's own areas or outside normal working hours, e.g. when working from home or travelling.
- Description of what to do if employees ignore the employer's safety requirements.

3.2 During Employment

3.2.1 MANAGEMENT RESPONSIBILITY

Information security at AAU is highly dependent on the employees. Employees must therefore be trained in information security in relation to their job function and receive the necessary information. It is the management's responsibility to ensure that all employees:

- Are adequately informed about their roles and responsibilities in relation to security before they
- Are granted access to AAU's systems and data.
- Are familiarised with the necessary guidelines so that they can comply with AAU's information security policy.
- Achieve a level of awareness of information security issues that is consistent with their roles and responsibilities at AAU.
- Stay within the guidelines and regulations that apply to their employment, including AAU's information security policy and specific working methods.
- Gain knowledge of how information is classified.

3.2.2 INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING

SECURITY POLICY TRAINING

All employees must read the AAU Information Security Policy. All new employees receive a reference to AAU's information security policy no later than on their first day of work. All employees receive regular instructions on compliance with and training in AAU's information security policy.

The unit management is responsible for ensuring that new employees are given an introduction that includes familiarisation with AAU's IT code of conduct.

Before users are given access to information assets, they must be given the necessary instruction in log on/log off procedures, use of applications, etc.

SECURITY TRAINING FOR IT STAFF

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

In connection with their employment, IT employees must be familiarised with the information security principles with associated appendices and supplementary guidelines.

3.2.3 SANCTIONS

Management must establish a formal sanction procedure for employees, students and others who use AAU's information or information systems and who violate AAU's information security policies, rules or guidelines.

It is the management's responsibility to ensure that sanctions for breaches of AAU's information security policies, rules or guidelines are enforced in accordance with applicable legislation.

Violations of information security are sanctioned in the same way as other violations of AAU's policies and rules (reprimand, warning, dismissal, withdrawal of the right to use AAU's network, expulsion and, in special cases, reporting to the police).

3.3 Ending or changing the employment relationship –

3.3.1 END OR CHANGE OF EMPLOYMENT

The employee must hand over all information and assets provided by AAU upon termination of employment. The employee must also delete company information from private equipment upon termination of employment. In collaboration with IT, HR must create and maintain a procedure for revoking privileges in connection with changes in the employment relationship, resignation or dismissal of staff.

4. Asset Management

4.1 Responsibility for Assets –

4.1.1 ASSET INVENTORY

An inventory of AAU's critical and sensitive information assets must be provided that also complies with legal requirements for personal data inventories.

4.1.2 OWNERSHIP OF ASSETS

SECURITY RESPONSIBILITY FOR INFORMATION ASSETS

A responsible data owner must be appointed who is responsible for classifying each asset and ensuring that it is protected in accordance with the classification.

It is the unit manager's responsibility to create and maintain a list of information assets. The list must indicate the data and system owner for each asset.

PREPARATION OF AN OVERALL RISK ASSESSMENT

Based on the list of information assets, regular risk assessments are conducted to determine the necessary information security measures.

It is the responsibility of the organisation's management to prepare risk assessments for the organisation's critical and sensitive information assets. The assessment must highlight which threats exist, the likelihood of them occurring and the possible consequences. The risk assessment can be carried out in collaboration with the Chief Information Security Officer and must be documented in a centralised tool.

The risk assessments must be updated at least every year and also in the event of major changes in the organisation and/or information assets that may affect the overall risk picture.

The collected material constitutes AAU's overall risk assessment.

4.1.3 ACCEPTED USE OF ASSETS

ACCEPTABLE USE OF INFORMATION ASSETS

An "IT code of conduct for employees and students" has been drawn up. This code describes detailed rules and general guidelines for user behaviour.

4.1.4 RETURN OF ASSETS

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

4.2 Classification of Information

4.2.1 CLASSIFICATION OF INFORMATION

All employees should be aware of how information is classified. To ensure the confidentiality of information, a 4-level classification model has been developed:

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

Regardless of the classification level, 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 or organisation responsible for classifying data and ensuring that it is protected in accordance with the classification.
- Administrator: Person or organisation that, based on the data owner's classification and instructions, manages access to data.
- Data Processor: Person or organisation that processes data on behalf of the data owner and according to their instructions.
- User: Person or organisation that uses data.

4.2.2 LABELLING OF INFORMATION

Each data owner is responsible for ensuring that information is appropriately classified.

RESPONSIBILITY FOR ACCESS RIGHTS

The data owner is responsible for establishing and continuously reviewing access rights.

CLASSIFICATION LABELLING

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

4.2.3 ASSET MANAGEMENT

CONTROL OF CLASSIFIED INFORMATION

The Information Security Committee is responsible for defining a fixed set of appropriate and relevant security measures to protect each piece of information.

4.3 Media Management –

4.3.1 PORTABLE MEDIA MANAGEMENT

STORAGE AND REGISTRATION OF DATA MEDIA

The data owner must ensure that media or the information on the media is classified and that users are instructed to store the media according to classification rules.

USE OF DATA MEDIA

The chosen data media must be able to protect the information according to its classification.

USE OF PORTABLE MEDIA FOR CONFIDENTIAL DATA

Data media must be protected against loss and misuse according to the rules for mobile devices. Confidential and sensitive data, including personal data, must be encrypted if stored or transported on portable media such as USB memory, tablets, phones, DVDs, floppy discs, etc.

4.3.2 DISPOSAL OF MEDIA

DISPOSAL AND RECYCLING OF MEDIA

All data media, e.g. hard drives, floppy disks, CDs, DVDs, tapes and memory devices must be securely erased or destroyed before disposal if they contain data that is not classified "Public". Please refer to the "Scrapping/recycling procedure for IT equipment at AAU", which is handled by ITS Support.

4.3.3 PHYSICAL MEDIA DURING TRANSPORT

All data media, e.g. hard drives, floppy disks, CDs, DVDs, tapes and memory devices containing confidential or sensitive data must be encrypted. The applicable encryption requirement is at least 256-bit AES encryption.

5. Access Control

5.1 Business Requirements for Access Management –

The requirements for access control are determined by the value of the data and systems being accessed. A layered security approach should be sought, so that the closer you get to the most critical and sensitive information, the greater the requirements for access control. For example, if access is only granted to the Internet, i.e. to public data and systems, it is not necessary to set the same requirements for passwords as are required when access is granted to confidential and sensitive information internally at AAU. These rules should be regarded as minimum requirements, and it is therefore permitted for the individual system and data owner to introduce a stricter policy if a risk assessment so requires.

5.1.1 ACCESS CONTROL POLICY

RESTRICTED ACCESS TO INFORMATION

Access by users and personnel to user system functions and information must be restricted in accordance with the defined work and business requirements and the classification of the information.

REVOCATION OF PRIVILEGES UPON TERMINATION OF EMPLOYMENT

There must be an up-to-date procedure for the revocation of privileges in connection with resignation, organisational reassignment, change in position or dismissal of staff. It is the unit management's responsibility to inform the IT and HR department of changes to employees' work tasks, including organisational reassignment and resignation, so that assigned privileges can be adjusted or removed.

5.1.2 ACCESS TO NETWORKS AND NETWORK SERVICES

NETWORK MONITORING

ITS Infrastructure is responsible for continuously monitoring the use and security of AAU's network infrastructure. It is recommended to use automated monitoring systems.

GUIDELINES FOR THE USE OF NETWORK SERVICES

Users may only access the services they are authorised to use.

ACCESS TO WIRELESS NETWORKS

Students, staff and guests have the opportunity to use wireless networks at Aalborg University. Read more here.

SPLITTING OF NETWORKS

To improve the reliability of critical servers, separate server networks with a stricter filtering policy must be established. Separate networks must be established for equipment in different "risk groups", e.g. private computers, university computers and printers.

NETWORK ACCESS CONTROL

Only authorised users and equipment may access networks at AAU.

AUTHENTICATION WHEN ACCESSING THE NETWORK

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

5.2 User Access Management –

5.2.1 USER REGISTRATION AND DEREGISTRATION

IDENTIFICATION AND AUTHENTICATION OF USERS

All users must have a unique identity for personal use. An appropriate authentication technique must be used to verify the identity of users. The user identity must be traceable to the person responsible for a given activity. Common user identities must be avoided.

5.2.2 GRANTING USER ACCESS

ASSIGNMENT OF USER RIGHTS

The data owner is responsible for ensuring that each user is granted exactly the user privileges that the user's work tasks warrant.

GUIDELINES FOR ACCESS MANAGEMENT

The administrator is responsible for the ongoing registration, management and monitoring of the granting and use of privileges according to the data owner's classification of information.

RESTRICTING ACCESS TO INFORMATION

Applications must ensure that access to information follows a well-defined access policy.

5.2.3 MANAGING PRIVILEGED ACCESS RIGHTS

ACCESS PROTECTION

Always use a password for access with system administrator privileges.

EXTENDED ACCESS RIGHTS

The extended access rights, e.g. administrator rights, may only be granted to a limited extent and solely on a work-related need. The extended access rights must be registered. The extended access rights may not be put into effect until the necessary authorisation has been obtained. Automated system engineering processes shall be used as far as possible to minimise the need to grant extended access rights.

Individual user programmes shall, as far as possible, be designed to limit the need for intervention with extended rights. Special user identities must be used for the extended rights for monitoring and follow-up purposes.

MODIFICATION OF PASSWORDS WITH EXTENDED ACCESS RIGHTS

Extended privileges passwords must be changed or revoked if it is suspected that outsiders have gained knowledge of them, or where an authorised user changes job function that no longer justifies the extended privileges.

PASSWORD CHANGE FOR EXTENDED RIGHTS UPON TERMINATION OF EMPLOYMENT

If a person with knowledge of extended access rights resigns, these passwords must be changed immediately.

5.2.4 MANAGEMENT OF SECRET AUTHENTICATION INFORMATION ABOUT USERS

STORAGE OF PASSWORDS

Passwords must never be stored electronically in plain text.

5.2.5 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 similar that need to be removed or changed.

5.2.6 REVOCATION OR ADJUSTMENT OF ACCESS RIGHTS

USER PROFILES

Guests and external consultants may only be created as users with time-limited access.

Normally, the time limit may not exceed 12 months before re-authorisation. Users are granted access to AAU solely on the basis of a work and/or study-related need.

RESIGNATION

When employment or temporary contracts are cancelled, associated rights must be assessed and, if necessary, changed or removed. ID cards and the like must be handed in and IT equipment must be confiscated.

EMPLOYEE REASSIGNMENT

Assigned access rights and privileges must be reassessed in connection with departure or reassignment. It is the unit management's responsibility to establish local procedures for this.

REGISTRATION OF USERS

Users must have a unique username and user ID. Access rights must be aligned with business needs. It must be verified that the level of authorisation is in accordance with AAU's general security guidelines. Service providers must use similar or the same authorisation procedure as AAU.

The system owner must authorise user access and maintain user records for the system. AAU must maintain instructions on how to remove or modify users or user rights upon termination or change of user job function. Access rights must not violate any segregation of duties requirements. The procedures must cover the entire period during which access rights are valid, i.e. from registration of a user to formal cancellation of a user who no longer has a work or study-related need for access.

Efforts must be made to ensure that the user has the same identification on all of the IT systems to which the user has access. Shared IDs for a group of employees should be avoided as far as possible.

5.3 User Responsibilities –

5.3.1 USE OF SECRET AUTHENTICATION INFORMATION

SELECTION OF SECURE PASSWORDS

Users must follow good security practices when selecting and using a password. A password should be chosen that is easy to remember but difficult to guess. See applicable guidance and help here.

PASSWORD CHANGE REQUIREMENTS

Passwords must be changed if it is suspected that others have gained knowledge of them and at least once a year. For information that is protected by a more qualified access control (where the access control consists of more than just username/password), the frequency of password changes can be changed in agreement with the Information Security Committee and the Head of Information Security.

PASSWORD LENGTH REQUIREMENTS

User passwords must contain at least 14 characters and at least 3 out of 4 different character types (upper and lower case letters, numbers or special characters). Passwords with extended rights, e.g. administrators, must contain at least 14 characters and at least 4 different character types (upper case, lower case, numbers or special characters).

PASSWORD REUSE

It is not allowed to use the same password on AAU's systems that is used on external systems.

PASSWORDS ARE STRICTLY PERSONAL

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

PASSWORD GUIDELINES

Upon user creation or password reset, users must be assigned a secure, temporary password that must be changed immediately after first use. A procedure must be established and maintained for establishing a user's identity before a new temporary password may be issued. Temporary passwords must be unique, must not be reused and must meet the general requirements for passwords.

SECURING CRITICAL INFORMATION

After installing a new system, the default passwords must be changed immediately in the new system.

5.4 System and Application Access Control

5.4.1 PROCEDURES FOR SECURE LOG-ON

SECURE LOG-ON

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

5.4.2 PASSWORD MANAGEMENT SYSTEM

PASSWORD MANAGEMENT SYSTEMS

IT systems shall, as far as possible, ensure that password requirements are met and that passwords are not reused.

IMPLEMENTATION OF A PASSWORD MANAGEMENT SYSTEM

A password management system must be implemented for critical systems that do not integrate with AD and enforce AAU's password rules.

5.4.3 USE OF PRIVILEGED SYSTEM PROGRAMS

USE OF 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 the security of systems or devices) is limited to a minimum of trusted and authorized users.

5.4.4 MANAGING ACCESS TO APPLICATION SOURCE CODE

ACCESS CONTROL FOR SOURCE TEXT

Source code for applications under development must be protected with access control systems to ensure integrity.

CONTROLLED ACCESS TO SOURCE CODE

The source code of development projects must be secured against unauthorized access. Changes must be controlled to ensure integrity and version control processes must be in place. Any hard copies of source code must be stored securely.

6. Cryptography

6.1 Cryptographic Controls –

6.1.1 POLICY FOR THE USE OF CRYPTOGRAPHY

ENCRYPTION OF FILES
Files with information classified as confidential or sensitive are protected according to AAU's data classification model by using cryptography in certain contexts.

APPROVAL OF ENCRYPTION PRODUCTS
Only cryptography that uses recognized encryption methods may be used.

USE OF ENCRYPTION IN CONNECTION WITH INFORMATION STORAGE
Confidential and sensitive information must always be sent encrypted when processed electronically outside AAU's network.

6.1.2 MANAGEMENT OF ELECTRONIC KEYS

KEY MANAGEMENT
A key management procedure must be established and maintained to describe how the generation, distribution, storage and destruction of keys are handled.

7. Physical and Environmental Security

7.1 Physical and Environmental Security –

Physical security includes doors, windows, alarms, video surveillance - as well as 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 a certain extent ensure that only people with legitimate business can access the university's area during the times when the system is activated.

7.2 Safe Areas –

7.2.1 PHYSICAL PERIMETER SECURITY

BURGLAR ALARMS
Most AAU areas have established perimeter security, and there are agreements with a security company for surveillance, call-outs and response in the event of an alarm.

7.2.2 PHYSICAL ACCESS CONTROL
Physical security and access rules are part of AAU's security policy. Access control systems are an element of physical security that ensures that only people with legitimate business are allowed access to AAU's premises.

ACCESS CARDS

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

7.2.3 SECURING OFFICES, PREMISES AND FACILITIES

SECURING OFFICES, PREMISES AND EQUIPMENT

Offices and other premises where confidential and sensitive information is stored must be lockable.

INFORMATION ABOUT SECURE AREAS

Information about secure areas and their function must only be provided on a work-related need-to-know basis.

7.2.4 PROTECTION AGAINST EXTERNAL AND ENVIRONMENTAL THREATS

FIRE SAFETY

Server rooms must not be used as storage for flammable materials. Hazardous or flammable materials must be stored at an appropriate distance from safe areas. Automatic fire extinguishing and fire alarm systems must always be installed in rooms where the total value of IT and other information assets exceeds DKK 700,000 in 2018 prices.

ENVIRONMENTAL SECURITY OF SERVER ROOMS

Server rooms, junction boxes and similar areas must be adequately secured against environmental incidents such as fire, water ingress, explosion and similar impacts.

7.2.5 WORKING IN SECURE AREAS

LOCKING OF PREMISES AND BUILDINGS

All doors and windows with access to/from buildings must be closed and locked at the end of working hours. Doors to secure locations in the buildings must also be locked.

7.2.6 LOADING AND UNLOADING AREAS

LOADING AND UNLOADING AREAS

Deliveries must be registered in accordance with the applicable goods receipt procedure.

7.3 Equipment –

7.3.1 LOCATION AND PROTECTION OF EQUIPMENT

LOCKING OF MAIN JUNCTION BOXES AND SIMILAR TECHNICAL ROOMS

All junction boxes and technical rooms must be secured and locked.

ACCESS TO SERVER ROOMS AND MAIN JUNCTION BOXES

Access to server rooms and main junction boxes is described in the "Access to machine rooms" guide.

LENDING OF ACCESS CARDS AND/OR KEYS

Access to secure areas can be temporarily granted to craftsmen, technicians and others, provided that all access rules are observed.

ACCESS FOR SERVICE PROVIDERS

Service providers may only be granted access to secure areas when required and access is monitored.

7.3.2 SUPPORTING UTILITIES (SECURITY OF SUPPLY)

EMERGENCY POWER SYSTEMS

The risk assessment available for critical assets must include an assessment of the use of uninterruptible power supplies (UPS).

SECURITY OF SUPPLY

Data communication is secured by establishing redundancy and strategic placement of equipment and lines to avoid single points of failure.

7.3.3 SECURING CABLES

Data communication cables must be protected against unauthorized interference and damage. Ensure that cables in the ground are registered with relevant stakeholders. Fixed cables and equipment must always be clearly and unambiguously labeled. Documentation must be updated when the fixed cabling is changed.

7.3.4 MAINTENANCE OF EQUIPMENT

EQUIPMENT AND FACILITY MAINTENANCE

System owners should maintain equipment according to the supplier's instructions. Only qualified suppliers should perform repairs and maintenance. The repair company must comply with applicable security requirements if equipment is repaired or maintained outside AAU.

Critical and sensitive information must be deleted from equipment repaired or maintained outside AAU. System managers are responsible for keeping a log of all faults and defects as well as repairs and preventive maintenance.

7.3.5 REMOVAL OF ASSETS

Unit management sets rules for the authorized disposal of AAU assets.

7.3.6 SECURING EQUIPMENT AND ASSETS OUTSIDE THE ORGANIZATION

SUPERVISION OF MOBILE DEVICES

Mobile devices must not be left unattended in unlocked rooms. Portable devices must be configured according to the applicable AAU mobile device rules.

7.3.7 SAFE DISPOSAL OR REUSE OF EQUIPMENT

DISPOSAL OR REUSE OF EQUIPMENT

IT equipment containing storage media - e.g. fixed hard drives in workstations, servers and copiers - must be checked before removal to ensure that all information, including licensed and proprietary user programs, has been deleted.

7.3.8 UNATTENDED USER EQUIPMENT

LOCATION OF EQUIPMENT

Laptops and similar equipment, if left in an office unattended (e.g. after working hours), should be locked up so that they are not immediately visible from the outside. Equipment should be placed or protected to minimize the risk of damage and unauthorized access. Equipment used to process critical or sensitive information must be placed so that the information cannot be read by unauthorized persons.

7.3.9 CLEAR DESK AND BLANK SCREEN POLICY

STORAGE OF PHYSICAL DOCUMENTS

Confidential and sensitive information must be stored in a locked cabinet or drawer after working hours, according to the data classification model.

USE OF PASSWORD-PROTECTED SCREEN SAVER

Users must activate password-protected screen lock when leaving the workstation. As a general rule, the system should enable password-protected screen lock on computers after a maximum of 15 minutes of inactivity.

PRINTING

Print queues and similar with sensitive or critical content must be secured against unauthorized access. Users must ensure that confidential and sensitive printouts are picked up immediately. Where possible, the Follow-You print system should be used for printing.

8. Operational Safety

8.1 Operating Procedures and Responsibilities –

8.1.1 DOCUMENTED OPERATING PROCEDURES

SECURING SERVER SYSTEMS

All servers must be secured and approved before going into production.

DOCUMENTATION

Site management must ensure that well-described operating procedures are in place for all critical IT systems 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, up-to-date and accessible to operational staff and others with a work-related need.

RECORDING OF OPERATIONAL STATUS

Significant disturbances and irregularities in the operation of the systems and their causes must be recorded.

PROTECTION OF DIAGNOSTIC AND CONFIGURATION PORTS

Physical and logical access to diagnostic and configuration ports must be controlled. Remote diagnostic and maintenance access points - including special diagnostic ports, console switches, out-of-band management, etc. - must be secured against unauthorized use.

Procedures for external vendor access to remote diagnostics must be established by the system owner. Any use of diagnostic ports should be logged.

8.1.2 CHANGE MANAGEMENT

CHANGE MANAGEMENT

The IT department follows the change management principles of ITIL, as exemplified by the rules below. Changes must be preceded by a review of security measures and integrity controls to ensure that these are not degraded by the implementation.

Approval must be obtained from the system owner before the change is implemented. System documentation must be updated with each change. Outdated system documentation must be archived or destroyed.

Maintain a version control for all system changes and a log of all changes. Where possible, operational functionality should be tested before changes are implemented.

PLANNING, TESTING AND APPROVAL OF CHANGES

Changes must follow a formalized procedure prior to implementation, which involves planning and, where possible, testing before going live. In addition, the impact of changes must be assessed before they are implemented.

GUIDELINES FOR CHANGES

Changes should only be implemented when there is a justified need.

The IT department is responsible for ensuring that significant changes are clearly identified and registered. Information regarding implemented changes must be communicated to relevant stakeholders. The IT department is responsible for ensuring that there is an emergency procedure per system/service to mitigate the impact of failed changes.

8.1.3 CAPACITY MANAGEMENT

CAPACITY PLANNING

IT systems must be dimensioned according to capacity requirements. Load must be monitored so that upgrades and adjustments can be made on an ongoing basis. There must be a high focus on all business-critical systems at all times.

CAPACITY MONITORING

All server systems must be monitored to ensure sufficient capacity, reliable operation and availability. Major deviations from normal capacity must be recorded and handled as an incident.

8.1.4 SEPARATION OF DEVELOPMENT TEST AND OPERATIONAL ENVIRONMENTS

SECURING THE APPLICATION DEVELOPMENT ENVIRONMENTS

Development environments must be secured against threats such as unauthorized access, changes and loss. Information must be secured according to its classification.

ACCESS TO PRODUCTION DATA

Access to confidential information by system administrators must be restricted.

SEPARATION OF DEVELOPMENT, TESTING AND OPERATIONS

Development and test environments must be systemically or physically separated from the operational environment.

8.2 Protection Against Malware

8.2.1 CONTROLS AGAINST MALWARE

ANTIVIRUS REQUIREMENTS FOR COMPUTERS

All computers must use an updated antivirus program or be protected by other methods. This also applies to private computers connected to AAU's network. Protection against spyware and other malware must be used where deemed necessary.

8.3 Backup

8.3.1 BACKUP OF INFORMATION

BACKING UP INFORMATION ON SERVER SYSTEMS

The IT department is responsible for the secure storage and backup of information on server equipment, as well as for the storage and backup of all business-critical information on server systems. There must be a procedure or guide for backing up all essential/business-critical data, programs and parameter setups

Backup must be accurate, complete and include documented restore procedures. The extent and frequency of backup should reflect current business, IT and regulatory requirements. Backup data must be protected with appropriate logical and physical access controls. Backed up information must be tested regularly to ensure that the information is restored correctly. Backup data must be stored off-site to ensure redundancy in the event of a disaster.

MONITORING OF BACKUP PROCEDURES

The ability to restore information from backup systems must be regularly tested. Furthermore, restoration should be tested after system or process changes that may affect backup routines.

BACKUP CONTINGENCY PLANS

All critical systems must have a backup contingency plan in place to minimize the risk of information loss.

STORAGE OF BACKUPS AT AN OFFSITE LOCATION

Data media for recovery of critical systems must be stored in a secure storage location at an appropriate distance from production data.

8.4 Logging and Monitoring

8.4.1 EVENT LOGGING

EVENT LOGGING

All production systems must log access and access attempt information to track unauthorized activity. Log files should be reviewed regularly and advantageously using automated tools.

All information security incidents must be logged and retained for a defined period of time for follow-up on access controls and possible investigation of errors and misuse. The IT department is responsible for configuring systems in a way that relevant information is logged and stored for possible future use.

STORAGE OF FOLLOW-UP LOGS

AAU's rules for logging must comply with applicable Danish legislation.

MONITORING OF INTERNET USAGE

AAU reserves the right to filter, log and restrict the use of networks, including the internet, to the extent required for operational reasons.

8.4.2 PROTECTION OF LOG INFORMATION

Log files may contain information that must not be publicly available. Log facilities and log information must be protected against manipulation and technical errors.

All log records must be protected from unauthorized access through the use of access control systems, physical separation or network segmentation. Log records must be immediately transferred to a central log server or to a secure medium that is difficult to modify. Only persons whose work requires it are granted access to logs.

8.4.3 ADMINISTRATOR AND OPERATOR LOG

MONITORING THE SERVICE PROVIDER

The IT department must regularly monitor the service providers, review the agreed reports and logs, and perform actual audits to ensure compliance with the agreement and that security incidents and issues are handled appropriately.

ADMINISTRATOR LOG

All actions performed by persons with administrator rights in connection with critical system components in operation, including network equipment, must be logged.

8.4.4 TIME SYNCHRONIZATION

All equipment (servers, PCs, network equipment) that provide logs according to the logging rules are required to synchronize their clocks using NTP.

8.5 Managing Operating Software –

8.5.1 SOFTWARE INSTALLATION ON OPERATING SYSTEMS

Maintaining and updating IT systems is necessary to maintain an appropriate level of security for AAU. Operating IT systems includes elements of monitoring the health of the systems, updating and backing up data. Most IT systems today rely on networks and therefore managing, building, securing and maintaining networks is vital for AAU. The threat of unauthorized access makes it necessary to have clear rules for the use of AAU's network and monitoring of the infrastructure.

8.6 Vulnerability Management –

8.6.1 MANAGEMENT OF TECHNICAL VULNERABILITIES

PATCHES FOR OPERATING SYSTEMS AND APPLICATION PROGRAM PACKAGES

The IT department must continuously assess available security fixes, 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 done as soon as possible and usually within one week after assessment and positive functional and compatibility testing.

MAJOR OPERATING SYSTEM UPDATES, E.G. SERVICE PACKS

When major updates, e.g. service packs, are made available from suppliers, the IT department must assess whether these should be installed. Updates in critical systems must be thoroughly tested for compatibility with used applications before the updates are installed in the production environment.

SOFTWARE UPDATES IN GENERAL

The IT department must stay informed about patches for programs used at AAU and install these on all computers, e.g. servers and workstations, as soon as possible when it is assessed that the patches have a positive impact on overall security. System owners are responsible for ensuring that the software used is regularly updated.

CHANGES TO CRITICAL SYSTEMS

All changes to critical systems must be carried out according to an approved procedure in accordance with the ITIL standard. All procedures must include an alternative plan for restoring the critical system. The conditions for activating the alternative plan must also be stated in the procedure.

8.7 Considerations when Auditing Information Systems

8.7.1 CONTROLS FOR AUDITING INFORMATION SYSTEMS

SECURITY IN RELATION TO AUDITING

Audit requirements and audit procedures for systems in operation must be carefully planned and agreed with those involved to minimize the risk of disruption to AAU's business activities.

The planned audit procedures must only include read access to systems and data. If the audit requires more than read access, this may only be allowed on copies of the affected files, which must be deleted after use. All audit access must be logged. The persons performing the audit must be independent of the audited area.

PROTECTION OF AUDIT TOOLS

Access to audit tools must be restricted to prevent misuse.

9. Communication Security

9.1 Network Security Management

9.1.1 NETWORK MANAGEMENT

INSTALLATION OF NETWORK EQUIPMENT

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

SETTING UP WIRELESS ACCESS POINTS (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 prepare and publish rules for connecting equipment to the local network.

INCOMING NETWORK CONNECTIONS

Local area networks should be divided into zones with a well-defined filter policy between zones. The filter policy should ensure that only necessary services and resources (servers, PCs, etc.) are accessed. Filtering can be done centrally or locally.

SECURING THE NETWORK

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

USE OF WIRELESS LOCAL AREA NETWORKS

Students and employees at AAU are recommended to use the wireless network AAU-1x. Read more about wireless networks here.

INSTALLATION OF WIRELESS EQUIPMENT

Wireless networks (access points) must not be set up on campus without prior agreement with the IT department's network group.

ACCESS TO THE NETWORK

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

ACCESS TO INFORMATION ON AAU'S NETWORK

Access to information on AAU's network must be through security-approved solutions and in accordance with the classification of the information.

STORAGE OF CONFIDENTIAL OR SENSITIVE INFORMATION ON PRIVATE EQUIPMENT

Processing or storage of sensitive or confidential information on equipment that does not belong to AAU must comply with the rules described for data classification.

9.1.2 SECURING NETWORK SERVICES

USE OF ENCRYPTION IN CONNECTION WITH INFORMATION EXCHANGE

It is required that files containing confidential or sensitive information are always encrypted during transmission to recipients outside AAU, cf. 10.1.1.

INTERNET-BASED SERVICES

It is permitted to use internet services that do not involve increased security risks.

REMOTE MANAGEMENT AND ADMINISTRATION

Remote administration connections for maintenance and support tasks may only be activated when necessary and upon request to the system owner.

9.2 Information Transfer –

9.2.1 INFORMATION TRANSFER POLICIES AND PROCEDURES

DISCLOSURE OF CONFIDENTIAL INFORMATION AND DATA

Information that is not classified "Public" may not be disclosed to third parties in any form without the approval of the data owner. Requests for access should be referred to the Management Secretariat (by the Rector/Director).

ENCRYPTION OF ADMINISTRATIVE NETWORK CONNECTIONS

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

PROCEDURES FOR INFORMATION EXCHANGE

Each unit manager is responsible for ensuring that local guidelines and procedures are in place for any critical or sensitive information exchange, both physical and electronic.

PRINTS

Users must pick up printouts containing confidential and sensitive information immediately. Where possible, the Follow-You print system is used for printouts.

9.2.2 INFORMATION TRANSFER AGREEMENTS

INFORMATION EXCHANGE AGREEMENTS

When exchanging information and software between AAU and third parties, AAU's rules regarding the classification of information must be observed.

9.2.3 ELECTRONIC MESSAGES

ELECTRONIC EXCHANGE OF MAIL AND DOCUMENTS

Confidential and sensitive information must always be sent encrypted when processed electronically outside the AAU network.

AUTHENTICATION

Users should be aware that communication via social services on the internet can be insecure and therefore does not provide certainty about who you are communicating with.

ATTACHMENTS

The IT department may choose to block file types that are deemed dangerous or inappropriate.

PHISHING AND FRAUD

As part of ongoing awareness training, users are made aware of "phishing" and "social engineering", which can mean, for example, receiving seemingly sincere emails that attempt to steal valuable information or try to get the user to take unwanted actions.

CONFIDENTIAL MAIL

E-mail with confidential or sensitive content sent to external recipients must be encrypted using a recognized method, see 10.1.1.

EMPLOYEES' PRIVATE USE OF EMAIL

Employees may use the email systems for personal use to a limited extent if this does not affect AAU's operations and security in general. Private emails must be stored in a folder with the name: "PRIVATE".

AAU'S INFORMATION ON SOCIAL NETWORKS

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

PRIVATE USE OF INTERNET ACCESS

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

PROCESSING OF PERSONAL DATA

The processing of personal data and the procedure for unintentional publication of information on the internet is described in AAU's privacy policy.

STORAGE AND DELETION OF E-MAIL

Email containing personal data must be processed in accordance with the applicable personal data law.

INTEGRITY OF MESSAGES

If there is a need for verification of the integrity of a message, the use of an employee certificate or similar solution for signing such messages may be required.

SPAM MAIL PROTECTION

AAU filters out emails that meet AAU's criteria for spam emails.

9.2.4 CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENTS

CONTENT OF THE NON-DISCLOSURE AGREEMENTS

The template for a non-disclosure agreement defines the requirements for the content of the agreements.

NON-DISCLOSURE AGREEMENT FOR THIRD PARTIES

The device manager must ensure that third parties with access to systems and information are subject to confidentiality requirements.

10. Systems Acquisition, Development and Maintenance

10.1 Security Requirements for Information Systems –

10.1.1 ANALYSIS AND SPECIFICATION OF INFORMATION SECURITY REQUIREMENTS

SECURITY IN APPLICATION DEVELOPMENT

Information security, including personal data protection, must be included as an integral part of all development projects.

PROCUREMENT PROCEDURES

The unit manager must ensure that new acquisitions do not give rise to conflicts with existing requirements in adopted policies. This is documented in a risk assessment.

Where acquisitions give rise to an increased risk of security incidents, management must accept this.

10.1.2 SECURING APPLICATION SERVICES ON PUBLIC NETWORKS

SECURING APPLICATIONS ON PUBLIC NETWORKS

Secure authentication and authorization processes must be used to secure service transactions over public networks. The integrity and confidentiality of information must be ensured when using application services over public networks using e.g:

- Cryptographic solutions (such as SSL, SFTP, HTTPS, secure APIs or web services)
- Integrity assurance (e.g. hashing)

10.1.3 PROTECTION OF TRADING APPLICATIONS AND SERVICES

ONLINE TRANSACTIONS

Systems where external users are offered the possibility of direct updating in AAU's databases must have special security measures to prevent transmission errors, misdirection, manipulation and unauthorized access and repetition of already completed transactions.

ELECTRONIC COMMERCE

Information relating to electronic commerce over public networks must be protected against fraud, contractual discrepancies, unauthorized access and alteration. AAU must implement a variety of measures to secure its electronic commerce. This includes a set of terms and conditions that are accessible, understood and accepted by the customer, including how authenticity is determined, who sets prices and what the requirements for confidentiality, integrity and availability are. The protection must apply to both the exchange of information and the systems used to store or process data.

10.2 Security in Development and Support Processes –

10.2.1 SECURE DEVELOPMENT POLICY

VALIDATION OF INPUT DATA

Data submitted to the systems must be validated for correctness. Periodic review of key data should confirm its validity and integrity. Data is tested for plausibility before it is entered into the systems. Generate a log of the activities that send data into the system.

Data validation should protect assets from input errors. Input data must be validated to ensure it complies with formal format requirements, e.g. checking date format and social security numbers.

DATABASE INTEGRITY

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

10.2.2 SYSTEM CHANGE MANAGEMENT PROCEDURES

10.2.3 TECHNICAL REVIEW OF APPLICATIONS AFTER CHANGE OF OPERATING PLATFORMS

REVIEW OF SYSTEMS AFTER CHANGES

Before changing operating environments, critical business systems must be reviewed and tested to ensure that there are no unintended secondary effects on AAU's day-to-day operations. For externally accessible systems and particularly critical systems, it must always be considered, based on a risk assessment, whether an actual penetration test should be carried out by an external independent third party.

10.2.4 LIMITATION OF CHANGES TO SOFTWARE PACKAGES

CHANGES TO STANDARD SYSTEMS

Changes to externally supplied standard systems must be limited to necessary changes and such changes must be carefully managed and assessed in relation to any compatibility issues with other software used in AAU. Built-in security measures, e.g. logging, access and integrity controls, should be reviewed to ensure that they are not compromised.

The extent to which AAU will be responsible for the future maintenance of the software should be assessed.

10.2.5 PRINCIPLES FOR DEVELOPING SECURE SYSTEMS

SECURITY REQUIREMENTS FOR INFORMATION PROCESSING SYSTEMS

AAU's requirement specifications for both new and existing systems must include information security, including personal data protection, which is adapted according to specific risk assessments for the solution.

SECURITY IN SYSTEM PLANNING

When planning systems, information security considerations must always be taken into account.

Information security requirements must be taken into account when designing, testing, implementing and upgrading IT systems, as well as when making system changes.

SPECIFICATION OF SECURITY REQUIREMENTS

All new information assets and associated systems must be classified and risk assessed. The same applies to any major change to existing systems.

CONTROL OF INTERNAL DATA PROCESSING

Validation and reconciliation controls must be built into systems to detect inconsistencies and ensure data integrity. The level of control depends on the classification of the information and must be described in the requirements specification.

10.2.6 SECURE DEVELOPMENT ENVIRONMENT

SECURING DEVELOPMENT ENVIRONMENTS

When risk assessing system development, the following should be considered:

- The extent of confidential and sensitive information
- Legal requirements
- Separation of development, test and production environments
- Access control and audit trail policies
- Secure exchange of information between systems and between development, test and production and any external parties
- Secure storage of backups
- Audit trails of changes to environments

Security requirements should identify all relevant security aspects of information processing. The analysis of security requirements should also take into account the following:

- Requirements for access granting and authorization processes
- Support for role-based access
- Requirements from other system interfaces
- Requirements for logging
- Compatibility with other systems and security solutions

10.2.7 OUTSOURCED DEVELOPMENT

SYSTEM DEVELOPMENT PERFORMED BY AN EXTERNAL SUPPLIER

AAU requires access to monitor the development process, delivery testing and documented ongoing quality assurance.

Vendor selection must be carefully considered to ensure stable development and maintenance. Functional requirements for systems must be developed, including specification of input and operational validation and network management. The ownership or usage rights to the system and information must be specified in the agreement with the supplier. Consideration should be given to whether it would be appropriate to enter into a maintenance agreement with the supplier.

EXTERNAL AUDIT OF OUTSOURCING PARTNERS

Outsourcing partners must arrange for an external audit at least once a year and must be able to present the audit certificate on request.

10.2.8 SYSTEM SECURITY TESTING

10.2.9 SYSTEM ACCEPTANCE TESTING

APPROVAL OF NEW OR CHANGED SYSTEMS

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

10.3 Test Data –

10.3.1 SECURING TEST DATA

SECURING TEST DATA

Data for testing must be carefully selected, controlled and protected according to its classification. Copying data from an operational environment to a test environment must be approved by the data owner and personal data must always be anonymized. Copying and use of data from the operating environment to testing must be logged to ensure an audit trail.

Decisions regarding the use of fully or partially complete data from an operating environment must always be documented.

11. Supplier Relationships

11.1 Information Security in Supplier Relationships –

11.1.1 INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS

INFORMATION TO EXTERNAL PARTNERS

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

ASSESSMENT AND APPROVAL OF OUTSOURCING SUPPLIER

The supplier must be able to document a satisfactory security level.

11.1.2 HANDLING SECURITY IN SUPPLIER AGREEMENTS

OUTSOURCING PARTNERS

Before entering into agreements, the security level of the partner must be clarified and approved by the system and data owners. An ISO/IEC 27001 certification, an ISAE 3402/3401 audit statement from outsourcing partners or similar relevant documentation of compliance with an appropriate security level must be available.

SECURITY WHEN WORKING WITH PARTNERS

Risks associated with the use of external service providers must be assessed and documented before establishing a collaboration, and security measures must be agreed and stated in the contract. When integrating AAU's systems and processes with third parties, the requirements for security measures are higher.

SECURITY ASSESSMENT OF THIRD PARTIES

A security assessment of relevant third parties must always be performed before establishing a collaboration with a supplier.

ADDRESSING SECURITY IN SUPPLIER AGREEMENT PROCEDURES

Relevant security requirements must be identified and agreed with suppliers who access, process, store or provide IT infrastructure for the organization's information assets. The requirements include (but are not limited to):

- Description of the relevant information assets
- Alignment of the organization's and vendors' classification systems
- Identification of regulatory requirements, such as data protection, copyright, intellectual property and industry compliance (PCI DSS, ISO/IEC 27001)
- Acceptable use policies
- Incident management and BCM requirements
- Security requirements for logical and physical access
- Security requirements for data and information exchange
- The right to perform audits
- Supplier's obligation to be compliant with organizational security policies
- Awareness and training programs.

11.1.3 INFORMATION AND COMMUNICATION TECHNOLOGY SUPPLY CHAIN

NETWORK SECURITY - OUTSOURCING SUPPLIER

The Supplier must ensure appropriate network design, firewall, segmentation and encryption.

11.2 Supplier Service Management –

11.2.1 MONITORING AND REVIEW OF SUPPLIER SERVICES

MONITORING AND AUDIT - CLOUD SOLUTION

The provider must be able to document an appropriate level of security, e.g. an audit statement, internal audit, ISOIEC 27001 certification, outsourcing audit statement or equivalent. The provider must be able to provide reporting on the extent to which agreed service goals have been met. AAU must assess to what extent own auditing of the provider is necessary.

11.2.2 CHANGE MANAGEMENT OF SUPPLIER SERVICES

CHANGE MANAGEMENT AT THE SERVICE PROVIDER

It must be ensured that change management of the service provider's services follows the same guidelines as AAU's own.

12. Information Security Breach Management

12.1 Information Security Breach Management and Improvements –

12.1.1 RESPONSIBILITIES AND PROCEDURES

INFORMATION ABOUT SECURITY INCIDENTS

AAU must inform affected parties of any information security incidents in accordance with applicable legal requirements. The head of the relevant main area or the Head of Information Security should approve such information before it is released externally.

RESPONSIBILITIES AND PROCEDURES FOR SECURITY INCIDENTS

The CISO, together with ITS, is responsible for establishing procedures that ensure a fast, efficient and methodical handling of information security breaches.

AVAILABILITY INCIDENTS

Incidents that affect availability must be resolved in accordance with applicable service level agreements (SLA). Operational incidents that cannot be resolved within the agreed time must trigger incident management procedures and contingency plans. The affected users, system and data owners must be informed.

12.1.2 INFORMATION SECURITY INCIDENT REPORTING

REPORTING OF SUSPECTED SECURITY INCIDENTS

If a breach of information security measures is detected or suspected, this must be reported immediately to the immediate manager and to ITS via the security incident form. In exceptional cases directly to ITS support (support@its.aau.dk or tel.: 9940 2020). Both AAU and external service providers are obliged to report any observed or suspected security incident. There should be easy access to reporting these incidents. All security incidents must be documented in the applicable support tool and archived according to current legislation, currently for 5 years.

12.1.3 REPORTING OF INFORMATION SECURITY WEAKNESSES

REPORTING OF PROGRAM ERRORS

Users who observe program errors that they have not experienced before must report this to support@its.aau.dk tel.: 9940 2020.

12.1.4 INFORMATION SECURITY INCIDENT ASSESSMENT AND RESOLUTION

ASSESSMENT OF PAST INCIDENTS

The Information Security Committee shall regularly review the past period's incidents and on this basis recommend whether information security can be improved. This may result in an updated risk assessment, as well as suggestions for new or changed technical, physical or behavioral measures.

FOLLOW-UP ON REPORTED SECURITY INCIDENTS

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

12.1.5 HANDLING OF INFORMATION SECURITY BREACHES

The ITS, in cooperation with the CISO, must ensure that procedures for handling information security breaches, including error remediation, controlled recovery after a breach and communication to internal and external persons, organizations or authorities, are prepared.

12.1.6 EXPERIENCE FROM INFORMATION SECURITY BREACHES

CONTROL AND FOLLOW-UP ON SECURITY BREACHES

Information security breaches and unauthorized access to systems and information must be recorded.

12.1.7 COLLECTION OF EVIDENCE

COLLECTION OF EVIDENCE

If a security breach results in legal action - whether by an individual or a company - adequate evidence must be collected, stored and presented. Securing evidence is difficult and should be coordinated with experts in the field on a case-by-case basis. A wrong approach can result in evidence being thrown out in court.

CONTACT WITH RELEVANT AUTHORITIES

The unit manager is responsible for contact with external parties in information security matters.

13. Information Security Aspects of Emergency, Contingency and Recovery Management

13.1 Information Security Continuity –

13.1.1 INFORMATION SECURITY CONTINUITY PLANNING

EMERGENCY PROCEDURES FOR CRITICAL PROCESSES AND SYSTEMS

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

FRAMEWORK FOR CONTINGENCY PLANS

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

Management must establish a consistent framework for AAU's contingency plan to ensure that it is coherent and addresses all security requirements, and that it prioritizes testing and maintenance. The contingency plan must reflect the possibility that physical locations may be inaccessible or destroyed.

13.1.2 IMPLEMENTING INFORMATION SECURITY CONTINUITY

ACTIVATION OF THE CONTINGENCY PLAN

It must be clearly defined who is responsible for activating the contingency plan. Employees who are part of the contingency plan must be informed of this responsibility. All employees must be informed of the existence of the contingency plan.

13.1.3 VERIFY, REVIEW AND EVALUATE INFORMATION SECURITY CONTINUITY

TRAINING IN CONTINGENCY PLANS

ITS is responsible for ensuring that there is adequate training of employees in the agreed emergency response procedures, including crisis management.

TESTING AND MAINTENANCE OF CONTINGENCY PLANS

Contingency plans must be tested and updated on an ongoing basis to ensure that they are up-to-date and effective. Testing contingency plans should include at least one of the following:

- A desktop test of the different scenarios.
- Simulations (to train participants to handle their roles after the incident).
- Technical restoration (ensuring that technical systems can be effectively restored).
- Restoration in other premises than the original (conducting parallel operations in other premises).

UPDATING DISASTER PLANS

At least once a year, contingency plans should be reviewed for updating.

13.2 Redundancy –

13.2.1 AVAILABILITY OF INFORMATION PROCESSING FACILITIES

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

14. Compliance

14.1 Compliance with Legal and Contractual Requirements –

14.1.1 IDENTIFICATION OF APPLICABLE LAW AND CONTRACTUAL REQUIREMENTS

STORAGE AND PROCESSING OF PERSONAL DATA

AAU has prepared a separate policy for the processing of personal data: AAU's privacy policy.

CONTROL OF COMPLIANCE WITH PERSONAL DATA LEGISLATION

The unit manager is responsible for ensuring that applicable personal data legislation is complied with locally in the unit.

TRACEABILITY

Processing of personal data must, as far as possible, be logged automatically so that it is possible for an auditor to check who has worked with what information at what times.

14.1.2 INTELLECTUAL PROPERTY RIGHTS

COPYRIGHT GUIDELINES

Management has the overall responsibility for ensuring that AAU maintains appropriate attention to the protection of third party copyrights. Each user is responsible for complying with applicable copyright laws at all times. Documentation of ownership of licenses, original material and manuals must be maintained.

Continuous checks must be made to ensure that software license agreements are complied with, e.g. that any limitations on the number of users, servers or copies are observed. Regularly check that only authorized systems with authorized licenses are installed on AAU's equipment.

ADMINISTRATION OF SOFTWARE LICENSES

Registration of software licenses is done through the IT department. It is the overall responsibility of each main area unit manager to ensure a sufficient number of licenses within their main area. The use of software licenses must be coordinated with the IT department or the person responsible for managing licenses in the unit.

Employees must not commit AAU by accepting license terms in software that have not been accepted by the individual unit. The individual units must locally register which licensed programs are available on the unit's IT systems. License registers must be updated on an ongoing basis, preferably in a specialized software solution.

14.1.3 PROTECTION OF RECORDS

STORAGE OF SYSTEM DOCUMENTATION

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

PROTECTION OF SYSTEM DOCUMENTATION

System owners must protect system documentation, which implies, among other things, that the number of access rights to system documentation is kept to a minimum and approved by the system owner.

REGULATED DATA

AAU must protect regulated information against modification, deletion and unauthorized access.

STORAGE AND PROCESSING OF DATA

Business-critical information must always be stored and processed in such a way that its integrity cannot be questioned.

14.1.4 PRIVACY AND PROTECTION OF PERSONAL DATA

Privacy and personal data must be protected in accordance with applicable legislation. Rules for storage, transmission, transfer, disclosure and deletion of personal data must be implemented and communicated to all employees, affiliated parties and students at AAU who are involved in the processing of personal data.

14.1.5 REGULATION OF CRYPTOGRAPHY

REGULATION IN THE FIELD OF CRYPTOGRAPHY

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

COMPLIANCE WITH LEGISLATION

All systems must comply with relevant legal requirements.

14.2 Information Security Review –

14.1.1 IDENTIFICATION OF APPLICABLE LAW AND CONTRACTUAL REQUIREMENTS

STORAGE AND PROCESSING OF PERSONAL DATA
AAU has prepared a separate policy for the processing of personal data: AAU's privacy policy.

CONTROL OF COMPLIANCE WITH PERSONAL DATA LEGISLATION
The unit manager is responsible for ensuring that applicable personal data legislation is complied with locally in the unit.

TRACEABILITY
Processing of personal data must, as far as possible, be logged automatically so that it is possible for an auditor to check who has worked with what information at what times.

14.1.2 INTELLECTUAL PROPERTY RIGHTS

COPYRIGHT GUIDELINES
Management has the overall responsibility for ensuring that AAU maintains appropriate attention to the protection of third party copyrights. Each user is responsible for complying with applicable copyright laws at all times. Documentation of ownership of licenses, original material and manuals must be maintained.

Continuous checks must be made to ensure that software license agreements are complied with, e.g. that any limitations on the number of users, servers or copies are observed. Regularly check that only authorized systems with authorized licenses are installed on AAU's equipment.

ADMINISTRATION OF SOFTWARE LICENSES
Registration of software licenses is done through the IT department. It is the overall responsibility of each main area unit manager to ensure a sufficient number of licenses within their main area. The use of software licenses must be coordinated with the IT department or the person responsible for managing licenses in the unit.

Employees must not commit AAU by accepting license terms in software that have not been accepted by the individual unit. The individual units must locally register which licensed programs are available on the unit's IT systems. License registers must be updated on an ongoing basis, preferably in a specialized software solution.

14.1.3 PROTECTION OF RECORDS

STORAGE OF SYSTEM DOCUMENTATION
System documentation must be retained for as long as the system is used for development, testing or operation.

PROTECTION OF SYSTEM DOCUMENTATION
System owners must protect system documentation, which implies, among other things, that the number of access rights to system documentation is kept to a minimum and approved by the system owner.

REGULATED DATA
AAU must protect regulated information against modification, deletion and unauthorized

access.

STORAGE AND PROCESSING OF DATA

Business-critical information must always be stored and processed in such a way that its integrity cannot be questioned.

14.1.4 PRIVACY AND PROTECTION OF PERSONAL DATA

Privacy and personal data must be protected in accordance with applicable legislation. Rules for storage, transmission, transfer, disclosure and deletion of personal data must be implemented and communicated to all employees, affiliated parties and students at AAU who are involved in the processing of personal data.

14.1.5 REGULATION OF CRYPTOGRAPHY

REGULATION IN THE FIELD OF CRYPTOGRAPHY

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

COMPLIANCE WITH LEGISLATION

All systems must comply with relevant legal requirements.