AARHUS
UNIVERSITET

Information security

Information security policy and rules
Version 2.0

Data classification: Public

AARHUS UNIVERSITET

Contents

AARHUS
UNIVERSITET

Rector's foreword

Dear employees and students at Aarhus University,

Aarhus University is a knowledge business. An increasing share of our knowledge is created, processed and stored on IT systems. Therefore, everyone working at AU, in other words researchers, teachers and technical and administrative employees as well as students, must have the greatest possible focus on information security.

Information security means different things to different people. This guide tries to address all the key issues involved. If you thought that information security was simply to do with viruses and hackers, you should study the policy, the rules and the procedures carefully, as the picture is far more complex.

Systematic information security rests on three main pillars – availability, integrity and confidentiality. The importance of ensuring the highest possible availability is obvious to everyone. A university – on the same lines as any modern businesses – is basically paralysed if its IT systems are down. Likewise, the entire university's work is based on our integrity, which must never be open to question, so our IT systems must always present a true and fair view. Finally, even though our role is to disseminate knowledge, we must not be blind to the fact that significant parts of our data contain sensitive or confidential information which must be protected. This applies, for example, to research data containing sensitive personal data or confidential information relating to public-sector consultancy and advisory services.

So, whatever our work at Aarhus University – be it within research, education, monitoring, consultancy, information or administration – we must always have information security at the back of our mind.

The information security guide for Aarhus University sets out the rules for information security. It is an integral part of the rules and regulations which everyone should know and comply with as a condition of being employed or enrolled at the university.

Much of the content is ordinary common sense. And things you probably already know. Now it has been compiled in a guide, which everyone is obliged to read and adhere to.

Kind regards,

Lauritz B. Holm-Nielsen

Rector

Information security policy for Aarhus University

Introduction

This information security policy sets out the overall framework for information security at Aarhus University. As part of the overall security management, the management reviews the information security policy at least once a year based on ongoing monitoring and reporting.

The policy covers Aarhus University's information, which is any information which belongs to Aarhus University in addition to information which does not necessarily belong to Aarhus University, but for which Aarhus University can be made responsible. This includes, for example, all staff data, financial data, all the data which contributes to the administration of Aarhus University, as well as information which has been passed to Aarhus University by others, including experimental and research data.

This policy covers all Aarhus University's information, irrespective of the way in which it is stored and communicated.

Purpose

Information and information assets are both necessary and vital for Aarhus University, and information security is therefore of considerable importance for Aarhus University's credibility and ability to function.

The purpose of the information security policy is to define a framework for protecting Aarhus University's information and, in particular, to ensure that the confidentiality, integrity and availability of critical and sensitive information and information assets are retained.

Aarhus University's management has therefore decided on a level of protection which is based on risk and the importance of the information based on appropriate technical and organizational level and which complies with legal requirements, Generel Data Protection Regulation(GDPR), Data protection act and agreements, including licensing terms. The management will inform staff and students of their responsibilities in relation to Aarhus University's information and information assets.

The purpose of the information security policy is also to demonstrate to everyone who has a relationship with Aarhus University that the use of information and information systems are subject to standards and guidelines. This will help to prevent security problems, limit any possible damage and ensure the recovery of lost information.

Scope

This policy applies to all employees without exception, both permanent staff and people who are temporarily working for Aarhus University. All these persons are here called "employees".

The policy also applies to students who, in connection with their studies, use information and/or information assets belonging to Aarhus University.

In outsourcing partial or entire IT operations, it must be ensured that Aarhus University's security level is maintained, so that the service provider, its facilities and its employees who have access to Aarhus University's information, must as a minimum comply with Aarhus University's information security level.

Organising information security

Aarhus University's information security organisation comprises a number of information security committees.

Operational responsibility for the daily management of information security rests with the information security manager. In cooperation with, primarily, the security committees and, secondly, the deputy director of IT, this ensures that the activities, standards, guidelines, controls and measures which are described in the security guide are implemented and observed. Likewise, it is important that information security is integrated in all business procedures, operational tasks and projects.

The local information security committees are responsible for implementing the work which is specified in the annual cycle, which is described in section 1.8.

Security level

It is Aarhus University's policy to protect its information and only allow access to and the use and dissemination of information in accordance with Aarhus University's guidelines and subject to applicable legislation.

Based on a risk assessment, Aarhus University decides a security level that corresponds to the importance of such information.

A risk assessment must be conducted at least once a year to keep the management informed of the current risk scenario. A risk assessment must also be conducted in the event of any major organisational changes which have a bearing on the overall risk scenario.

Security levels are decided in individual cases depending on the practicality of the work and financial resources. The objective of a high security level has to be balanced with the desire for the expedient and user-friendly use of IT, as well as the fact that the university performs a role in society as a supplier of freely available information.

Security awareness

Information security relates to Aarhus University's overall information flow, and an information security policy cannot be implemented by the management alone. All employees and students are responsible for helping to protect Aarhus University's information against unauthorised access, alteration, destruction and theft. All employees and students must therefore be informed regularly about information security as and when relevant. Employees and students are also required to treat the information assets which are made available to them in an appropriate manner.

As users of Aarhus University's information, all employees and students must adhere to the information security policy and the resulting guidelines. Employees and students may only use Aarhus University's information for the purpose of the work they perform for Aarhus University, and they must protect the information in a way which is consistent with the sensitivity of the information.

Breaches of information security

If an employee or a student becomes aware of any threats to information security or of any breaches, they must immediately notify the information security department.

Violation of the information security policy or of any of its rules and guidelines must be reported to the information security department which, together with the relevant immediate superior and the HR department, makes a decision on any steps to be taken. It is the responsibility of the manager to ensure that any steps taken comply with general labour laws, ensuring, for example, that the relevant union representatives are involved. Breaches by students are handled like any other disciplinary matter.

Any breaches under criminal law, the law of torts and other punishable offences will be reported to the police.

Annual cycle of information security activities

Aarhus University has drawn up an annual cycle that describes the information security work.

The annual wheel comprises five activities:

1. System and data classification
2. Risk assessments
3. Emergency planning and tests
4. Follow-up, auditing etc.
5. Awareness

The responsibility for performing the tasks lies with the local information security committees at the faculties/administration. The information security department can facilitate the process and make relevant tools available, but the main areas are responsible for carrying out the work. As the work requires sound local knowledge, it is recommended that the work is based at the departments and/or with the research groups etc.

All activities specified in the annual cycle are carried out once a year, starting with system and data classification.

Awareness is a key element in the work throughout the year. This part is handled by the information security department together with the information security committees.

Information security rules for Aarhus University

Introduction

Background for work with information security at AU	Aarhus University must, like other state organisations in Denmark, comply with and work from ISO/IEC 27001 standard, which defines a number of requirements for information security at the university. Looking forward, work will be done, so Aarhus University within a foreseeable number of years, can be certified in the ISO27000 series.
Definition of information security	Information security is defined as the measures required to preserve the confidentiality, integrity and availability of the university's information, assets and data.
Glossary	Should: The word "should" is used several times in this guide. In general, "should" = "shall/must", unless an exemption has been granted, or the costs of implementation exceed the benefits. If you deviate from the recommendation, you must either apply for an exemption or document that it is not worth adhering to. Work use: Unless otherwise mentioned, the formulation "work use" also covers use for study purposes by students. The same applies for "work-related use". Outsoucing: The word "outsourcing" covers all cases where all or parts of IT support are provided by an outside company. Outsourcing therefore also covers cloud computing, i.e. the purchase of services from a third party, for example email, web servers, computing etc. Mobile devices: "Mobile devices" is used as a generic term for mobile phones,

	smartphones, tablets etc. Portable PCs, netbooks, laptops etc. are not covered by the term "mobile devices", but are described instead as "portable PCs". Information assets: "Information assets" are all the systems etc. which contain, generate or process information. They include, for example, PCs, servers, mobile devices, portable PCs, freezer boxes, cold rooms, server rooms etc.

1. Organisation and implementation

Responsibilities must be allocated to ensure awareness of the university's information assets. The organisational structure at the university and collaboration with external partners is important to maintain a security level which is in keeping with the times. Contracts with partners and other agreements also have a bearing on information security.

1.1 Risk awareness

Risk analysis	Aarhus University classifies its systems as A, B and C systems. Type A systems require both a risk analysis and an emergency plan to be prepared, type B systems require a risk analysis to be prepared, while neither a risk analysis nor an emergency plan is required for type C systems. All identified information assets must be classified in connection with registration. System classification is determined on the basis of the data classification and an assessment of the importance of the individual assets.
Impact assessment	The consequences of incidences affecting information assets must be continually assessed.
General risk assessment	A general risk assessment must be carried out of the threats facing the university. The general risk assessment must include an impact assessment and a vulnerability assessment. The risk assessment must be updated in

	the event of significant changes to the risk scenario, however at least once a year.
Information on new threats, viruses and vulnerabilities	AU IT must set up a procedure for identifying new vulnerabilities. A responsible person or group must be appointed to handle this task. AU IT must stay informed about security within the operating systems used, and about the systems and applications being used on both the client and server side. Through the central information security committee, AU IT must inform relevant members of the management about new threats which may affect individual business units with a view to adapting their business procedures and procuring the necessary resources to counter the threats.
Handling security risks	When the risk assessments identify security needs which are not being met by the existing protective mechanisms and procedures, the information security manager must raise the issue with the central information security committee. In the case of significant/critical risks, the information security committee can demand that the owners of the affected asset(s) identify possible solution models and give higher priority to implementation. In the case of non-critical risks, the solution must be included in the normal prioritisation of tasks and projects at AU.

1.2 Information security policy

Exemption from security policy requirements	Exemptions from the information security policy are only granted for well-founded business reasons and if it is guaranteed by the respective system and process owners that this is sensible. Exemptions are granted by the central information security committee. An exemption is always granted in writing and for a limited period of time – usually one year. The user must apply for an extension, if necessary. The information security manager keeps a list

	of the exemptions which have been granted. The relevant system and/or process owner is responsible for all security incidents which happen as a direct consequence of the exemption.
Announcement of the information security policy	The security policy must be made public, and all relevant stakeholders, including all employees and students, must be made aware of the policy.
Approval of the information security policy	In the event of any changes, the information security policy must be approved by the senior management team upon recommendation from the central information security committee.
Follow-up on implementation of the information security policy	All managers must continually ensure compliance with the information security policy within their respective areas of responsibility.
Maintaining the information security policy	The university's information security policy, rules, procedures and derived documentation must be maintained by the information security manager in collaboration with relevant parties, including AU IT, the information security committees, the students and the university management.

1.3 Security implementation

Role of management	The management must support the university's information security by establishing clear guidelines, demonstrating commitment and ensuring the precise allocation of responsibility.
Coordinating information security	The information security manager is responsible for coordinating security across the organisation.

1.4 Outsourcing

Outsourcing partners	All outsourcing partners must maintain acceptable levels of security. To protect AU's IT architecture and operations, all outsourcing partners must be approved by the deputy director of IT and the information security manager. When outsourcing areas involve personal data, attention must be paid to the requirements of the Danish Act on Processing of Personal Data (*Dataloven*) and the guidelines issued by the Danish Data Protection Agency (*Datatilsynet*).
Security when outsourcing	AU's overall security must not be compromised by outsourcing. When outsourcing IT systems, information on the outsourcing partner's security level as well as the outsourcing partner's security policy must be obtained before concluding the contract.
Monitoring of service provider	The person responsible for the contract must regularly monitor the service provider. This can be done via reporting and status meetings, but in the case of major contracts, the right should be reserved to carry out supplier inspections and audits. When outsourcing, an audit statement must be requested or certification in accordance with DS484, ISO27001 etc.

1.5 Security in connection with third-party access

Partnership agreements	Access must not be granted between the university's information assets and those of external partners before a partnership agreement has been signed which, as a minimum, must include a confidentiality agreement.
Agreements on information exchange	When exchanging sensitive or confidential information and data between AU and a third party, a written agreement must be

	made. Moreover, legislation requires a data processor agreement to be made if sensitive information is being processed.
Confidentiality agreements	Definitions of the information which is covered by the agreement. A specified term. Description of what happens when the agreement expires. The signatory's responsibility for preventing violation of the agreed confidentiality. Information on copyrights covered by the agreement. A description of how the information may be used, for example which rights the signatory is granted to use of the information. The university's right to monitor and follow up on compliance with the duty of confidentiality. Procedure for notifying and reporting breaches of confidentiality. Conditions for the return or destruction of information assets when the agreement expires. Sanctions in the event of violations of the duty of confidentiality.
Security when collaborating with partners	When integrating AU's systems and processes with a third party, the system owner must ensure that the security risks are assessed and documented.
Information for external partners	It must be ensured that third parties are made aware of the expected security level, and, for example, given access to the described policies.
Confidentiality agreement for students	It must be ensured that students who are granted access to the university's sensitive and/or confidential data sign a confidentiality agreement.

2. Identification, classification and responsibility for assets

Information assets must be protected whether in the form of physical assets such as signed documents, production equipment or IT systems. It is therefore necessary to identify, classify and allocate ownership for all assets.

2.1 Handling information and assets

Accepted use of information assets	The system owners must produce guidelines for the accepted use of AU's information assets.
Storage of sensitive or confidential information on private equipment	Personally owned IT equipment such as PCs, tablets, hard disk drives, memory sticks, optical disc drives must not be used for storing sensitive or confidential data.
Use of portable media for sensitive and confidential data	Sensitive and confidential information must be encrypted when stored or transported on portable media, for example USB flash drives, tablets, mobile phones, CDs or DVDs.

2.2 Classification of information and data

Control of classified information	The central information security committee is responsible for defining a fixed set of appropriate and relevant security checks for protecting the individual categories of information. The deputy director of IT must ensure that the necessary precautions, procedures and controls are implemented in the IT department. The local management must ensure that the necessary precautions, procedures and controls are implemented in the main areas.
Responsibility for data classification	The owner is responsible for data classifying individual assets and ensuring that they are properly protected in accordance with the classification.
Classification of data and other types of information	AU's data and information, in the following "data", must be classified according to the

following scale:

Public data: Defined as data to which everyone, if they so wish, has been or can be given access. Public data may, for example, be data on public websites, brochures about study programmes etc. Generally, this data does not require any special protection, although it must be ensured that only authorised persons are able to edit such data.

Internal data: Defined as data which must only be used and communicated internally, and which in day-to-day operations is necessary for the users who need to use it. This data may include minutes of meetings, forms, invoices etc. Internal data requires a certain degree of protection. As a minimum, it must be ensured that only authorised persons have access to both read and change the data.

Confidential data: Defined as the data which only specially entrusted users can access in order to carry out their work, and where a breach of confidentiality can be detrimental to Aarhus University or its partners. This data includes applications, contracts, financial information etc. Confidential data requires a high degree of protection. Access to confidential data must be restricted to authorised persons, and the use of encryption should be considered, especially when transferring such data to external media or services. Confidential data must never be stored or processed on private equipment.

Sensitive data: Defined as data which is covered by the Act on Processing of Personal Data (*Lov om behandling af personoplysninger*). Sensitive data requires an extra high level of protection. Access must be limited to as few people as possible, and encryption must be considered. Sensitive data must never be stored or processed on private equipment, and if data is moved to external media, it must be encrypted. Please also note that it may be necessary to enter into data

	processing agreements and to notify the Danish Data Protection Agency. Read more on the Danish Data Protection Agency's website. Related procedures Classification of data
Responsibility for importance assessment	The owner is responsible for assessing the importance of individual assets and ensuring that they are properly protected in accordance with their significance for AU.
Importance of information assets must be assessed	The importance of information assets must be assessed in accordance with the applicable standard at AU. An asset must always be classified as belonging to the uppermost of the relevant categories. Related procedures Importance assessment of information assets

2.3 Owners of systems and data

Legal ownership	Generally speaking, Aarhus University is the legal owner of all data on the university's computers (servers, desktop PCs, laptop PCs etc.). However, not in the following cases: - If a written agreement has been made - If otherwise provided by applicable legislation, for example copyright rules etc. - If the data is private, for example private digital images - If the data is research data which a third party makes available to AU. The content of a student's network drives is generally regarded as being private property, unless the student is employed by AU. Network drives must only be used for study-related purposes, and AU reserves the right to monitor the use of network drives and analyse the content

	with a view to preventing misuse.
Right of use of equipment	Regardless of whether data is owned by AU, an employee or a third party, AU is free to use its own equipment as it wishes. This means that AU is entitled to delete content on a computer, network drive, USB memory stick etc. if an employee has left the university without first having to consult the employee. Likewise, AU may reset mobile phones and tablets. AU cannot be held responsible for any loss as a result of the above.
Designating an administrative owner	All information assets must have a designated administrative owner. Ownership is defined at AU as a job function which can be assigned to individual employees. At AU, ownership is hierarchically passed down from the rector through either the deans and heads of department/centre directors, or the university director and the deputy directors to the individual employees. In the event of a person's resignation or other absence, ownership reverts to the previous person in the hierarchy until a new owner has been designated.
Responsibility for personal data	The system owner of assets that contain data which is covered by the Danish Act on Processing of Personal Data is responsible for personal data.
Responsibility for access rights	The owner of an asset is responsible for creating and continually reassessing access rights. The granting of access must take place in accordance with applicable rules on e.g. passwords etc.
Administration of Internet domain names	A list must be kept of AU's registered domain names, status on use, payment information and date of renewal. AU IT is responsible for registering the

	primary domain names. The responsibility for project-oriented domain names can be delegated to local units, but AU IT must be informed of the domains.
Responsibility for data on mobile devices	The primary owner of a mobile device is responsible for data. In the case of mobile devices without a primary owner, the most recent user is responsible for removing data from the device after use. Users of the university's mobile devices are responsible for protecting the data which is processed on the device as well as for the device itself.

2.4 Data integrity

Data storage and processing	Data must always be stored and processed in such a way that data integrity is maintained. Legislation etc. may place special requirements on documenting the integrity of the information/data.

2.5 Identification and registration of assets

Identification of information assets	All the university's information assets must be identified and classified. See section 2.2

3. Staff security and user behaviour

Information security in an enterprise depends to a large extent on its employees. It is necessary to protect the enterprise through employing the right employees, training the employees in their respective job functions and security – and establishing rules on how to act in relation to security incidences and risks.

3.1 Employment and resignation

Background checks of employees	Together with the deputy director of IT, the HR department must ensure proper background checks of IT staff. Together with the unit appointing new employees, the HR department must ensure that proper background checks are

	conducted on employees who are taking up particularly responsible positions, including managerial posts.
A background check on employees should as a minimum cover:	A personal reference. The applicant's CV. Educational background and professional qualifications.
Returning assets on retirement/resignation	At the end of their employment, employees must return all assets which they have been supplied with by AU. If special agreements have been made, for example emeritus schemes, the employee can retain possession of the asset(s) until the expiry of the agreement.
Withdrawal of privileges on retirement/resignation	In collaboration with the deputy director of IT, HR must establish and maintain a procedure for withdrawing privileges in connection with the retirement/resignation or dismissal of employees. The procedure must be reviewed/updated at least once a year. The procedure for withdrawing privileges must contain a list of functions and persons who must be informed when an employee leaves his/her job. Privileges cover access to systems, buildings etc. as well as rights to undertake commitments on behalf of AU.

3.2 Separation of duties

Protecting IT systems	IT systems must be protected through a separation of duties to minimise the risk of privileges being misused.

3.3 Management's responsibility

Management's responsibility	The immediate superior is responsible for ensuring that all employees: Are sufficiently well informed of their roles and responsibilities in relation to security before being granted access to the

	university's systems and data. Are told about the necessary guidelines so they can live up to AU's information security policy. Become sufficiently aware of information security issues for them to fulfil their roles and responsibilities at the university.

3.4 Training

Security training for IT employees	All IT employees must be trained in the security aspects of their jobs. For example, to reduce the risk of incidences in connection with any privileged access.
Knowledge of classification of information	All members of staff should know how data and documents are classified. System owners, data owners and system administrators must keep up to date on classification.
Knowledge of security policy	Together with AU HR, the immediate superior is responsible for ensuring that new employees familiarise themselves with AU's information security policy. As a minimum, new employees must be given the leaflet "Information security for employees at Aarhus University". All relevant users receive regular instructions in how to comply with AU's information security policy. Existing students and employees at Aarhus University are obliged to stay informed about the applicable rules at http://www.au.dk/en/informationsecurity/ New students at Aarhus University must be acquainted with the necessary guidelines before starting at the university. The Studies Administration is responsible for ensuring this.

3.5 Logging and monitoring

General rules for logging

AU IT is entitled to log all information relating to security, operational reliability and troubleshooting.

This includes information on access or

	attempts to access systems, incidences which can impact the confidentiality, availability or integrity of AU's systems or infrastructure, network connections and activity on AU's network, email traffic and the use of various programs. Logging potentially makes it possible to trace an individual person's actions on AU's equipment and/or network.
Use of log files	It is not permitted to use log files to track an individual person's actions except in the case of enquiries concerning unlawful acts, antivirus/antispam alerts or similar security system alerts, or in cases of suspected prohibited behaviour. Therefore, AU IT does not draw up lists of the activities of individual users and does not assess whether or not the activities of individuals are relevant to their work at AU. If it is necessary to track the actions of individual users, it is first necessary to obtain permission from the person in question (for example when following up on alerts) or the person's immediate superior (for example if prohibited behaviour is suspected, cf. policies, legislation etc.). AU IT is able to use log files for the following purposes: - Statistics of e.g. email, Internet and network traffic to and from AU. - Statistics on the use of e.g. certain programs or certain types of network traffic. - Statistics related to smaller sections of AU, e.g. a department/centre or a deputy director area, as long as it is not possible to identify individual persons in the material. - Troubleshooting and alarms. - Following up on security incidents.

3.6 Code of conduct

Circumventing security measures	Trying to circumvent security mechanisms is not permitted. The conduct of unauthorised security tests is

	not permitted.
Duty of confidentiality	AU's employees are subject to a duty of confidentiality. IT employees with privileged access to information must exercise special care not to disclose information which they become aware as part of their job.
Freedom of speech	Like all Danish citizens, AU's employees enjoy the right to freedom of speech, which is only limited by the clauses of the Danish Criminal Code (*Straffeloven*) relating to slander, racism etc. AU follows the Danish Ministry of Justice's guide on public employees' freedom of speech (September 2006). Related procedures Guide on public employees' freedom of speech

3.6.1 Code of practice for passwords

Use of password-protected screensaver	As a user, you should activate the password-protected screen lock when leaving your workstation so that it is outside your field of vision. All PCs, servers and mobile devices must automatically activate the screen lock after 10 minutes of inactivity.
Reusing passwords	Employees and students must not reuse passwords for AU's infrastructure for accessing third-party systems such as websites and online banking. The use of the same password on third-party systems increases the risk that the confidentiality of the password will be violated.
Transfer of passwords	Temporary/one-time passwords may be transferred orally after checking the identity of the recipient. Temporary/one-time passwords may be sent by text message after checking the identity of the recipient. One-time passwords may be sent by email

	after checking the identity of the recipient. When sending a password by text message or email, the message or email must not specify where the password can be used.
Passwords are strictly personal	Passwords are strictly personal and must not be shared with other persons, not even IT employees.

3.6.2 Code of practice for using the Internet

Blocking Internet access	AU IT reserves the right to block user accounts and immediately disconnect a given user's computer if deemed necessary in order to maintain network security or in any other way protect operations.
Downloading files and programs from the Internet	Files may be downloaded from the Internet for work use and, to a reasonable extent, for private use, cf. the rules on private use of the Internet. Programs may be downloaded from the Internet for work use provided that the information security policy and all licence terms have been complied with and provided there is no local ban on installing third-party programs on the machine in question. Programs may be downloaded from the Internet to a reasonable extent for private use, provided that the information security policy is observed and that all licence terms are complied with. Please note that, as with all other purchases, the applicable procurement rules must be complied with.
Criminal activities – Internet access	Use of the Internet connection for criminal activities of any kind including (but not restricted to) hacking, downloading or distributing child pornography, downloading or distributing pirate software, music, films or other circumvention of copyright law is prohibited.

	Any attempt to circumvent AU's security mechanisms is prohibited. Likewise, any attempt to circumvent other people's security mechanisms using AU's Internet connection is prohibited.
Other restrictions – Internet access	Restrictions regarding access to certain applications may also apply to work-related tasks (e.g. transferring large volumes of research data), where AU IT may, for example, deem that these activities should happen outside normal working hours. If so, this will be announced via email and/or the intranet.
Commercial use – Internet access	AU's Internet connection must not be used for private commercial activities. Students and employees who have their own business outside AU may access their business from the university's network as long as it does not pose a security risk for AU and as long as existing technical measures allow this. Permission will not be granted to open e.g. firewall gateways etc. to provide access for private purposes. Students and employees must under no circumstances run private businesses from equipment on the AU network so that the business can thereby be associated with Aarhus University.
Vigilance – Internet access	AU IT does its utmost to protect Internet traffic by means of antivirus programs, firewall rules as well as regular security updates on PCs. However, these security mechanisms may be insufficient in certain cases, and all users must therefore stay informed of and be alert to threats to IT security from the Internet.
Restricted Internet use from certain machines	Please note that network access should be limited for some machines (for example, although not limited to servers, control computers for laboratory and clinical equipment etc.). For example, this type of equipment should not be used for surfing

	the Internet etc.
Waiver of liability – Internet access	If you choose to use your work PC to carry out private financial transactions (online banking, PC-bank etc.) using AU's Internet connection, you must be aware that AU does not accept liability for errors or losses of any kind.
Access and identity – Internet access	Computers connected to AU's local networks have Internet access – and will usually have IDs that refer to au.dk or other AU domains. Individual users are therefore responsible for ensuring that their behaviour on the Internet does not compromise security nor AU's reputation.
Use – Internet access	Access to WWW and other online services is primarily for activities directly related to work/studies, but AU's Internet connection may be used for private purposes. Private activities must not under any circumstances be on such a scale that they impede or interfere with the legitimate work or study-related activities of other employees or students.

3.6.3 Mail policy and code of practice for using email

Click on this link to get access to the mail policy for AU employees:

Applicable mail policy

3.6.4 Code of practice for using wireless networks

Connection to a foreign wireless network	As a user, you should exercise caution when connecting to a foreign wireless network. You cannot rely on it being secure. It is recommended that you use a VPN connection on top of the wireless network. On smartphones, tablets etc. you should be particularly careful as there is no internal firewall. In so far as possible you should use a VPN connection on top of the wireless connection.
Installing wireless equipment	Employees, students and guests must only use the official wireless networks. No equipment may be installed or used which offers secondary wireless Internet access to AU's production network.

3.6.5 Code of practice for data protection

Backup	As an employee, you must protect work-related data by making regular backups, for example by saving the data on one of the university's network drives. This ensures that the data can be restored if it is deleted or overwritten, or in the event of a disk error or if the computer is stolen.
Use of servers and network drives	AU's servers and network drives are covered by backup systems, and all data should therefore generally be stored on AU's servers.
Precautions when data	If data cannot be stored on secure servers

cannot be securely stored online	(for example data which is collected in the field or while calculations are being performed), as an AU employee you are obliged to ensure that the data is stored at the first available opportunity. Until it is possible to store the data, you should make sure that there are several separate copies of the data.

3.6.6 Code of practice for using social networking services

University's information on social networks	Social networks such as Facebook, Twitter, Google+ etc. are not closed and are not secure. Only information which can be published on AU's public websites (i.e. in the lowest classification category) may be distributed via social networks.
Misuse of information on social network services.	IT criminals use social networks extensively to obtain information about a given company. You therefore need to be careful about which information you publish about AU on the social networks, and especially whether the information can be used in connection with criminal activity.

3.6.7 Code of practice for complying with licensing rules

Commercial use – licensed software	Many of the programs which AU uses have been procured on particularly favourable terms because AU is a research and educational institution. These programs will be subject to restrictions in relation to commercial use. If you are in any doubt about whether a given application is permitted, you should consult AU IT's licence section.
External parties – licensed software	Many of AU's IT systems are only licensed for AU's own use. Therefore, it is usually necessary to purchase additional licenses if a system needs to be used by external parties – and especially if a system is being made widely available via the Internet. If in doubt, consult AU IT's licence section.

Home and private use – licensed software	Some of the programs for which AU has a licence permit installation on several machines, for example a workstation on AU premises and a laptop or a PC at the employee's home address. Generally, the licence is restricted to work-related activities, i.e. it does not cover private use, and especially not being used by the employee's family. If you are in doubt whether a private activity is acceptable, you should first consult the AU IT licence section. The individual user is also obliged to comply with the licence rules in this area, and is obliged in particular to delete all AU-supplied software on private PCs in the home in connection with his/her resignation/retirement.
Distribution and installation – licensed software	AU IT is able to help with the distribution and installation of licensed software via automatic roll-out systems. The individual user is therefore entitled to assume that if AU IT installs the program automatically, the licence will cover his/her use. Other programs, which only one or very few people are to use, are distributed differently, for example by borrowing installation media from AU IT, or through the project's own procurement of licences and media. The use of such programs is often personal and/or linked to a given machine. Thus, it is not normally possible to "lend/borrow" licences to/from other users. Employees at AU must not download or upload software which seeks to circumvent licence checks. The installation of software demo versions, for example in connection with the identification of new tools, is permitted. Trying to circumvent the demo versions' restrictions in relation to functionality and/or duration is not permitted.
Installing programs on	In so far as is possible, users must use the

workstations	programs which are offered through the automatic installation mechanisms. Self-installed programs on the university's workstations must comply with all the licence terms. Any breaches of licence terms etc. may result in disciplinary sanctions.

3.6.8 Code of practice for mobile devices

Synchronising email and calendar with mobile devices	Email and calendar functions may be synchronised with mobile devices such as tablets and telephones which are made available by AU. Email and calendar functions may be synchronised with private mobile devices such as tablets and telephones. If you want to synchronise your email and calendar functions with mobile devices such as tablets and telephones, you must accept that the device (both AU-owned and private) will be covered by the following policy: - A PIN code of min. four characters must be used. - The device automatically deletes all content if an incorrect PIN code is entered more than 25 times. - The PIN code is activated automatically after 10 minutes of inactivity.
Responsibility for data on mobile devices	The primary owner of a mobile device is responsible for data. In the case of mobile devices without a primary owner, the most recent user is responsible for removing data from the device after use. Users of the university's mobile devices are responsible for protecting the data which is processed on the device as well as for the device itself.

3.6.9 Code of practice for using cloud services

Use of cloud services	Public cloud computing services such as Dropbox, Gmail, GoogleDocs, Office365, Skydrive etc. can be useful collaborative tools for AU employees and students. Unfortunately, security is not always adequate when using these services, and it is therefore important that you use them with caution. In general, the services must be regarded as a supplement to the services which AU makes available. As an employee, you should therefore have an up-to-date copy of your data on your network drive at AU. As a student, you should always keep a copy of your data stored locally. Sensitive data must not be transferred to cloud services unless AU has signed a data processing agreement with the provider in question. Confidential data may only be transferred to cloud services by agreement with the owner of the data. Confidential data should be encrypted before being transferred to a cloud service.

4. Physical security

Physical security and access rules for guests are natural elements in the university's security policy. Physical security covers, for example, doors, windows, alarms – as well as protection of the university's physical assets, e.g. IT equipment, against burglary/theft. Access control systems are also an element of physical security, and ensure that only authorised persons are able to access the university's premises.

4.1 Technical security measures

Fire protection	Server rooms must be protected with well-dimensioned fire-detecting and fire-extinguishing equipment. Server rooms must not be used as storerooms for flammable materials. Hazardous or inflammable materials must be stored at an appropriate distance from secure areas.
Cooling	Rooms with a lot of IT equipment must be

	protected with cooling systems.
Emergency power plant	All server systems must be protected with emergency power plants which can supply power for at least 15 minutes of continuous operation to allow the systems to be shut down properly. This also includes auxiliary systems such as associated cooling plant. Business-critical systems and associated cooling plant should also be connected to emergency power plants which can maintain operation in the event of a long-lasting breakdown, for example a diesel generator.

4.2 Protection system

Environmental protection of server rooms	Server rooms, main wiring closets and similar areas must be appropriately protected against environmental events such as fire, ingression of water, explosion and similar impacts.

4.3 Secure areas

Monitoring of secure areas	AU IT must ensure that third-party work in the server rooms and other secure IT areas is monitored in so far as is possible. The manager responsible for the area must ensure that third-party work in other secure areas, for example laboratories, is monitored if sensitive or confidential data is being handled.
Information about secure areas	Information about secure areas and their functions should only be given on a need-to-know basis.
Access for service providers	Service providers may only be given access to secure areas when necessary.
Locking of main wiring closets and similar technical rooms	All wiring closets and other technical rooms must be locked. Main wiring closets and similar rooms must

	be fitted with access control so it is possible to check who has accessed the room and when.
Access to server rooms and main wiring closets	Access to server rooms and main wiring closets is subject to permission from AU IT's management, or monitoring by trusted AU IT employees. The deputy director of IT is responsible for ensuring that only trusted persons have access to server rooms and wiring closets.

4.4 Equipment security

Disposal or reuse of equipment	When equipment is to be reused, data-carrying media must be overwritten so that data cannot be recovered. Defective or worn-out hard drives or other data-carrying media from servers, photocopiers, computers, mobile devices etc. must either be overwritten or destroyed so data cannot be recovered.
Maintenance of equipment and facilities	AU IT must maintain the equipment according to the supplier's instructions. All information which is not classified as public must be deleted from equipment which is being repaired or maintained outside AU.
Securing cables	Permanent cables and equipment must be marked clearly and unambiguously. Documentation must be updated when any changes are made to the permanent cabling.
Placing of equipment	Equipment must be placed or protected to minimise the risk of damage and unauthorised access. Equipment used to process sensitive/confidential information must be located so the information cannot be seen by unauthorised persons.

Security marking of IT equipment	All equipment with a purchase cost in excess of DKK 3,000 must be clearly marked to minimise the risk of theft. In collaboration with the primary suppliers, AU IT must make efforts to ensure that equipment is marked on delivery. This also applies to mobile phones, even though they do not cost more than DKK 3,000.
Securing mobile devices and laptop computers	Access to data on laptop computers must be protected with a login password. Equipment with sensitive or confidential information must use hard disk encryption. Smartphones and similar mobile units must be locked with a PIN code etc. which is different to the SIM card code.
Use of mobile devices	Mobile devices and laptop computers must be carried as hand luggage when travelling.
Storage of laptop computers	Laptop computers must be removed, locked up or in some other way secured against theft at the end of the working day.

4.5 Guests

Guests' access	The host is responsible for the movement of guests at AU.

5. IT and network operations

Maintenance and updating of IT systems is necessary to maintain an appropriate security level for the university. The operation of IT systems includes elements of monitoring the health of the systems, updates and data backup. Most IT systems today are dependent on networks, and therefore the administration, structure, security and maintenance of networks is of crucial importance for the university. The threat of unauthorised access means that it is necessary to have clear rules concerning the use of the university's networks as well as monitoring of the infrastructure.

5.1 Daily administration

Protection of system documentation	Access rights to system documentation must be kept to a minimum. AU IT must store system documentation in

	a suitably secure way.
Securing servers	Servers must be configured so that only the necessary services are available. The above should be ensured by disabling the functions which are not necessary as well as by possibly using a built-in firewall to restrict access.
Securing workstations before use	All workstations must be secured before use. Minimum security includes the installation of the latest security patches for operating systems and programs as well as an up-to-date antivirus program.
Systems for managing passwords	The access control system must lock a user account for 15 minutes if the user has exceeded the permitted number of access attempts.
Monitoring backup procedures	The possibility of restoring data from backup systems must be tested regularly in a lab environment. In addition, data restoration must be tested after system or process changes which may affect backup routines.

5.2 Handling data media

Protection of sensitive and confidential data on data media	All data media, e.g. USB flash drives, which contain sensitive or confidential data must be encrypted.
Virus scanning of data media	AU's antivirus solution automatically scans all new media. The user does not need to do anything unless the IT system provides a specific warning or request.
Disposal and reuse of media	All data media, for example hard disks, CDs, DVDs, tapes and memory devices must be securely erased or destroyed before disposal.

5.3 Operational procedures and areas of responsibility

Separating development, testing and operation	Development and test environment systems must be technically or physically separated from the operating environment.
Backup of data on server systems	AU IT is responsible for the secure storage and backup of data on server equipment. Planning must take place in cooperation with the system owners.
Operational management procedures	Operational management procedures for type-A systems must be documented, up to date and available for operational management employees and others with a work-related need.
Antivirus products on servers	Antivirus protection must be installed on all systems, where possible.
Software updates in general	AU IT must stay informed about patches for the programs which are used to run the university's IT. AU IT must install these patches on all computers, e.g. servers and workstations, when it is deemed that the patches are necessary to maintain a satisfactory security level, or if the updates are deemed to enhance the stability of the operating environment.
Documentation	AU IT must ensure that all key systems and IT-related business procedures are documented, for example by collaborating with the system owners and process owners on the documentation.

5.4 System planning

Capacity planning	The IT systems must be dimensioned according to capacity requirements, and regularly adapted to need.
Security in system planning	In connection with system planning, it is always necessary to include security considerations. IT security requirements must be

	considered when designing, testing, implementing and upgrading new IT systems and when making any system changes.

5.5 Monitoring of systems

Capacity monitoring	All server systems with critical information must be continuously monitored to ensure sufficient capacity for reliable operation and availability. All server systems must be continuously monitored to ensure sufficient capacity for reliable operation and availability. Monitoring must reflect the system's classification.
Monitoring of availability	AU IT must continuously monitor all its IT systems. Monitoring should make it possible to document the availability of important systems. The importance of a system is decided on the basis of the system's classification.
Registration of operational status	AU IT is responsible for registering major disturbances and irregularities in the running of the systems.

5.6 Change management

Definition of change	A change is any change in a service or a system which can lead to a call to help desk, or a change which can cause a loss of confidentiality, availability or integrity.
Change management – IT systems	AU IT must have a process for handling changes to the infrastructure. The process should support recognised methods such as ITIL, COBIT, ISO 20000 etc.
Change management – other areas	The managers responsible for other assets (systems, facilities and processes) should have a procedure for handling changes which ensures that all relevant parties are

	informed of the changes.

5.7 Protection against harmful programs

Antivirus products on workstations	Antivirus software must be installed on all workstations. The program must protect against viruses, worms, Trojan horses etc. It must be possible to update signature files etc., even though the workstation is not connected to AU's network.
Updates	AU IT makes antivirus software, security updates and other protection mechanisms available, and as an AU employee or student, you are obliged to ensure that your own PC is updated. Usually, your desktop PC will be automatically updated, but you should regularly check that, for example, the antivirus program is active and up to date, and users of laptop computers have a special responsibility for ensuring that all updates have been effected. AU IT prepares guidance on this and is always available to provide help with data protection.

5.8 Content filtering

Automatic content filtering	All incoming emails are scanned for spam and phishing. Emails which are marked as spam or phishing must either be quarantined or moved to the users' spam folders.

5.9 Network management

Division of networks	AU IT must segment its networks to establish an appropriate separation between the different services, user groups or systems.
Securing networks	AU IT has the overall responsibility for protecting AU's network according to AU's joint guidelines.
Protection of diagnosis and	Physical and logical access to diagnosis

configuration ports	and configuration ports should be checked.
Remote management and administration	Remote management tools are permitted if access is encrypted using technologies such as SSH, VPN or SSL/TLS, and if permission has been obtained from AU IT. The owner of the equipment in question is responsible for any breach of security in connection with remote management.
Connecting equipment to networks	It is not permitted to connect equipment such as servers, network hard drives, printers, etc. to AU's production network without prior agreement with AU IT. Even if permission has been obtained, AU IT may require that the equipment is disconnected if it interferes with normal operations. Unauthorised equipment on AU's production networks will be confiscated.
Installation of network equipment	It is not permitted to install network equipment without prior authorisation. However, it is permitted, in cooperation with AU IT, to temporarily connect a switch for sharing a network connector for the purposes of demonstrations, meetings or the like, provided that such connections give access to the Internet only. Default values, for example administrator login, must be changed before a system is installed on the network. Network equipment may be used for teaching activities as long as it has been agreed with AU IT.
Access to active network connectors	Network connectors in publicly accessible areas where no validation is required may only provide Internet access. To access AU's internal networks, a VPN connection must be used.
Routing and network services	Employees' computers must never act as a router between different networks or offer

network services without prior permission from AU IT.

5.10 Wireless networks

Guests' use of the university's wireless networks	The guest network can and should only be used for Internet access and not for directly accessing internal systems, with the exception of services specifically intended for guests.
Use of wireless local area network	AU makes a wireless network available to both employees and students. Unencrypted and/or non-validated wireless networks only provide access to the Internet and possibly printing. To access AU's internal networks, a VPN connection must be used.

5.11 Connections with other networks

General policy for remote access	AU makes a VPN connection available to all employees at the university. Employees thus have the opportunity to work from home or while they are on the move. If you use equipment which has been supplied and checked by AU IT, you have full access to the AU network. If you are using other equipment, such as a private computer or a PC purchased independently of AU IT, access in some areas will be limited. No equipment or programs must be set up which make it possible to establish remote access to AU's networks or machines on AU's networks. In connection with special research needs, which cannot be covered by the normal VPN connection, it may be possible to make a special arrangement with AU IT and the information security manager. VPN access can be made available to external partners, e.g. consultants etc. Such a connection must be limited to the greatest extent possible to the relevant

	systems. External parties must always complete a written agreement on VPN access, which must contain a detailed description of the systems which can be accessed, the permitted method(s) of remote access, the user's signature that he/she will comply with AU's IT security rules and a signature from the responsible manager at AU who vouches for the user's remote access. Students should not have full VPN access, but only access to the services which are relevant, e.g. network drives and the email and calendar system.
Authentication	Two-factor authentication must always be used for remote access. The first factor is your user name and password, while the second factor depends on who you are and whether you are using equipment which is private or owned by AU.

5.12 Monitoring system access and use

Storage of follow-up log files	AU IT must keep logs of security and fault events on each system for at least 3 months.
Time synchronisation	All AU computer systems, including network equipment, must use the correct time. Systems which can use automatic time synchronisation must do so. Other systems must be regularly checked and set.
Error log	Errors must be logged and analysed, and any corrective actions and countermeasures must be taken.
Administrator log	All actions carried out by people with administrator rights in connection with system components (including network equipment) must be logged.

Protection of log information	Log facilities and log information must be protected against manipulation and technical error.
Follow-up logging	AU IT must log security incidents on AU's systems. A security incident is all incidents which affect either confidentiality, availability or integrity.
Incident logging	All systems must log information about access and attempted access to be able to trace unauthorised activity.

5.13 Mobile workplaces and home workstations

Security checks vis-à-vis remote equipment.	Laptops must always be protected with antivirus, firewall and access control systems. These measures must be continually updated. Mobile devices must use antivirus software if so warranted by the risk scenario.
Access to data on AU networks	For remote access to data on the university's networks, it is important to remember that sensitive and confidential information must not be stored on private equipment. In the case of remote access, you should in so far as is possible work on AU's network drive, rather than a local copy. This will avoid problems with versioning, and you can be sure there is a backup copy of the data. If it is not possible to work on AU's network drive, you should copy your work back to the AU network drive as soon as possible.
Access to applications on AU networks	Remote access to AU's applications is normally limited to standard office applications such as email, word processing, spreadsheets and the like. Further access to applications is limited /is given by the respective system owners.

5.14 Network services with login

Protection of login	All web pages that allow login must use SSL. All services which require a login must use encryption. Telnet, FTP etc. are thus not permitted. Instead, SFTP, SSH etc. must be used. If transactions take place on an internal closed network, they may be exempt from the above.

5.15 Use of cryptography

Use of encryption in connection with data storage	Sensitive and confidential information must always be encrypted when it is stored on portable equipment, e.g. laptop computers, hand-held computers, USB flash drives etc. If it is not possible to use encryption, e.g. on mobile devices such as tablets and smartphones, you should not use the device for processing sensitive or confidential data. Passwords etc. must never be stored unencrypted, neither on mobile nor stationary equipment. Passwords should be encrypted using a recognised encryption technology.
Use of encryption in connection with data exchange	Email and data which contain confidential information must always be encrypted when being transmitted across open networks.

6. Access control and methods

Access to perform actions on the university's IT systems is protected by authorisation systems. The purpose of the systems is to protect the IT systems against unauthorised changes, orders, errors and fraud. Employees and students help to protect the information assets through the correct use of the authorisation systems.

6.1 Access control to operating systems

Change of administrative passwords	Administrative passwords must be changed if an outsider finds out what the

	password is, or if, for example, an administrator leaves the university. Administrative passwords, which are only used in emergencies or in rare cases (e.g. Enterprise Admin), must be kept in AU IT's fireproof safe. These passwords must be changed after each use, and must be at least20 characters long.
Service accounts	For tasks where you do not want to change a password, service accounts must be used in so far as is possible. Passwords to service accounts must be kept in AU IT's fireproof safe and must be at least 20 characters long. Passwords to service accounts must be changed if users who know the password leave AU. Service accounts must not be used by employees for the purpose of their daily work, or as a substitute for ordinary user accounts.

6.2 Access control for applications

Limited access to information	Access for users and support staff to user system functions and information must be restricted in accordance with the defined business-related requirements and how the information is classified.

6.3 Logical access control

Required length of password	Passwords must contain at least twelve characters. Longer passwords may be required for privileged access, for access to sensitive information or to business-critical systems.
Guidelines for passwords	When creating a user or resetting a password, users must be allocated a secure, temporary password, which must be changed immediately after it is used for the first time.

	Temporary passwords must be unique and comply with the general password requirements.
Requirements for changing passwords	Passwords must be changed after no more than 730 days.
Requirements for password content	Passwords must contain combinations of at least three of the following categories: Upper case letters, lower case letters, numbers and special characters.
Choosing secure passwords	Users should follow the guidelines for choosing good passwords. Related procedures How to create a secure password

6.4 Administration of access control

Extended access rights	Extended access rights, for example for system administrators or super users in the administrative systems, must only be assigned to a limited extent and solely based on work-related needs. The extended access rights must be registered. Special user IDs must be used for the extended rights for the sake of monitoring and follow-up.
Guidelines for access control	In cooperation with the system owners, AU IT has the overall responsibility for establishing and maintaining access management procedures.
Review of user profiles	All user profiles in AU's IdM (Identity management) system (and the derived directory services) must be automatically reviewed at least once every three months to identify inactive profiles etc. which must be removed or amended.
Relocation of employees	When relocating employees, all relevant

	user rights must be reviewed.

6.5 Access control to network

Authentication when accessing network	Two-factor authentication must be used for remote access to the internal network.
Guidelines for the use of network services	Users must only have access to the services which they are authorised to use.

7. Development, procurement and maintenance

The procurement, development and implementation of new systems at the university must be controlled in order to avoid an unnecessary increase in the risk to information security. When solutions are implemented, security considerations must always be included as an integrated part of the process.

Procurement procedures	The orderer must ensure that new acquisitions are not in conflict with existing security policy requirements. Acquisitions must not lead to an increased risk of security incidents, unless the management accepts the increased risk. All new systems must be classified, and a risk assessment must be made and, possibly, a contingency plan if the system is classified as type A or B.

7.1 Security requirements in connection with procurement

Security requirements for information processing systems	The university's wishes with respect to both new and existing systems must include security requirements based on a risk assessment.
Acquisitions	Purchases of IT equipment must comply with the current purchasing agreements and/or public procurement rules.
Security requirement specifications	Security requirements must be documented in connection with all major new IT system acquisitions or IT system upgrades.
System development	In connection with system development

performed by external suppliers	carried out by an external supplier, the following questions must be considered: Does AU need to monitor the development process? Should there be a delivery test? How is it possible to ensure documented ongoing quality assurance? Should AU demand that the source code is deposited? Should AU demand the copyright to the source code?

7.2 Security in the software development environment

Aarhus University uses a broad range of systems. The following rules are therefore not a "one size fits all", but should be interpreted depending on the system's importance, and the classification of data in the system.

Protecting test data	Data for testing must be selected, checked and protected carefully and in relation to its classification. Test data must possibly be anonymised. The owner of the data must formally approve any copying of data from the operating environment to a test environment. Copying and using data from the operating environment for testing must be logged to ensuring tracking. Production data must not be used directly from the development or test environments.
Controlled access to source code	The source code for development projects must be protected against unauthorised access. All changes must be checked to ensure integrity. The source code must not be stored in the operating environment. Script code such as PHP, JavaScript, Coldfusion etc. which is not interpreted until executed, is exempt from this rule.

Migration management	Migration from development to production must undergo testing and control to ensure operating level, security level and usability prior to implementation. In addition, approved software must be protected against subsequent unwanted changes. If possible, only object-code, not source texts, should be migrated to production systems.
Security in application development	Security must be included as an integrated part of all development projects.

7.3 Integrity for programs and data

Validation of data	Data which is sent into the systems must be validated for correctness. Database security, integrity management and data validation should be used to reduce the risk of integrity being compromised.

8. Managing security incidents

Responsibility and procedures for security incidents	The management must delegate responsibility for establishing procedures which ensure a fast, efficient and methodical handling of security breaches.

8.1 Discovery and reporting of incidents

Reporting of software bugs	Users who observe a bug must report this to their local AU IT help desk.
Reporting of suspected security incidents	Breaches or suspected breaches of IT security measures must be reported immediately to the local AU IT help desk.
Reporting of security incidents	AU IT or any outsourcing partners must, once every three months, report any incidents which impact the security of key systems. The reporting should include an overview of any breaches of confidentiality, integrity and availability. Type A and type B systems are regarded

	as key systems. Also, systems with sensitive data are regarded as important systems.

8.2 Reaction to security incidents

Control and follow-up on security breaches	Security breaches, unauthorised access and attempts at unauthorised access to systems, information and data must be registered.
Process for reacting to incidents	The information security department must define telephone numbers, email addresses and electronic forms for reporting any security incidents. The information security department must establish and maintain a procedure which ensures a suitable response to people who report a possible security incident.

8.3 Follow-up on incidents

Assessment of previous incidents	At least once a year, the information security department and AU IT must review any incidents which have occurred in the previous period and on this basis recommend whether the IT security system can be improved or clarified.
Collection of evidence	If a security breach has legal consequences, regardless of whether the security breach is by a person or a company, satisfactory evidence must be collected, stored and presented.
Learning from a breakdown in security	The information security department must collect and present the incidents so others can learn from them.
Information on security incidents	AU must in a factual way inform the affected parties internally and externally of any security incidents. The information security manager and/or the deputy director of IT, should approve all external messages.

Follow-up on reported security incidents	The information security manager is responsible for collecting statistics of reported security incidents.

9. Emergency response plan and continued operation

Risk management and disaster planning aims to reduce the risk and effect of unforeseen events. Emergency plans must help maintain operations so that damage to the university is minimised.

9.1 Emergency response plans

Types of emergency response plans	AU has two types of emergency response plans. A general emergency response plan for IT operations as well as more system-specific emergency response plans for type A systems. Responsibility for the overall emergency response plans lies with the A IT team leaders. Responsibility for the system-specific emergency response plans lies with the system owners.
Testing of emergency response plans	The testing of an emergency response plan must, as a minimum, include a desk test of the various scenarios as well as regularly simulating an emergency situation with a view to training participants in how to handle their roles.
Maintenance of emergency response plans	The general emergency response plans must be updated twice a year to ensure that they are up-to-date and effective. This is the responsibility of the team leaders. The system-specific emergency response plans must be reviewed and possibly updated in the event of changes to the affected systems.
Re-establishing business-critical systems at a new location	For type A systems, the emergency response plans should reflect the fact that the physical locations may be inaccessible or destroyed, and that you should therefore be able to establish emergency operation at other locations.
Training in emergency	The system owner is responsible for

response plans	ensuring that employees receive adequate training in the agreed emergency procedures, including crisis management.
Activation of the emergency response plan	It must be clearly defined who is responsible for activating the emergency response plans. Employees who are part of the emergency response plans must be informed of this responsibility. All employees must be informed of the existence of the emergency response plans.

9.2 Backup

Backup procedure	AU IT must have an overall backup and restore strategy, which is followed for all systems unless otherwise agreed or stated in the system documentation. The backup and restore strategy is designed to ensure that regular restore tests are carried out on key systems. For systems where a complete restore is not practical, it is necessary to do random testing using random data to demonstrate that the entire system can be restored. If there are special backup requirements, for example special archiving requirements, it is the responsibility of the system owners to agree this with AU IT.
Storage of backup copies and redundant systems	Backups, backup copies and redundant systems must be placed so that accidents at the primary site cannot be transmitted to the secondary location.

10. Legislation, contracts and ethics

Many aspects of the university's activities may be covered by legislation. The university must comply with current legislation and the regulations that apply to state sector enterprises, and any reporting must be in accordance with instructions from public government agencies and institutions.

10.1 Compliance with legislative requirements

Identification of relevant legislation	The management is responsible for identifying legislation that is relevant to AU's operation, or appointing a person who is responsible for this task.

10.2 Copyright

Copyright guidelines	The management has the overall responsibility for ensuring that AU is sufficiently careful not to breach third-party copyrights. Users must not copy, convert or extract information from image and sound files or similar resources unless this has been specifically permitted by the copyright holder, or if there is an agreement with special interest organisations such as CopyDan. Users must not copy books, articles, reports or other documents, fully or partially, unless this has been specifically permitted by the copyright holder, or if there is an agreement with special interest organisations such as CopyDan, etc.

10.3 Identified acts and rules

Regulation of encryption	Cryptographic products are regulated in many countries. If encryption is used, this issue must therefore be studied closely when cooperating with foreign partners, travel or import/export.

10.4 Control, auditing and testing

Security testing	A security test must be conducted at least four times a year of the security level at externally accessible network equipment and servers. The security test must be a combination of automatic and manual tests. A security test must be conducted at least twice a year of internal security measures, restrictions, limitations and network connections. The security test can include

	both automatic scans and manual inspections. Any vulnerabilities must be evaluated and assessed. The handling of the vulnerabilities is then part of the normal job prioritisation.
Revision of security policy	The information security department must check that the security policy is implemented in AU IT's daily work, and that the rules and procedures are complied with. This should be checked at least once a year, and the result must be reported to the central information security committee and the senior management team.