RULES FOR INFORMATION SECURITY
As an Aarhus University employee, you are obliged to comply with the university’s rules for information security. This folder describes the most important rules, but it is not exhaustive. As an employee, you must keep informed of the rules, which can be found at informationsecurity.au.dk.

PASSWORDS AND PINS
As an Aarhus University employee, you will be issued with passwords for the university’s IT systems, and you will also be issued with an access card and accompanying personal identification numbers (PIN) for those parts of the university where you work. These passwords and PINs are personal, and you must never pass on either your password or PIN to other persons. If you have any reason to think that someone knows your PINs or passwords, contact AU IT and then change the codes. Passwords must be safe yet easy to remember. See how to generate safe passwords which are easy to remember as well as other helpful advice about passwords at informationsecurity.au.dk.

NETWORK DRIVES
As an employee, you have access to a personal network drive where you can save your work etc. All work-related material must be saved on the network drive. AU IT can scan the contents of the network drive with a view to preventing misuse. For backup reasons, your network drive should be your primary storage place.
INTERNET ACCESS
The university’s Internet connection can be used freely for work purposes. You may use the Internet connection for private purposes, as long as it is not of a commercial nature. It is not permitted to use the Internet connection for downloading copyright-protected music, films or other material without permission from the relevant copyright holders; AU IT may conduct checks in order to prevent misuse.

EMAIL
The university provides an email and calendar account for all permanent employees at the university. The account is primarily intended for work-related use. The account may also be used for private purposes as long as it is not of a commercial nature and will not impair the university’s reputation.

The contents of your email account are basically the property of Aarhus University – if the account is used for private purposes, it is recommended that you save private correspondence in a folder called ‘Private’.

CLASSIFICATION OF DATA
As an AU employee, you must classify your data. AU uses four classification categories:
- Public
- Internal
- Confidential
- Sensitive
You can read more about these categories at informationsecurity.au.dk.
USE OF NON-AU EQUIPMENT
Equipment and devices which do not belong to AU must not be used for storing or processing information and data which are classified as confidential or sensitive.

Apart from the above, you may use private equipment on AU’s network as long as it does not disrupt work-related use and is not of a commercial nature.

RETURNING PROPERTY
When you cease to be employed at Aarhus University, you must return any property which you have been supplied with by AU. This also covers devices and/or equipment which you have purchased for AU’s account.

BACKUP OF DATA
As an employee, you must ensure that a backup of work-related information and data is always available on a medium which is directly accessible to AU.

The best way of ensuring this is to keep all your data on your network drive or, in the case of very large data volumes, on another medium following agreement with the IT department.

DUE CARE
As an AU employee, you must always show due care with regard to information security.

As an employee, you should, in particular, be careful how you conduct yourself in the public arena.
Avoid talking loudly about sensitive or confidential matters in public places, and consider the use of a privacy filter which restricts the angle of view when working on your PC when, for example, you are on a train, at an airport or on a plane.

**SOCIAL MEDIA**
Social media are useful but not safe. Therefore you must only ever exchange publicly available data via social media.

Please note that social media are often used to obtain information about businesses and their employees, so consider whether information about AU on social media is open to abuse.

**LICENCES**
AU has many different licences which cover the university’s software use.

As an employee, you can assume that software which has been installed by AU IT is covered by a valid licence, while you are responsible for ensuring that a valid licence is available for software which you have installed.

You are not permitted to install private software on equipment which belongs to AU, including games etc., even though you have a valid licence. This is because AU has to own the licences which are installed on AU’s equipment, and, if not, AU will be held liable vis-à-vis the licensors.
HANDLING EQUIPMENT
Mobile devices, for example mobile phones, smartphones, laptops and tablets, must, because of the risk of theft, never be left unattended in unlocked rooms or in public areas. Mobile devices must be carried as hand luggage when travelling.

PCs must be protected by a username and a password, and if the device contains confidential or sensitive information, the unit must be encrypted.

Mobile phones, smartphones and tablets etc. must be protected by a PIN or similar which differs from the SIM card code.

ANTIVIRUS
All PCs which belong to AU must have an antivirus program installed. AU-installed machines will have an antivirus program, but machines which you install yourself must also have antivirus software installed. The help desk is able to assist with installation.

You must never disable an antivirus program. If it is necessary to disable an antivirus program temporarily, contact AU IT.

CONNECTING EQUIPMENT
You must not connect equipment such as servers, network hard disks, printers, wireless access points etc. on the AU network without prior agreement with AU IT.
REPORTING INCIDENTS
As an AU employee, you must report breaches or suspected breaches of information security to the help desk or to the information security department.

Program errors which occur repeatedly must also be regarded as security incidents and also need to be reported.

REMOTE ACCESS
Remote access is possible to the university’s resources, for example from a workplace at home or when travelling etc. via a VPN connection.

LOCK YOUR COMPUTER
It is important that you lock your computer every time you leave it. If you have Windows, enter Windows key+L. If your computer is not locked, it is possible for all and sundry to do what they want with your data.

If you use Mac or Linux, read how to lock the screen at informations-security.au.dk.

UPDATE YOUR COMPUTER
Errors continually occur in the operating system or software that runs on your computer, tablet or mobile phone. It is therefore important that you always update both the computer and the programs on it. Today, many programs offer automatic updates, and it is recommended that you activate this functionality.
USEFUL LINKS

INFORMATION SECURITY DIVISION
informationsecurity.au.dk
informationsecurity@au.dk

IT SUPPORT
au.dk/it