Information security – or “IT-security” – aims to ensure that you do not lose your own data or leak confidential data when using the university’s IT-systems.

By acting thoughtfully, you can avoid unnecessary frustration and waste of time, so pay attention to the contents of this leaflet.

As a student at Aarhus University, you must follow the university’s information security rules.

Therefore, you should consult informationsecurity.au.dk on a regular basis to familiarise yourself with the current rules and recommendations.

**Passwords and Pins**

As a student, you will be issued passwords for a number of the university’s IT systems, and you will receive a PIN for your student card. Do not give passwords or PIN to others – not even the IT department.

If you suspect that others have gained access to your passwords, it is your responsibility to notify AU IT, and afterwards change your password as soon as possible.

If you suspect that others have gained knowledge of your PIN, you need to contact your local buildings services offices to change your PIN.

Passwords must be safe yet easy to remember.
You will find information on how to generate safe passwords which are easy to remember as well as other helpful advice at informationsecurity.au.dk

BACKUP OF DATA
You should back up your data frequently.

Where AU provides a network drive, keeping a copy of your data there is the easiest way to protect it.

If you use one of the university's network drives as your primary storage place, you can be assured that there is a backup.

If you keep data other places, you need to make sure that a backup is made.

The content of students' network drives is considered your private property, unless you are also an employee of the university.

NB: Keeping material not relevant to your studies on the university network drives is not allowed.

AU IT reserves the right to scan the content of the students' network drives in order to prevent misuse.

Today, many use Box, Dropbox, Google Drive, SkyDrive or similar services to store their data.

These services function well in general but there is no guarantee that the data can be recovered after an IT-failure, for example.
Therefore, make sure that you have a copy of your most important data (such as your Master’s thesis) somewhere else.

Please notice that it is not permitted to store some types of university data in Dropbox or similar services. Make sure to ask your supervisor or instructor or the like before copying AU’s data to such a service.

INTERNET ACCESS
The university’s Internet connection can be used freely for study-related 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 frequently conducts checks in order to prevent misuse.

EMAIL
AU provides students with an email account. This account is used for receiving official messages to you from the university, and you are obligated to regularly check for messages.

The account is primarily for study-related use but may be used for private use, as long as it is not of a commercial nature and that it will not damage the university’s reputation.
USE OF PRIVATE EQUIPMENT
Private equipment and devices or public services, such as Dropbox, must not be used for storing or processing information and data classified as confidential or sensitive by AU. This includes data such as assignments.

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.

Before you connect your device to AU’s network, you need to make sure that your device’s operating system, programmes and anti-virus software have been updated.

CONNECTING EQUIPMENT
You must not connect equipment such as servers, network hard disks or printers on the AU network without prior agreement with AU IT. Installing network equipment such as wireless access points without prior agreement with AU IT is not allowed.
DUE CARE
As a student, you must always exhibit due care with regard to information security.

You should in particular be careful of how you handle information you get through your studies or time spent at AU. For example, special rules apply for confidential or sensitive information.

LOCK YOUR COMPUTER
It is important that you lock your computer every time you leave it.

If you do not lock your computer, anyone could misuse your account or delete important files such as assignments.

Please notice that AU is a public place where most spaces are accessible for all.

Consider the risk of theft before leaving your equipment unattended.
SOCIAL MEDIA
Social media can be useful but are not necessarily safe.

This is why you should think about what you write on pages such as Facebook.

Data belonging to AU may only be shared on social media if it is public information.

IF SOMETHING GOES WRONG...
We all have a shared responsibility for information security at AU.

If you become aware of a security breach, you should immediately report it to AU IT Helpdesk or the Information Security department.
USEFUL LINKS

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

IT SUPPORT
au.dk/it