AARHUS BSS
DEPARTMENT OF BUSINESS DEVELOPMENT AND TECHNOLOGY
AARHUS UNIVERSITY

Guidelines for **IT and information security** at AU and BTECH

All employees at AU, be they researchers, lecturers and technical/administrative staff as well as students, must focus extensively on information security. In practice, this means all information for which AU can be held accountable: E.g. **experimental and research data, employee data, data on financial matters, all data related to the administration of Aarhus University as well as information entrusted to Aarhus University by third parties in connection with research projects**.

On the following page, you will find guidelines for what you are expected to do in order to comply with the university's rules for information security.

Find more information, contacts, etc. here:
informationsecurity.au.dk

1. Read AU's information security folder, which you will find in your pigeonhole at campus. It is also available here:

   https://medarbejdere.au.dk/en/informationsecurity/informationsecuritypolicy/

2. Make sure to lock your computer when you leave it. This also applies to your mobile, tablet, etc. if they contain sensitive and confidential information.

3. Your computer must be encrypted. Not sure if it is? Learn how to find out here:

   https://medarbejdere.au.dk/en/administration/it/guides/security/data-encryption/

4. If you are using USBs, external hard drives, etc., for other purposes than teaching material and presentations, they must be encrypted. Ask IT support if you are not sure if the devices are encrypted or not.

5. Always lock your office when leaving it.

6. Papers with sensitive and confidential information, key cards, keys, etc. must not lie on desks, bookshelves or other places that are not locked – this also applies if the office door is locked.

7. Dropbox, Google Drive, etc. must not be used to exchange sensitive and confidential information or research data. As of the autumn of 2019, however, all AU staff have the opportunity to use OneDrive, as AU has entered into a data processing agreement with Microsoft. Furthermore, unencrypted emails cannot be used to exchange research data or sensitive and confidential information. Read more:

   https://medarbejdere.au.dk/en/informationsecurity/email-policy-for-employees/

8. You must be able to identify if the data that you are working with are public data, internal data, sensitive data or confidential data – and how such data must be protected:

   https://medarbejdere.au.dk/en/informationsecurity/classification-of-data/

9. AU IT ensures that all network drives are always backed up. Therefore, you should always save your data on AU's network drives. If you are saving data locally on your computer, a removable device or a foreign test server, for instance, you are obliged to ensure that your working data are properly backed up.

10. Should you lose your computer or other AU IT equipment, contact AU IT as soon as possible. This also applies if you are hacked, your data get stolen or your email account is compromised.

11. If you become aware of an information security breach (e.g. material on AU's web that should not be publicly accessible or if a user of an AU IT system has access to information that they should not have), contact IT support as soon as possible.

12. Set aside time for watching AU's 12 videos that explain briefly (1 minute each) how AU employees should address the issue of information security:

    https://medarbejdere.au.dk/en/informationsecurity/

As a **researcher,** you must pay special attention to information security when starting projects and acquiring IT equipment and software for research projects.

Read about data protection and data processing agreements, https://medarbejdere.au.dk/en/informationsecurity/data-protection/in-particular-concerning-research/, and find inspiration for Data Management Plans (DMPs) in connection with research projects, https://www.deic.dk/en/data-management-plans-dmp-online.