AALTO IT QUICK GUIDE TO INFORMATION SECURITY

Information is the most important and most valuable property of any organisation.

Take good care of information
Make sure that your important files have been backed up. Always keep your files in the network folder. Do not leave printouts lying around on the printers when using shared network printers. Recognise confidential information and remember to store and destroy it in accordance with the relevant guidelines. Remember to log out after using software and computers.

Protect your equipment and surroundings
Make sure that the security software of your computer is working and updated regularly. Do not leave your laptop in a visible spot in an empty car. Use an automatic screensaver with a password prompt. Make sure that the information on the screen of your workstation is not visible to others. Remember to lock the door even when you only leave the office for a short while.

Find out about the origins of information, files and other material before use
A message may contain malware or be forged. The name and address of the sender or who s/he claims to be do not guarantee anything. Do not install programmes unless you are sure that they are safe. Do not open any files if you are not sure about their origin or nature. Be careful not to open any links and websites you are unsure of. Before disclosing any information, make sure that the person requesting the information has the right to obtain it.

Be cautious and follow rules in your own work
When you send something articulate clearly what it is you are sending. Remember to also delete so-called hidden data. Consider carefully before giving your e-mail address to anyone or publishing it. Have a healthy suspicion of anyone asking for information without expressly stating why they need it. Get to know the Aalto University guidelines on the use of systems and on data management and act accordingly.

Pay attention to how and where you give information about yourself and Aalto
Be careful about the way you write in the social media. Remember that any material you submit cannot be recovered. Messages are easily misunderstood; do not comment in the name of the university unless it is part of your job. Consider carefully before sharing inside information about the university.

Choose a good password and keep it to yourself
Choose a strong password with both upper and lower case letters, numbers and special characters. Do not disclose your password even to the system administrators or your family members. Any requests for your passwords are always frauds without exception. Familiarize yourself with the password guide. Use different passwords for university IT Services and other services.
Be cautious also when travelling
Consider what and where you can talk about the university. Only use secure wireless networks. Use the locking feature of your smartphone. Do not keep the Bluetooth connection on unduly. Since data sticks are easy to misplace, do not store any confidential information on them. Be cautious also about other people's data sticks.

If something goes wrong, don’t panic
Often panicking only makes things worse. Contact Service Desk and wait for advice. (09) 470 24550, servicedesk@aalto.fi, security@aalto.fi. If you have reason to suspect that someone has had access to your password, change it using another computer.

Do not hesitate to notify us!

Links

Inside – Intranet for Aalto staff
Into – For Aalto students
Aalto IT guidelines
Inside – Information Security
IT Policies and Guidelines
Policy of information systems usage at Aalto University
Password guideline
Policy on email handling at Aalto university for students
Policy on email handling at Aalto university for units and employees
Ownership of the information systems
Guideline for the validity of the access rights in Aalto university’s information systems