SecurIT

Information Security at the IT University of Copenhagen

IT DEPARTMENT

Table of Contents

1: When working at ITU

The IT network and services at ITU is a digital community that you as an employee, student or external party have become a part of and must help keep sound. It is important to protect the IT systems and data at ITU, to avoid systems and services being hacked or crashing. It is vital that personal information about our employees, students and anyone else that we hold information about is protected against unintended sharing of information, theft or destruction. Every day the IT department strive to keep the network and servers at ITU secure and protected. However, we need your help to do so!

ITU asks you to take responsibility in helping to secure the network and data at ITU, by:

- Protecting the devices you are responsible for
- Protecting the data you are processing
- Protecting your identity from being compromised

Read this pamphlet and follow its guidelines where applicable.

It´s that simple!

Code of conduct for the IT University of Copenhagen

I. ITU's network, equipment, and services are to be used to facilitate the exchange of information consistent with the academic, educational, business, and research purposes of the university. As a user of ITU's network, equipment and services you are expected to conduct yourself in a manner that does not interfere with or harass individual or institutional activities.

II. As a user, you must always exhibit good behaviour and responsibility by applying common sense, decency and courtesy in connection with the use of IT systems and network.

This includes abstaining from:

- Appropriating system rights for which you is not approved
- Threatening or violent behaviour when communicating
- Downloading and/or sharing offensive, rude, obscene or harassing material
- Political, commercial or discriminating purposes
- Illegally downloading and/or sharing material protected by copyright or intellectual property rights
- Illegally downloading and/or sharing material that violates applicable laws and regulations
- Disturbing the services of central servers and networks, causing unreasonable pressure on IT system resources, or otherwise causing unnecessary inconvenience to the other users, for example by performing network or port scans on the network.
- Tampering with any physical installations at ITU

Please consult the IT Department if you have any doubt as to whether you are permitted to perform an action.

III. As a user, you must not encourage, collaborate in, or tolerate the violation of this Code by any other person. It is ITU's policy that anyone with knowledge of violations or suspected violations must report this information to the Information Security Function via IT@ITU.dk or SecurIT@ITU.dk.

2: When logging on to the ITU Network

As a user, you are responsible for your own user account, for the IT equipment that you have been provided with, and for maintaining the appropriate security level when using IT systems and accessing data.

We ask you to create strong passwords and use MFA whenever possible.

Take note that ITU permits users to apply their user accounts for personal purposes, provided that such use does not affect the day-to-day operation.

Remember to secure your password by:

- Always keeping your ITU passwords as a secret – even from your spouse and the IT Department!
- Never writing down your ITU passwords in clear text or keeping them in an unsecure manner – so… no post-it's in the drawer or on the screen!
- Changing it immediately if you suspect a compromise or leak at www.itu.dk/password and contact the IT Department.
- Never using the same password for multiple logins – consider using a password manager.
- Always locking your screen or logging out completely when leaving your computer unattended, as you never know how long you will be gone or who will enter your office!

Read the policies and guidelines for Information Security at ITU, such as the password policy for ITU.
Check out ABC, Tools & Guides / Information Security.

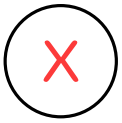
3: When browsing the internet

Always think before you act when browsing the internet or downloading applications or files. If something seems too good to be true... It most likely is! Consider that when something is free of charge, you will pay some other way – most likely with your personal data, or even worse someone else's personal data!

This includes:

- Never use your ITU passwords to log into services on the internet.
- Only download material from trusted sites.
- Always be aware of where you are! You might unwittingly have been redirected to a website that looks right – but is fake, and filled with malicious code.

For example: www.itu.dk 

www.itu.com 

Be advised that all networks are monitored for maintenance and security purposes.

4: When using your e-mail

To comply with GDPR, the following has been decided:

- Sensitive personal data must be sent using either SecureMail (Outlook) or "Send Sikkert" (F2).

- Setting up automatic forwarding or redirection of emails is **not allowed**. This is to avoid transmitting sensitive personal data over an unsecure network.

- If necessary, you can send private emails from your ITU user account, however, private emails must be kept separate from your work emails. To achieve this, we ask you save private emails in a separate subfolder with a title that clearly indicates a *private* folder, as well as add "Private" in the subject field.

In addition, please keep the following best practices in mind:

- When sending a mail to multiple recipients, use "Bcc" instead of "To"

- Avoid writing personal data in the "Subject" field

- *Most cyberattacks starts with an email!* Be aware of emails, especially with attachments or links, from unknown people as they often pose a security risk.

If in doubt – contact the IT Department.

5: When working with Personal and Confidential Data

Please refer to the ABC, Tools & Guides/GDPR/Toolbox/SOP's for ITUs policies regarding processing personal data.

Personal and otherwise confidential data – whether it is digital or on paper – must be protected at all times. Remember to:

- Clear your desk and lock away paper containing personal or confidential data when you do not need it.
- Lock away your computer and/or your phone when leaving the office for an extended period such as vacation, conference etc., or bring it with you.
- Clear meeting rooms of papers and wipe whiteboards that contain personal or confidential data.
- Use the designated special bins found in the printer rooms, when throwing away papers containing personal or confidential data.
- Minimize or close digital documents containing personal or confidential data when you are not working on it.
- Think twice before providing sensitive or confidential information to others, and take care to provide only the required and necessary information.
- Take care not to discuss sensitive or confidential information in office areas or hallways. Use the phonebooths or meeting rooms.
- End system sessions when leaving the device.
- Avoid taking papers or digital media such as USB sticks, CDs, etc. containing personal or confidential data with you when you leave the premises.

6: When accessing the ITU Wireless Networks

You must always use a secure method to log into the ITU network. Depending on what you need to access, use ITU's secure VPN solution or SSH.

Installing the eduroam Configuration Assistant Tool (CAT) gives you access to the eduroam network, a secure wireless network that you can use not just at other Danish educational institutions, but also at educational institutions in more than a hundred countries. This means that you can have instant access to your regular systems and data.

Please refer to the Administrative ABC/IT services/Wireless internet for more information, or come visit us at the IT Helpdesk.

7: When working outside the ITU network/from home

When working on your ITU device outside the ITU network, we strongly advise you against using free wifi especially if there is no password, without using the ITU VPN solution, as the risk of getting malware on your device will be greatly increased. If you do connect to a public or free wifi, delete the connection after use.

When working in a public place or at home, remember to protect your data from others looking over your shoulder and reading along.

Take care to protect the physical device by not leaving it unattended in public, or in plain sight through windows.

Avoid using unknown USB devices or power chargers with your own device, as this is the most common way to infiltrate a network.

In case you have brought papers or a USB device containing confidential data, remember to keep it with you or otherwise secure, and if necessary, dispose of it in a secure manner.

When working from home, we strongly recommend that you change default passwords on your router and other network devices to keep your network more secure.

Please remember that your device is a tool for work, not for your kids to play on.

8: When travelling with ITU devices

When travelling with ITU supplied devices, the advice listed in section 6 and 7 still applies.

Depending on the destination, however, further precautions may be necessary for minimizing the risk of cyber-crime and cyber-espionage. ITU has identified the following Cyber Risk Countries:

China	USA	North Korea
Russia	Iran	Belarus

For Cyber Risk Countries there is an elevated risk of several scenarios, such as:

• When entering the country, you can be met with a demand, that you log into your device and entrust it to their custody, before being allowed into the country. This makes it possible for them to install spy- or malware, as well as copy your data.

• Third parties, e.g. government agencies, might monitor hotel or conference wireless connections.

• Since hotel staff always have access to the locked safe deposit box in your room, they can be forced to give third parties access to the contents.

If you are in doubt or have questions, contact IT@ITU.dk before travelling.

When travelling to a cyber risk country you are responsible for taking the following precautions:

Before you leave:

- Review and bring only the necessary devices on your travel.
- Verify that encryption is enabled locally on all devices that you take with you.
- Find and delete sensitive information locally on all devices that you take with you.
- Store necessary sensitive information on an encrypted USB stick.
- Remember to bring your own charger or power bank.
- Make sure your PC and mobile device is updated with the latest security patches.

During your stay/travel:

- Do not leave your PC, mobile device or printed information unattended, even in your hotel room.
- If you have stored necessary sensitive information on an encrypted USB, keep it on your person when in transit.
- Always log on through ITU's VPN.
- Consider using a privacy filter if you plan to work in public areas.
- Do not insert or use unknown usb devices, power chargers, power banks etc.
- If you have been forced to state your password, change it as soon as possible.
- Be aware of potential recording devices including phones during meetings.

Upon your return:

- If you suspect that your passwords may be compromised, change your passwords for all devices that you brought with you as well as for services you have accessed (i.e. LinkedIn, your Bank, School Intra, etc.).
- Consider changing your passwords in any case - just to be sure.
- If you have been forced to surrender a device, do a factory reset to clean your device.
- If your USB device has been inserted into someone else's device or left unsupervised, destroy it.

9: When storing data

ITU offer a variety of storage solutions. However, depending of the type of data that you wish to store, not all storage solutions are permissible to use. You can read more in the Administrative ABC on the intranet – search for "Storage on drive" – as well as on the ABC, Tools & Guides/GDPR/Storage of personal data.
Always remember that sensitive personal data must be stored in a secure manner and shared with as few people as possible. This also applies to personal data used in a scientific or statistical project.

For non-confidential/non-sensitive data and pseudonymized personal data
All ITU approved storage solutions can be used, but if access can be given to others, especially third parties, remember to restrict the use of personal data to only the necessary data.

For Confidential or sensitive data
As a rule you must use an ITU approved administrative system to ensure the appropriate level of access management and restrictions. For several systems you can store confidential or sensitive data for up to 30 days before deleting or archiving. This applies to e-mails, ITU files, OneDrive, and in some cases MS Teams.

For confidential or sensitive personal data never use
- Privately owned devices like laptops, phones, and tablets
- Public cloud services like Dropbox, Google drive, SmartSheet etc. unless specifically approved by the Legal Department at ITU.

Be aware that ITU requires you to use the backup solutions delivered by the IT Department. It is your responsibility to make sure your data is placed on the appropriate services. Check out the Administrative ABC/IT services.

10: When using private IT equipment

All private IT equipment including entities and peripheral equipment connected to the network at ITU, are covered by the same rules as IT equipment supplied by the IT Department.

Connection of own devices (laptops; phones; tablets) requires you to authenticate and register the device the first time you attempt to gain access to the network.

Connection of own network equipment such as routers and switches on the ITU network require prior permission from the IT Department.

If you are accessing your ITU mail, calendar and/or network drive with your own equipment you must make sure your equipment is authenticated and protected by:

- Access control e.g. a strong password or a pattern code.
- Anti-virus software
- Encryption
- The current ITU VPN solution
- MFA

When you stop using your device remember to make sure that all ITU related applications and data have been deleted.

Be aware that you are not allowed to access ITU mails on a private IT device or an ITU supplied mobile phone if you receive confidential or sensitive personal data on a regular basis in your mailbox.

11: Security incidents

A security incident can take various forms and utilize different methods.

Malicious attempts

Can occur via your e-mail, a website or a USB key left in the parking lot.

- Phishing e-mails – attempting to get information e.g. passwords.
- Ransomware – encrypting data and holding it for ransom.
- Malware – worms, Trojan horses etc.

Unintentional access to sensitive or confidential personal data

- Receiving personal data in a mail/on a USB key (e.g. names, CPR numbers, or sensitive data such as health data).
- Access to files in e.g. F2 that should be inaccessible to you.
- Access to documents with personal data due to a collaboration with others.

Everyday actions to avoid

- Leaving your device unlocked and/or unattended.
- Writing or printing personal data on paper and leaving it unattended.
- Tossing paper with personal data in the wastepaper bin without shredding it first.

The IT department and Information Security Function reserves the right to contact you with a request for action if a security vulnerability or breach has been detected. It is expected that all users immediately take the necessary action.

12: How to respond to a security incident

Malicious attempts

• Forward the e-mail to it@itu.dk, then delete it.

• Warn your friends and colleagues.

• If you have clicked on something you should not have, or your device starts acting strange – contact the IT Department immediately at it@itu.dk.

Unintentional access to sensitive or confidential personal data

• Contact the owner of the data, making them aware that you have received / have access to their personal data.

• Immediately notify the Information Security Function at it@itu.dk or the DPO at dpo@itu.dk.

• If access to data was via an e-mail – make sure not to distribute the email to others and delete the e-mail when asked to do so by the DPO.

Everyday actions to follow

• Always remember to lock your device or log out completely when leaving it unattended.

• Paper containing personal data must be handled securely at all times.

• Change your password immediately if you suspect it has been compromised.

Let's keep the hackers guessing!

Remember: Never disclose your password in any written or verbal form. Not even to the ITU IT Department.

13: How to protect your key card and entrance into ITU campus

As a user, you have been given a key card and a key to access the ITU building and secure areas, based on your affiliation. The key card and key are personal and must be kept safe. One way to ensure that is to make sure your key card is not visible when leaving the ITU building, especially if travelling with public transportation. This reduces the risk of social engineering.

Please wear your ITU ID card visible at all times.

In the event that you lose the key card or the key you must report this to FM immediately.

The key card and the key must be returned when you end you affiliation with ITU.

When entering a locked area with your key card or key, take care to avoid any strangers following or tailgating you into the area.

14: Training and awareness

ITU conducts training and awareness activities concerning Information Security on a regular basis. As a user at ITU, you are responsible for keeping up-to-date on current policies and participate in relevant training.

15: Where to find more information

Information Security policies and guidelines can be found on the ITU intranet under:

- ABC, Tools & Guides/Guides/Information Security
- Administrative ABC/IT services

16: Contact the ITU Information Security Function

Mail: SecurIT@itu.dk

Phone: +45 72185261

Text: Lilian Schelde Baunbæk
Design and graphics: Eva Louise Christensen, Julie Christine Binau

April 2021

Rued Langgaards Vej 7
2300 Copenhagen S