IT DEPARTMENT

IT SECURITY MANUAL

IT UNIVERSITY

INFORMATION SECURITY POLICY

IT University of Copenhagen
Version 1.1
October 2012

The IT security manual - IT users - was last updated and approved by the IT Security Committee in October 2012

Rued Langgaards Vej 7
2300 Copenhagen S

IT DEPARTMENT

Table of Contents

1 Introduction

This manual describes the applicable guidelines for the use of IT systems and data at the IT University (hereafter ITU). The general guidelines are described in the IT security policy.

Guidelines described in this manual are primarily aimed at both students and staff of the ITU. In some cases guidelines will only apply to staff. This will appear clearly from the context.

2 Rules of conduct for the use of networks

2.1 Risk impact assessment

It is the general view of the ITU that the IT equipment of the university should be used as much as possible but within the specified guidelines. This means that the staff and students at ITU must have a professional approach to the use of IT and the equipment provided. The following guidelines apply to the use of the IT equipment of the university:

- Users must always exhibit good behaviour and responsibility in connection with the IT systems. Users should consult the IT Department if they are in doubt as to whether they are permitted to perform an action.
- Tampering with the physical installation, including cabling, is not permitted. As an example, a user may not remove a network cable to obtain network access on the user's own laptop.
- The IT systems are a shared resource, and users are under a duty to use only a reasonable proportion of the resource. Users are not permitted to disturb the services of central servers and networks, cause unreasonable pressure on IT system resources or otherwise cause unnecessary inconvenience to the other users. You are therefore not allowed to perform any types of network or port scans on the network.
- Connection of own network equipment such as routers and switches on the ITU network require prior permission from the IT Department.
- Access to the internal network from locations outside the university must take place by the use of username/password via an encrypted tunnel (such as VPN or SSH). Any exception to this rule is temporary and requires formal approval from the IT Department.
- If a user causes damage to the IT University's systems or network, the options for holding the user liable will be investigated. See section 10. Sanctions in case of violation.
- ITU offers access to parts of the network and Internet access for equipment brought by users, such as laptops, mobile phones and tablets. The guidelines described above in this security manual also apply to the user's own equipment connected to the network. See section 8. Use of private entities and peripheral equipment on ITU's network.

2.2 Risk impact assessment

The IT installed at the ITU is logically and physically divided into several networks. The purpose of the division is to safeguard against the spreading of viruses.

2.2.1 ADM network

For staff, there is a network segment on each floor (ADM networks). ADM networks can only be accessed from computers that are installed and configured by the IT Department and, following prior agreement with the IT Department, from self-administering and portable computers.

Connection to an ADM network is only possible from special network sockets opened by the IT Department, mainly from staff offices and, in individual cases and for short periods of time, from computers in conference rooms, etc. The ADM network offer direct access to the IT University's services such as file servers, database servers, financial system, etc., and to the Internet.

See section 3. Rules of conduct for the use of Internet

2.2.2 STUD network

A number of network segments are available for educational purposes. Each classroom has its own STUD network, and an additional network covers the entire building: group study rooms, thesis workstations and computers installed by the IT Department on balconies. The STUD network offer direct access to a large number of ITU services such as file servers, database servers, etc., and to the Internet.

See section 3. Rules of conduct for the use of Internet

2.2.3 ITU Network

ITU are the wireless network for staff allocated a computer from the IT Department. To access the wireless network, users need to log in with their username and password.
Staff logged into the ITU will have the same access as in the ADM network.

Access is logged and misuse of the wireless network is traceable to individual persons. Misuse may result in sanctions, see section 10. Sanctions in case of violation.

See also section 3. Rules of conduct for the use of Internet.

2.2.4 ITU guest network

The ITU guest is the network provided for guests, consultants, conference participants, etc. To obtain access to the wireless guest network, guests are required to fill in an electronic form stating their name, telephone number and who they are visiting at the IT University. The user will then receive a text message with a username and password which are valid for 24 hours. The guest network only gives access via port 80, 443 and certain VPN ports. Users will thus have access to the Internet, but not to the services at ITU.

Access is logged and misuse of the wireless network is traceable to individual persons. Misuse may result in sanctions, see section 10. Sanctions in case of violation.

See also section 3. Rules of conduct for the use of Internet.

2.2.5. EDUROAM network

EDUROAM is the network to students and guests from institutions connected to EDUROAM. Access to EDUROAM requires login with username and password. IT University students who use EDUROAM at the ITU will have the same access as in the STUD network. Guests using EDUROAM at the ITU will have the same access as in the guest network called ITU guest.

Access is logged and misuse of the wireless network is traceable to individual persons. Misuse may result in sanctions, see section 10. Sanctions in case of violation.

See also section 3. Rules of conduct for the use of Internet.

3 Rules of conduct for the use of Internet

3.1 Access to Internet surfing

All networks (STUD, ITU, ADM, GUEST and EDUROAM) allow Internet access. Internet access may not be used for:

- Downloading of offensive content.
- Threatening or violent behaviour.
- Illegal activities.
- Illegal downloading and sharing of material protected by copyright.

All networks are monitored. In case of violation of the above, sanctions may be applied as described in section 10. Sanctions in case of violation.

3.2 Web browser security settings

When visiting web sites on the Internet, the browser's security setting should reflect that the Internet is, by definition, not a safe place, regardless of the browser used.

It is not permitted to circumvent or breach the security measures.

3.3 Program execution in connection with Internet surfing

It is permitted to execute browser-based programs if these are digitally signed so the supplier is clearly identified.

3.4 Use of MSN Messenger and other chat programs

It is permitted to use MSN Messenger or other chat programs such as AOL Instant Messenger, Facebook Messenger, Yahoo! Messenger or ICQ on the network.

3.5 File download from the Internet

It is not permitted to download files from the Internet unless they are specifically scanned for viruses. See section 3.6. Use of antivirus software.

3.6 Use of antivirus software

Work stations have antivirus software installed that will automatically scan downloaded files and the hard drive for viruses. It is not permitted to disable or uninstall the installed antivirus software unless there is a work-related need to do so.

Users who bring their own computer and connect it to the ITU network are personally responsible for ensuring that their computer is appropriately protected by up-to-date antivirus software.

3.7 Terminal sessions for remote access

It is recommended to use encrypted sessions such as Secure Shell (SSH) and/or VPN for remote access.

4 Rules of conduct for the use of e-mail

4.1 Ownership

ITU considers all e-mails to be university property.

4.2 Employees' private use of e-mail

ITU permits the use of e-mail systems for private use if the IT security policy is followed. However, it is recommended that staff refrain from using their ITU e-mail for private use and instead use a private e-mail account.

4.3 Employees' private use of e-mail

Staff are advised to exercise caution in relation to attached files and not open these uncritically.

4.4 E-mails containing confidential and/or sensitive personal information

E-mails containing confidential and/or sensitive personal content must be protected in accordance with the Act on Processing of Personal Data (persondataloven) and the Executive order No. 528 of 27 June 2000 (sikkerhedsbekendtgørelsen).

Therefore e-mails containing confidential and/or sensitive personal information must not be forwarded or sent outside of the ITU network (e.g. by sending Social Security numbers to a Gmail or Hotmail account).

If confidential and/or sensitive personal information have to be sent to an e-mail address outside of the ITU network, the e-mail must be encrypted with a recognized and strong encryption algorithm. For example, using digital signature or NemID.

All ITU e-mail accounts are considered to be within the university's network. All other e-mail accounts are considered to be outside the university's network.

4.5 Deletion of e-mails

According to the Danish Executive order No. 528 of 27 June 2000 (sikkerhedsbekendt-gørelsen) and the DPA's (datatilsynet) security instructions the data controller must set up rules regarding the deletion of mails containing confidential and/or sensitive personal information if the audit requirements in §19 cannot be implemented. Read more at (in Danish only): https://www.retsinformation.dk/Forms/R0710.aspx?id=842

Detailed information about this regulation can be read at the following link, section 3.4.2.4. (in Danish only):
http://www.datatilsynet.dk/afgoerelser/seneste-afgoerelser/artikel/behandling-af-personoplysninger-i-cloud- loesningen-office-365/

4.6 Access to e-mails and documents

In case of operational problems and security events, system administrators and network managers may need to access e-mails. This will only take place with the written permission of the Vice Chancellor or by acceptance from the user. To prevent private e-mails from being read, they must be clearly marked 'private' in the subject field.

System administrators and network managers have access to exchange registers, servers and back-up copies.

System administrators and network managers are subject to a duty of confidentiality as long as no misuse is found.

5 Rules of conduct for the use of user accounts and passwords

5.1 Use of user accounts

The user must be approved by the ITU to have a user account created. To be approved, the user must be either a student, enrolled at the ITU, registered as staff or found in the alumni register. However, rare exceptions may be made to this rule.

Users of the IT systems of the ITU have a *user account* with a *username*, which is protected by a *password*. Holders of user accounts must comply with the following guidelines:

- Users may not appropriate system rights for which they are not approved. If a user finds a security flaw in the systems, the IT Department (it@itu.dk) or the IT Security Function(security@itu.dk) must be promptly notified thereof.
- As a user you are responsible for your own user account. The password for the user account is personal and must never be disclosed to others, not even staff or to the IT Department.
- User accounts may be subject to certain restrictions, such as space restrictions on file server and e-mail server. Such restrictions (also called quotas) must be observed at all times.
- A user account may only be applied for the purpose for which it was created. For students the purpose is mainly to carry out study activities, and for employees it is mainly to carry out work tasks.
- The IT University permits users to apply their user accounts for personal purposes as well, provided that such use does not affect the day-to-day operation. Users are not permitted to apply their user accounts for commercial purposes, for discrimination or for any other purpose that may harm the ITU or users of the ITU systems.

5.2 Password policy

Users at the ITU are personally responsible for choosing and using the password(s) required for access to IT systems and data.

The current password policy is as follows:

- Your password must be at least 8 and at most 256 characters long.
- Your password must consist of :
  - Uppercase (A..Z) and lowercase (a..z) letters.
  - At least 1 digit (0..9) or at least 1 of the following special characters: +!/(:)_*
- Your password must not consist of : o Your user name

    - Either of your first names

It is recommended that you change your password at least every 90 days.

5.3 Use of passwords

In addition to complying with the current password policy, which is decided centrally, the choice and use of passwords must be in compliance with good practice, as stated below:

- Choose a password that:
  - Is easy to remember.
  - Cannot be guessed or derived from personal information such as name, username, telephone number, birthday or other dates, etc.
  - Is not found in any dictionary or glossary.Does not contain consecutive or identical digits, characters or letters.
- Always keep your password secret.
- Never share your password with others. Not even the IT Department.
- Do not use the same password as for personal use.
- Do not write down or store your password in any way.
- Change your password immediately if you suspect that it has been compromised.

The IT Department will review the current password policy for all user profiles at regular intervals. If any user account does not comply with the current password policy the user will be notified hereof.

Users must contact the IT Department if their accounts have been closed. The IT Department is allowed to change the ITU password if a user account has been exposed to phishing attacks. In such cases the user must therefore contact the IT department to get a new password.

As a user, you must promptly change your password or contact the IT Department if you suspect that your password is known to others than yourself.

6 Rules of conduct for unmonitored equipment

Users must ensure that unmonitored equipment and systems are protected by complying with the following guidelines:

- When the individual user programs are no longer in use, they must be ended unless they are protected by a general lock such as a password-protected screen lock.
- When leaving the pc it must be locked or the user must log out completely.
- When the system is no longer in use, the user must log out. It is not sufficient to merely switch off the screen.

7 Backup of data

Only data located on the network drives and data located in your profile folder is included in the daily backup process.

As a user on the ITU network, it is your own responsibility to transmit data to the network drives - which is the preferred place to store your data. Your log on time is depending on how much data your Windows profile contains, so we recommend that you use your personal network drive (called P) as much as possible.

All production servers are also included in the back-up strategy of the IT Department. This also applies to essential systems such as the e-mail system, the financial system (Navision), the calendar system, file servers, databases and the user database (LDAP).

If you are handling important and business critical data please make sure that such kind of data is included in the backup process. This especially includes research data, which is considered to be business critical and must be included in the backup process.

For further details, see the backup policy or read more here: http://intranet.itu.dk/en/Intranet-hjem/Afdelinger/It- afdelingen/IT-Afdelingens-ABC/Backup-til-baerbare-computere

8 Use of private entities and peripheral equipment on ITU's network

8.1 Private entities and peripheral equipment

All private entities and peripheral equipment connected to the network at ITU, are also covered by this IT security manual.

ITU contributes the concept of bring your own device (BYOD). However, there are certain things that you should be aware of when using private entities and peripheral equipment (such as mobile phones, tablets and laptops, etc.) on the ITU network. If you are accessing your ITU mail, calendar and network drive with your own equipment you must make sure your equipment is protected by some form of access control. It may for example be a password or a pattern code.

The same goes for your own laptop, which must also be protected with a password that meets the general password policy on ITU. See section 5. Rules of conduct for the use of user accounts and passwords.

9 Regulatory Compliance

Users undertake to observe the legislation applicable at any time, including the Act on Processing of Personal Data (Persondataloven), the Danish Executive order No. 528 of 27 June 2000 (sikkerhedsbekendtgørelsen) and the Copyright Act, which are detailed below:

The Act on Processing of Personal Data and the Danish Executive order places strict requirements on how to handle information with confidentiality and personal sensitive content. If you handle that sort of information you must make sure that it happens in accordance with the act and the executive order. You can read more about the proper handling of information on the following link: http://intranet.itu.dk/en/Intranet-hjem/Afdelinger/It-afdelingen/Om-it- afdelingen/IT-sikkerhed/Vejledninger-og-retningslinjer/Haandtering-af-fortroligt-og-personfoelsomt-data

To comply with copyright law you may only install and use software, data, etc., at ITU systems if copyright and license conditions are observed. Data also include audio, picture and video files.

No software or data may be copied or transferred to other IT systems within or outside the university unless copyright and licence requirements are observed.

10 Sanctions in case of violation

In case of noncompliance with the guidelines, the IT Department will see to removal of software/hardware. Aggravated cases of misuse may lead to withdrawal of the user account and further sanctions in accordance with the staff policy.

In connection with maintenance of the IT systems of the IT University, the IT Department is entitled to obtain access to user data and software and to monitor network traffic.

IT DEPARTMENT

IT University of Copenhagen
Rued Langgaards Vej 7
2300 Copenhagen S

Opening hours:
Monday - Friday
10 AM to 13 PM
Wing 2C

it@itu.dk