Informationssicherheit im Homeoffice

Due to the measures taken by the Austrian Federal Government to combat the spread of the SARS-COV 2 (Covid 19) virus, the majority of TU Wien employees have been working from home since 13 March 2020. In times of crisis rapid action and improvisation is required, which is why data protection and information security may have been pushed into the background in recent weeks, as the focus is on maintaining ongoing operations.

However, data protection and information security should not be ignored even in times of crisis, as existing security gaps are used for attacks even when we work from home. The more security gaps there are, the more possibilities potential hackers have. A widespread attack on the systems of the TU Wien is a big problem even in quiet times and should be avoided especially now, in order not to restrict the operation even more.

Therefore you will find instructions and recommendations for use here, which make working from home as safe as necessary and as practical as possible. The recommendations regarding the use of private devices for professional purposes are valid until the buildings of the TU Wien are completely accessible again.

Here you will find the following information

- Data access and applications
  - VPN
  - E-Mail
  - Store and share data
  - Co-editing of documents
  - Phone and Chat
  - Webconferencing and scheduling
- Data security at home
  - General information
  - Cybercrime and social engineering
  - Passwords
- Devices
  - TU Laptop
  - Private PC or laptop
  - Mobile
  - Any questions?

Any questions?

If you have questions or problems with the implementation of these instructions, please contact help@it.tuwien.ac.at or the IT representative and/or IT admin of your institute. Additional requests and suggestions are welcome at infosec@tuwien.ac.at or datenschutz@tuwien.ac.at and will be forwarded to the appropriate departments. A continuously updated list of applications for the home office can be found in the coLab of the TU Vienna at: https://colab.tuwien.ac.at/display/HOT/Tipps+Home+Office

Data access and applications

VPN

Secure access to data stored at the TU Wien can be obtained via a VPN connection. This is a secure connection from any network to a network of the TU Wien.

Details on how to apply and install VPN can be found at https://colab.tuwien.ac.at/pages/viewpage.action?pageId=9437275 (no English translation available)

If the VPN connection is activated, you have access to the drives, data and applications at the TU Wien for which you have permission.

There is no permission to access computers of institutes via remote desktop from outside the TU Wien without VPN or SSH tunnel.

If your organizational unit uses its own firewall, you need a static IP address for VPN to access the resources. You can apply for this in Online Account Management at https://www.it.tuwien.ac.at/rechte-und-rollen/online-account-management/. Your local firewall admin will then open the firewall for this IP.

E-Mail

You can get access to your e-mails via https://upTUdate.tuwien.ac.at.

Store and share data

If you want to exchange data with colleagues from other departments, it is recommended to use the TU Vienna's owncloud (TUownCloud) available at https://owncloud.tuwien.ac.at/

If it is necessary to exchange data with external people external to the TU, use the proCloud of the TU Vienna. Details on applying for and using the proCloud can be found at https://www.it.tuwien.ac.at/en/services/cooperation-and-communication/collaboration/tuprocloud-sync-and-share-for-projects/

Co-editing of documents

If you want to edit documents together with colleagues, use the application TUdocs: https://www.it.tuwien.ac.at/en/services/cooperation-and-communication/data-storage/tuowncloud-sync-and-share/tudocs/

Phone and Chat

With the application Cisco Jabber application, you can make phone calls via PC just like you're your desk phone in the office. The instructions for setting up the application can be found here: https://colab.tuwien.ac.at/display/HOT/Softphone+Cisco+Jabber

TISS can also be used to change characteristics of the TUphone profile and the TUphone password. You can find instructions for this under: https://www.it.tuwien.ac.at/fileadmin/TUit/BILDERPOOL/service/TUphone_Festnetz/Anleitungen/Endanwender.pdf (available in German only. If you need help contact inside@tiss.tuwien.ac.at)

With TUchat you can exchange information in groups (channels) or individually via a simple, intuitively operated platform and send files, pictures or videos.

Webconferencing and scheduling

If you need a polling tool to find a date, the applications https://terminplaner4.dfn.de/ or https://www.termino.gv.at/meet/de are recommended.

For handling virtual meetings and courses the TU Wien recommends the following applications:

1. GoTo Meeting: https://colab.tuwien.ac.at/display/CORONA/GoTo+Meeting
2. MS Teams: https://colab.tuwien.ac.at/pages/viewpage.action?pageId=9439683
3. Cisco Jabber: https://colab.tuwien.ac.at/display/CORONA/Cisco+Jabber
4. Skype for Business/Microsoft: has been replaced with teams and has very limited functionality at the TU Vienna.

Please note that - due to the rapidity of the events - only the applications ZOOM and GoToMeeting have so far been finally audited with regard to compliance with the regulations of the GDPR and the requirements of information security. The free version of ZOOM in its current design is not compliant with GDPR and should therefore not be used at the Vienna University of Technology.

In general, the following applies to these applications:

- Do not create public events, but use the possibility to protect your meeting with a password. Some applications also allow you to set up a waiting room and control the access of participants.
- If possible, make documents for meetings or course material available only via TU platforms such as TUWEL, TISS, ownCloud and coLab (in TISS and TUWEL the permitted file size has been increased to 250 MB). If you make the data available on the institute's own web servers, the access data must be transmitted via TISS/TUWEL.
- Do not share the link to a meeting in public places (for example, in social media accounts), but send the link directly to the invited people.
- Make sure that only you as the meeting-organizer can share the screen.
- Make sure that all participants use the latest version of the application.

Data security at home

General information

Just as the computer at the TU Vienna has to be locked when leaving the workplace, the computer in the home office has to be locked when taking a break. It is best to activate a screen saver with password. If you have to work on a private computer that is also used by other family members, it is advisable to create a password-protected company account. You can find instructions for this here: https://support.microsoft.com/en-us/help/13951/windows-create-user-account

If you work with TUownCloud or TUproCloud, you should not automatically synchronize all data on your computer, but only those you need for your daily work.

If data from TU files is stored on the local computer for editing, you should save it back to TUfiles after finishing your work and delete it on the local computer.

If possible, do not use external data carriers to store data. Should it be necessary to use such media, they must be encrypted and kept in a safe place to prevent data from being lost or accidentally deleted.

Cybercrime and social engineering

(Source:https://www.dsb.gv.at/documents/22758/23115/Informationsblatt_der_Datenschutzbehoerde_Datensicherheit_und_Home-Office.pdf/)

The current exceptional situation and uncertainty is being abused by criminals. In particular, an increase in phishing attacks can be observed, by means of which criminals try to access user data via fake websites, e-mails or short messages.

Expect criminals to try to pass themselves off as trustworthy sources (e.g. health authorities). Under no circumstances give out user data or passwords when you are asked to do so. Check the URL ("the web address") before entering user information on a web page, and access login pages by manual input rather than following a link from an email. Do not install software on your (service) laptop without permission.

Always question instructions that ask you to perform unusual actions or install various programs. Please bear in mind that an identity can be falsified. If you receive unusual e-mails, always check the identity of the sender address and compare it with the sender address of trustworthy e-mails from your colleagues.

You should also be particularly careful if you are asked to take urgent action in an e-mail. Criminals often try to entice you to take certain actions under the pretext of special urgency ("If you do not carry out verification within the next 2 days, your account/access will be blocked").

In case of doubt, please consult the contact person for IT matters or TU.it.

Examples:

- You receive an e-mail asking you to install home office software.
- You receive an e-mail with an urgent request to verify your e-mail account for home office use.
- You receive an e-mail asking you to enter your user data or passwords to receive up-to-date information about the corona virus (COVID-19).
- A pop-up opens. An alleged security team informs you about the latest number of infection cases and asks you to install a new "messaging software".
- You receive a phone call. The unknown person pretends to be a health authority employee and asks you to give your credit card details so that a vaccine can be sent to you.

The first point of contact for IT security issues regarding firewalls, network security for servers, application security for workstations and various threat scenarios such as spam, phishing and malware (viruses) is the IT Security Department at TU.it

Passwords

Do not share passwords even within your family and use passwords that are as complex as possible.

If you send password-protected TUownCloud links to share important information, send the password via SMS or at least in a separate email. The same applies to password-protected meetings or other applications where access is password protected and shared with others. If you want to send sensitive data to TU Wien employees, it is best to use TUownCloud. For data exchange with external persons you can use TUproCloud.

Make sure that you use different passwords for different applications. The password for logging on to the company account or the TU laptop should be different from the password for any other private services. The same applies to the password for upTUdate e-mail access. This password should never be identical with the password for other e-mail services.

Do not store passwords in accessible text files, e.g. on the desktop or in shared file shares, nor write them on Post-its and the like. Passwords should also not be stored in web browsers, even if this seems comfortable. The best way is to use a password manager. The TU Wien provides the password manager 1password in test mode. If you have any questions, please contact infosec@tuwien.ac.at. The TU.it is making every effort to make the service available as soon as possible via its website.

Instructions on how to change your TU password can be found here: https://www.it.tuwien.ac.at/rechte-und-rollen/accounts-an-der-tuw/accounts-fuer-mitarbeiter-innen/

Devices

TU Laptop

These laptops are usually administratively supported devices, either by TU.it in the case of a TUclient or by the IT admin of the respective organisational unit in the case of decentrally serviced devices.

Primarily these supervisors should be contacted for questions or help, since they usually have the possibility of remote access (for example via Teamviewer) to your client and can thus provide direct support.

Questions to the TU.it can be sent by e-mail to help@it.tuwien.ac.at. There is also the possibility to create a ticket directly at https://support.tuwien.ac.at/assystnet/.

Security applications such as antivirus protection, firewalls, endpoint security, etc. should be kept up to date. The same applies to your operating system and the software used.

Please note that only you are allowed to work on your TU Laptop! It is not allowed to let other family members work on this computer.

Private PC or laptop

If you use a private laptop or PC, create a separate, password-protected "company account" if possible. Instructions for Windows computers can be found here: https://support.microsoft.com/en-us/help/13951/windows-create-user-account.

If it is not possible to create a separate account, please make sure that you actively log off from all services of the TU Wien after you have finished your work. If possible, save sensitive data only in folders to which only you have access. If this is not possible, save documents that you have edited locally in the TUowncloud or in your TUfiles folder and delete all data stored locally on your computer, as soon as you have finished your work.

If you are using the Windows operating system, it must be version 8.1 or higher, as there have been no security updates for Windows 7 and 8 for over a year. You can still upgrade from Windows 7 and 8 to version 10 free of charge (https://www.microsoft.com/de-de/software-download/windows10). Also make sure that your anti-virus software is kept up-to-date. With Windows 10 this happens automatically.

Similar to Microsoft Windows, Apple products offer onboard options for hard disk encryption. You can find more information about this here: https://support.apple.com/de-at/HT204837.

Please make sure that the device you are using is encrypted.

If you encrypt external data carriers with the onboard programs, the data can usually not be read on other operating systems, because mostly the file system on the data carriers is used for encryption.

If you want to work across operating systems, then the program Vera-Crypt is recommended. It can be installed on Windows, MacOS and Linux and can also create readable encrypted external data media for everyone. https://www.veracrypt.fr/en/Home.html

To synchronize data over "insecure" and mostly free cloud fileshares, the program Cryptomator is recommended, which generates a virtual drive and stores the data encrypted in the background in the cloud. This program is also available for Windows, MacOS and Linux. https://cryptomator.org/

Mobile

If possible, only download certified apps to your phone. If you have a company mobile phone, this may only be used by you. If you retrieve company e-mails via your private phone or synchronize your TU Wien address book, make sure that your phone is not used unattended by other people. Many mobile phones and tablets offer the possibility to create your own profiles (for example for children). Please check whether this is possible on your devices and set up separate accounts if your device is also used by other people. Make sure that your devices are encrypted.

Any questions?

If you have questions or problems with the implementation of these instructions, please contact help@it.tuwien.ac.at or the IT representative and/or IT admin of your institute. Additional requests and suggestions are welcome at infosec@tuwien.ac.at or datenschutz@tuwien.ac.at and will be forwarded to the appropriate departments. A continuously updated list of applications for the home office can be found in the coLab of the TU Vienna at: https://colab.tuwien.ac.at/display/HOT/Tipps+Home+Office