International travel guidelines

VU Amsterdam students and employees regularly travel abroad to carry out research, attend conferences, and to set up and promote international collaborative partnerships. Travel to most countries is not a problem. However, when traveling abroad, especially to countries with higher health and safety risks, you are strongly advised to read the travel advisories issued by the Ministry of Foreign Affairs. In addition, it is important to follow the guidelines of International travel policy for employees, the advice below and of the AIVD for international travel. Please keep in mind that the data you carry is not secure and that in situations someone may be watching over your shoulder while you log in and may even be overheard (for example by a taxi driver).

Therefore, consider traveling with "clean" electronic devices (such as your laptop, smartphone, electronic storage media, etc.) and follow the advice below. This can prevent access by (high) risk countries to your (private or work) data (such as passwords) and sensitive research knowledge.

Preparing for your trip

- Do not take unnecessary confidential information or documents digitally or on paper with you when traveling abroad.
    - It recommended to provide your electronic devices with the **latest updates**, a virus scanner and to secure them (via the use of EduVPN and disk encryption, regularly changing passwords, turning off Bluetooth, avoiding public WiFi and using from public USB ports or cables to charge your smartphone, even when traveling). Security updates to your devices are important because it makes it more difficult for malicious parties to gain access or install malware/spyware on your devices. If in doubt: contact the IT Service Desk.
- Try using different devices for personal and professional conversations. **If available***: when traveling use a loanable laptop that does not contain any personal files.
- Make sure there's nothing on your laptop that you don't want to share with others. Before departure, clear data and call history on your phone and/or tablet and use different passwords on all devices (in case making your password available is required).
- Do not use gifts with USB connections or USB sticks that you have received.
- If you are visiting a Chinese university: consult the ASPI list and check the risk level of the university. If this is 'high' or 'very high', please contact the *knowledge security contact person* within your faculty or service.

** The VU is working on making clean electronic work equipment available, such as loanable laptops. This is currently not available yet. Contact IT Service Desk for alternative solutions.*

During your trip

- When you are traveling and work requires access to VU services, please pay attention to the following points to prevent a security incident leading to damage on the VU network: **In all cases, IT must be asked in advance for each system whether there are any restrictions or risks in the country you are going to.**
- Try to log in to VU systems as little as possible. The less often you use your account information, the less likely your information will be collected.
- Use VU Onedrive for file storage and sharing, and in emergencies turn to SURFdrive. Under no circumstances should you use commercial storage services!
- Turn off Bluetooth on all your devices (also do not use Bluetooth equipment such as headphones, mice, etc.).
- Avoid active use of social media.
- Never leave your laptop, phone or other electronic devices unlocked or leave them to others, even for a small phone call.
- Do not rely on public or hotel computers or WiFi, even if there is an Eduroam point available: use the 4G/5G network of your phone or EduVPN where possible. At other educational and research institutions you can usually use institutional access via Eduroam, but always check whether this is a legitimate point and check with that institution if necessary! Consider using the Eduroam app.
- Do not store your laptop or phone in a hotel safe.
- Report directly to the VU IT Service Desk or call +31 20 5980000 in the event of an incident. Think of a laptop or other VU devices that have been stolen/lost, if you have had to make your VU password available or if you suspect that your login details are 'out on the street'.

After your trip

- When you return, change the passwords you used during your trip. You can change your VU password by clicking on your profile in the dashboard.

For more information about information security, see the information security page on vu.nl.