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. Follow the guidelines by the VU (International travel policy for employees) and the AIVD ('Travelling abroad - Safety risks') for international travel and consider travelling with 'clean' electronic devices, such as your laptop, smartphone, electronic storage media, etc. This can prevent access by risk countries to sensitive knowledge.

Please also take the following points into account:

- Do not take unnecessary confidential information or documents digitally or on paper with you when traveling abroad.
- It is also wise to secure your electronic devices (by using EduVPN and disk encryption, regularly changing passwords, turning off Bluetooth, avoiding public Wi-Fi and using a public USB port to charge your smartphone, even when traveling). If in doubt: ask the IT Service Desk.
- Try using different devices for personal and professional conversations.
- Always inform the security officer of your department immediately in the event of an incident. If in doubt: report!

Additional important tips for traveling to high-risk countries:

- Clear data and call history on your phone and/or tablet before departure
- Use different passwords on all devices (in case making your password available is required)
- **If available***: when traveling use a loanable laptop that does not contain any personal files
- Report directly to the VU IT Service Desk or call +31 20 5980000 if you have had to provide your password
- Turn off Bluetooth on all your devices (also do not use Bluetooth equipment such as headphones, mice, etc.)
- Do not use gifts with USB connections or USB sticks that you have received
- Avoid active use of social media
- Make sure there is nothing on your laptop that you do not want to share with others
- Never leave your laptop, phone or other electronic devices unlocked or do not leave them to others, even for a small phone call
- Please be aware that you may be overheard (for example, a taxi driver may also eavesdrop)
- Do not store your laptop or phone in a hotel safe

** 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.*

Working safely when traveling

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. If you are visiting a Chinese university: consult the ASPI list and check the risk level of the university. If the risk level is 'high' or 'very high', please contact the *knowledge security contact person* within your faculty or service.

At educational and research institutions, you can usually use institutional access via Eduroam, but always check whether this is a legitimate point and if necessary check with that institution! Consider using the Eduroam app.

Do not use on public or hotel wifi, and even if an Eduroam point is available, try to use the 4G network of your phone and EduVPN where possible, as this is more secure.

- Try to log in to VU systems as little as possible. The less often you use your account information, the less chance that your data will be captured.
- Secure your devices with a password and encryption.
- Use VU Onedrive for file storage and sharing and turn to SURFdrive in an emergency. Under no circumstances use commercial storage services!
- Do not use public computers, for example in hotel lobbies.
- Pay attention to your surroundings when you log in, prevent someone from looking over your shoulder.
- When you return, change your passwords that you used during your trip. You can change your password by clicking on your profile in the dashboard.
- Call (+31 20 5980000) the VU if your laptop or other VU devices are stolen/lost or email the IT Service Desk.

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