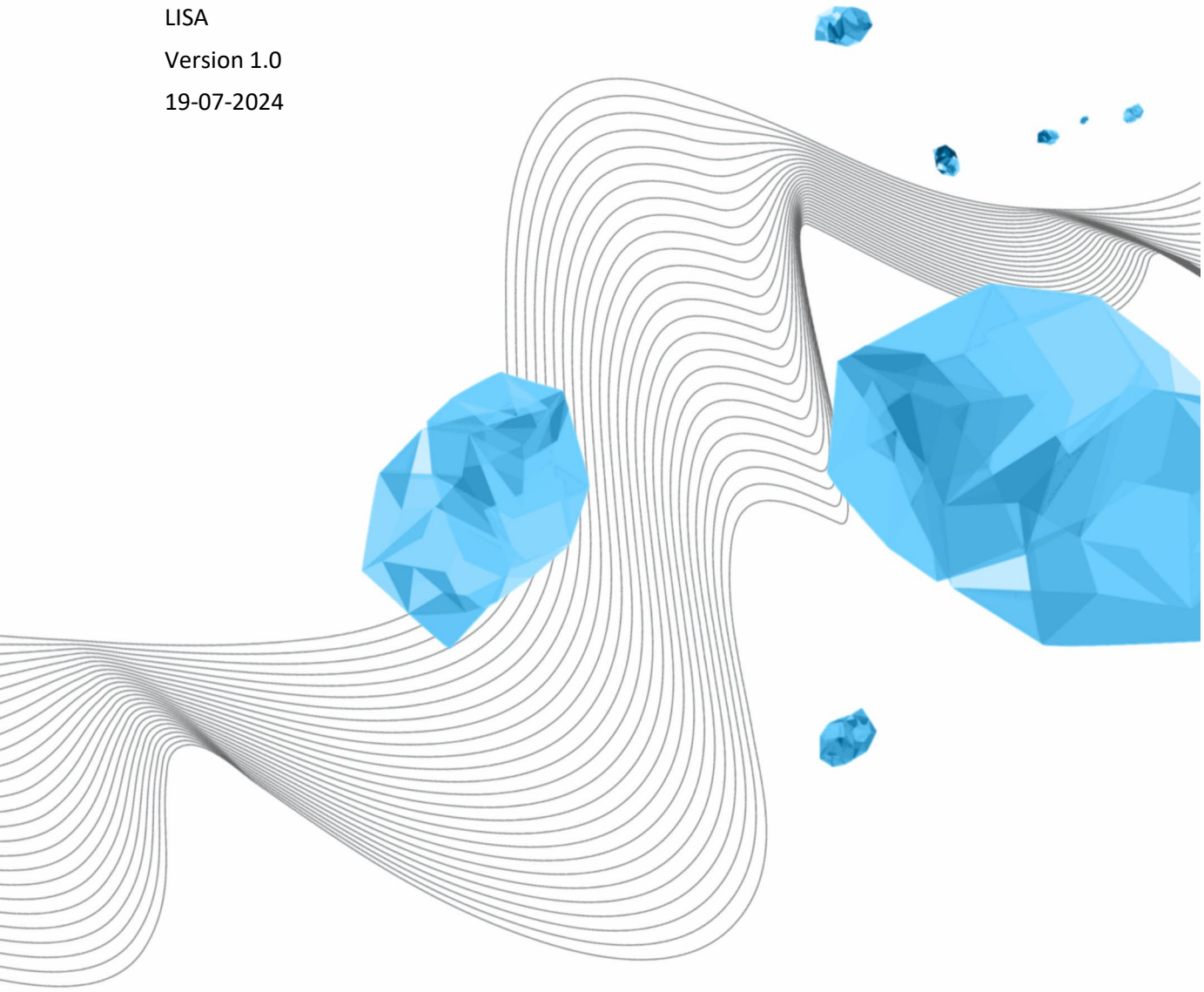
Status: Version 1.0
Date established in Executive Board: 03-09-2024
Date established MT-LISA: 22-07-2024
Author: Henk Swaters

KNOWLEDGE AND INFORMATION SECURITY WHILE TRAVEL ABROAD

LISA
Version 1.0
19-07-2024



UNIVERSITY OF TWENTE.

COLOPHON

ORGANIZATION
Library, ICT Services & Archive

TITLE
Knowledge and information security while travel abroad

ATTRIBUTE
LISA-0410

VERSION (STATUS)
1.0

DATE
19-07-2024

AUTHOR(S)
Henk Swaters

HISTORY

VERSION	DATE	AUTOR(S)	COMMENTS
0.2	14-06-2024	Henk Swaters	First version
0.3	21-06-2024	Henk Swaters	Feedback processed
0.4	25-06-2024	Henk Swaters	Feedback processed
1.0	19-07-2024	Henk Swaters	Added explanatory notes on measures

DISTRIBUTIELIJST

VERSION	DATE	DISTRIBUTED TO	COMMENTS
0.2	14-06-2024	LISA security & kennisveiligheid	
0.3	21-06-2024	LISA security & kennisveiligheid	
0.4	25-06-2024	LISA security & kennisveiligheid & MT	
1.0	22-07-2024	LISA-MT	Established

TABLE OF CONTENTS

1 INTRODUCTION

Are you travelling abroad for work soon? Business trips abroad involve espionage risks. The same applies to long-term work abroad. Foreign intelligence services and other stakeholders may be interested in you, especially in the knowledge you possess or carry with you. This information helps you take precautions to reduce the risk of (digital) espionage.

The basis for this guideline is the document “Travelling Abroad” [1] by the AIVD, with measures differentiated by the UT based on risk profiles. If you have a low-risk profile, the measures may sometimes not be proportional to the costs. To address this, the measures are linked to a risk profile. If you have a medium- or high-risk profile, the measures for lower risk profiles also apply.

1.1 READING GUIDE

Chapters 2 to 4 list all measures for all risk profiles. In Chapter 5, the measures are linked to a risk profile, making it possible to omit certain measures if the risk allows, in order to reduce costs.

[1] https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2017/12/20/op-reis-naar-het-buitenland/Brochure+Paspoort+Op+reis+naar+het+buitenland.pdf

2 BEFORE THE TRIP

2.1 GENERAL

Do not take or take as few confidential documents as possible. You are personally responsible for careful handling of this information. Therefore, always ask yourself the following questions before departure:

- Do I really need this?
- What is the value of the information I am taking (on paper, a data carrier, or otherwise)?
- How serious would it be if the information fell into the wrong hands?
- What devices am I taking with me?

If you do take confidential information with you, create a list of the documents, data carriers, and equipment you are taking. In case of loss, it will be immediately clear what is missing. Keep the list at the office, do not take it with you. Always carry your confidential documents and data carriers in your hand luggage, never in your suitcase.

Contact the Knowledge Safety Team (KST)[2] in advance to check if there are any special points of attention for your trip. Always do this if you are in doubt or if you are visiting a high-risk country. Currently, these countries are China, Iran, Russia, and North Korea. These countries have an offensive digital attack program. However, this does not mean that other countries cannot pose a high risk. Also, inquire about the rules for transporting (state) secret information, if applicable.

Coordinate visits to government organizations with the Dutch consulate or embassy, if present.

[2] https://www.utwente.nl/en/service-portal/internationalisation-foreign-affairs/knowledge-safety-export-control

2.2 DIGITAL

Consider using a disposable mobile phone with as few data and apps as possible, a temporary SIM card[3], and a temporary email address. If that is not possible, wipe the phone beforehand.

Install only the applications you actually need and avoid apps that have privacy or data security issues. Ensure that you only have necessary contacts in your contact list. For chat functionality, Signal is the most secure application, even though it is less popular than WhatsApp, SMS, or WeChat. It is important to use multi-factor authentication and strong passwords, also for your apps. Contact CERT-UT[4] for advice if necessary.

If you travel abroad regularly, it is advisable to purchase equipment that you use exclusively for this purpose. Bring your own chargers, adapters, cables, and car kit. Also, ensure that you can remotely wipe this equipment; instructions are often found on the smartphone manufacturer's website.

If you buy a SIM card with a data bundle before your trip, carefully consider the size of the data bundle. Nowadays, you can easily use 500MB per day, even if you use it sparingly. Do not buy a SIM card in a high-risk country!

If you buy the SIM card in a "safe" destination country, only do so at reputable stores. Never buy from street vendors. Also, keep in mind that you often receive an eSIM nowadays, and your device must be compatible with it.

Change passwords before (and after) your trip.

Use different passwords for all your devices and ensure they are not the same as your workplace login credentials.

Prevent someone from watching or tampering with your equipment unnoticed. You can cover your webcam, use a privacy screen, or special anti-tamper stickers. Due to the wide variety of equipment, this is a custom order through the Procurement department (CFM).

2.3 PRIVATE

Use different devices for your private conversations and your professional conversations, and keep them as separate as possible.

On a private trip, take as little business information and as few data carriers as possible.

Do not post on social media, such as Twitter and Facebook, that you are going on a trip.

[3] For example: https://reissim.nl/china-esim-simkaart-en-censuur/
[4] https://www.utwente.nl/nl/cyber-safety/meld-incidenten/

3 DURING THE TRIP

3.1 GENERAL

Do not have confidential conversations on the phone or in vehicles such as rental cars, trains, or airplanes. Keep information and data carriers with you as much as possible.

Do not tell your conversation partner more than necessary.

Be alert to 'coincidental' encounters with people who show a lot of interest in your work or private life. Attempts to contact you may also be made through social media.

Your behaviour can place you in a vulnerable position, either immediately or at a later time. Not only alcohol or drugs but also gifts or advances can be used to influence you.

Be aware that people may film you or make audio recordings to pressure you later. This also applies when using social media or dating apps!

Ensure you can check if someone has accessed confidential information. Use seal bags[5] for this purpose.

Although a hotel safe is better than no safe, it still poses a risk. Preferably do not use the hotel safe for confidential information or data carriers. Keep these items with you. If it is unavoidable, use the in-room safe or take a small travel safe with you. You can carry this in your suitcase and secure it with a cable somewhere in the hotel room.

3.2 DIGITAL

Turn off your devices when having a confidential conversation. If possible, remove the battery, or place your device between your clothes or in your bag to muffle the sound. You are especially vulnerable to espionage when your devices are on.

Turn off the Wi-Fi and Bluetooth functions on all your devices. Refer to your device's manual for this. Bluetooth is insecure, and espionage via this function is extremely easy. Only turn on Wi-Fi when necessary.

Do not download or install applications during the trip. Turn off automatic updates for the App Store or Play Store while traveling. In unsafe countries, fake app stores that contain malware may be offered. Once you return to a safe country, you should re-enable updates.

Pay attention to unexpected or strange (security) warnings on your phone, laptop, or tablet. These notifications may indicate an attack. Keep track of notifications and other unusual occurrences and report them to CERT-UT. Also, consult whether you can continue using the equipment.

Never give out your password and do not allow others to use your equipment or cables.

Do not use Wi-Fi offered in public places.

[5] For example: https://www.debatin.com/safebag-for-tablets-and-smartphones/

Do you want to work on the go? Never use equipment from others. Also, never connect your system to someone else's equipment (think of printers and chargers). It is better to email presentations in advance to the person who invited you so that you can present using the computer available there.

When traveling, it is important to browse the internet securely. Use the "Secure Internet" option of eduVPN[6]. This ensures your internet connection is encrypted and protects your data from hackers.

Do not use USB sticks. If it is absolutely necessary, only use your own USB stick from a reliable manufacturer. Ensure it is encrypted and securely stored.

Do not use USB chargers and other USB devices from others. This includes any USB ports in a (rental) car, as they can also transfer data. In emergencies, you can purchase a USB blocker before your trip, which allows for charging only.

Be cautious when opening emails, SMS messages, or other electronic messages from unknown senders. Beware of spear phishing. Always verify whether received messages are intended for you. If in doubt, first verify the origin of the message with the sender.

Never hand over your equipment. If you must do so due to security measures, place them in a seal bag[7] or give them to a colleague who is not entering with you.

Always immediately report an incident to CERT-UT. Do this even if you are in doubt!

4 AFTER THE TRIP

4.1 GENERAL

Change the password for the equipment taken and for accounts, such as email and social media. Re-enable automatic updates. It may be necessary for your equipment to be submitted for analysis or cleaning. In some cases, it might even be necessary to destroy the equipment upon return if safe use is no longer possible. There may be specific arrangements regarding this depending on your destination and organisation, so please coordinate this in advance with the Knowledge Safety Team[8].

Strangers may contact you for some time after the trip, referring to events and "friendships" made during the journey. Handle these contacts with caution.

5 PRINCIPLES AND GUIDELINES

5.1 INTRODUCTION

As previously mentioned, it is advisable to implement all measures before, during, and after your trip. However, if you have a low-risk profile, some measures may not be proportionate to the costs involved. To address this, measures are linked to risk profiles. If you have a medium or high-risk profile, the measures for lower-risk profiles will also apply.

[6] https://www.eduvpn.org/ of https://utwente.nl/vpn
[7] For example: https://www.debatin.com/safebag-for-tablets-and-smartphones/
[8] https://www.utwente.nl/en/service-portal/internationalisation-foreign-affairs/knowledge-safety-export-control

If employees wish to work temporarily in their home country, for example, due to family circumstances such as caregiving obligations, prior approval from their manager is required. However, outside the EU, it is never permitted to use special authorisations in company systems that provide access to sensitive data, such as personal data of others. Both the employee and the manager must ensure that authorisation is revoked if the employee is staying outside the EU.

5.2 RISK PROFILES

The risk you face during a trip is also dependent on the knowledge and information you possess or have access to. Therefore, the extent to which you need to implement measures will also depend on this. Ideally, you should adopt all measures, but sometimes you can be slightly more flexible. The risk profiles we distinguish are:

Low risk profile

- Administrative and support staff without access to sensitive research data or authorisation to access company systems that provide access to other sensitive data (see 5.1).
- Students participating in regular studies without involvement in sensitive research projects.

Medium Risk Profile

- Researchers working on projects with moderately sensitive information, such as public research projects or collaborations with other institutions.
- Staff with access to internal policy documents or strategic plans.
- Administrative and support staff authorised to access company systems that provide insight into sensitive business data or personal information.

High risk profile

- Professors and PhD students involved in research with a high degree of confidentiality or commercial value.
- IT administrators/officials with elevated privileges or access to sensitive data and infrastructure.
- Board members making strategic decisions and having access to sensitive institutional information.

5.3 LOW RISK PROFILE MEASURES

- Only take the equipment necessary for your trip.
- Create a list of documents and equipment being taken. Keep this list at home.
- Limit access to data to only those who need it for their work.
- It is essential to use strong, unique passwords for all IT services and, if necessary, change them regularly[9]. This includes using multi-factor authentication to further secure access to accounts, including your own social media accounts.
- Encrypt data carriers such as your laptop's hard drive and your phone's storage.
- Install and maintain reliable antivirus and anti-malware software on all your devices to protect them from malicious software.
- The managed workplace of the university has antivirus and anti-malware software to protect this computer from harmful software.
- Follow the guidelines for securely using personal devices[10] (Bring Your Own Device). This includes separating personal and work data and adhering to university-specific security protocols.
- Participate in security awareness training offered by the university. This helps in recognising phishing attacks and other cyber threats.
- Avoid public Wi-Fi and do not use third-party equipment.
- Do not use USB storage media.
- Avoid using USB devices from others, including chargers or USB ports in cars or other transport.
- Avoid discussing confidential information in public places.
- If something suspicious happens with a device, stop using it immediately.
- Turn off Bluetooth (and, if possible, Wi-Fi) when not in use.
- Report any incidents or suspicious situations that you are unsure how to handle directly to CERT-UT[11].

[9] Change your password if you suspect misuse of your login account
[10] https://www.utwente.nl/nl/cyber-safety/cybersafety/wetgeving/gebruik-van-eigen-apparatuur-nl.pdf
[11] https://www.utwente.nl/nl/cyber-safety/meld-incidenten/

5.4 MEDIUM RISK PROFILE MEASURES

- Take no or as little confidential data as possible, both digital and paper-based.
- Transport confidential documents in your hand luggage.
- Always use encrypted communication and eduVPN connections.
- Encrypt sensitive files stored on your laptop.
- Always use encryption when exchanging sensitive information, for example, via filesender[12].
- Limit access to sensitive data to only those who need it for their work. Provide explicit instructions on data usage and make it clear that sharing outside the project context is not allowed.
- Change passwords before and after the trip.
- Clear call history and delete messages from your phone.
- Use a disposable phone with a temporary SIM card.
- Avoid using hotel safes for confidential information (see 3.1).
- Do not download applications during the trip.

5.5 HIGH RISK PROFILE MEASURES

- Make an appointment with Servicedesk ICT (LISA) at least 3 weeks before the trip for instruction and preparation.
- Use sealbags for confidential data and devices.
- For foreign travel, use special equipment. So empty laptop and smartphone in consultation with Service Desk ICT (LISA).
- Always return equipment to the LISA Service Desk for analysis, erasure and reinstallation after the trip.

[12] https://www.surf.nl/diensten/surffilesender

6 CONTACT DETAILS

WIE		
CERT-UT	Computer Emergency Respons Team UT	https://www.utwente.nl/en/cyber-safety/reportincident/ +31 53 4891313 cert@utwente.nl
Servicedesk ICT (LISA)	Support Requests	servicedesk-ict@utwente.nl +31 53 4895577
KST-UT	Knowledge Safety Team UT	knowledge-safety@utwente.nl

7 REVIEW OF THIS POLICY

This policy is reviewed at least every three years. The next review will take place in mid-2027. There may be grounds for a mid-term review. If this evaluation gives cause to do so, the policy will be adjusted sooner.

The CISO of the University of Twente is responsible for this policy.

This policy is established by the Executive Board of the University of Twente.