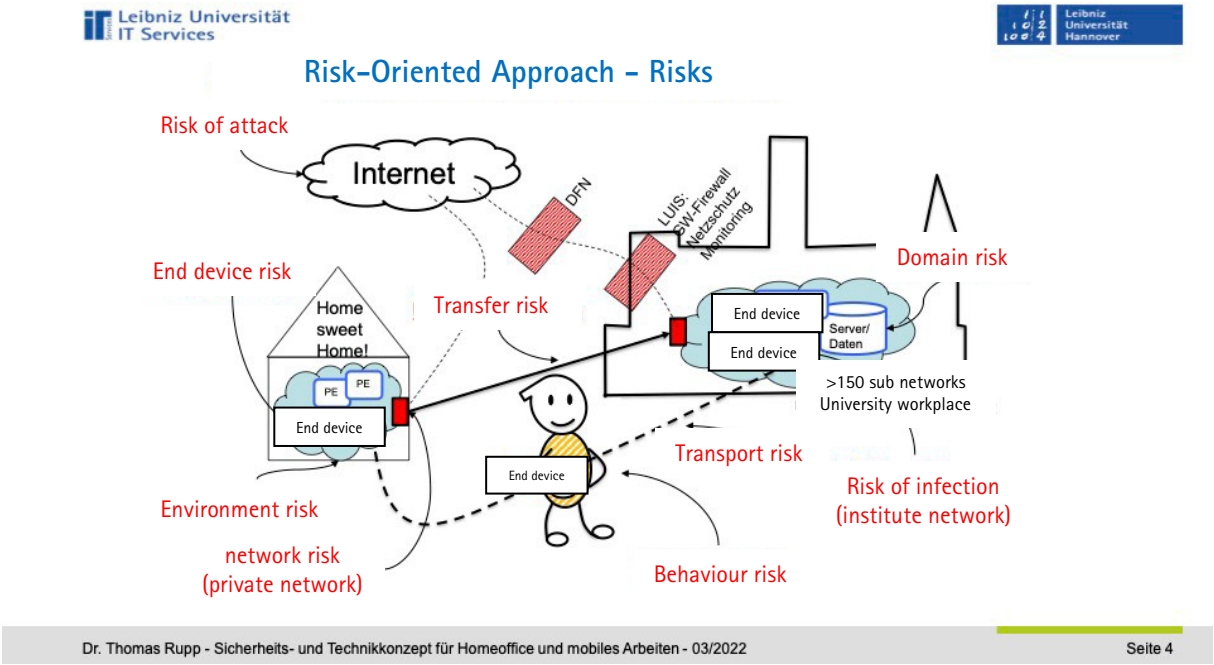
Interview Guideline for the "Mobile Working" Application:
Determining the Appropriate Technical Scenario

Applicant: _____

Superior: _____

(Counsellor:) _____

Date: _____



The goal of this interview is to determine the appropriate technical scenario for the tasks that will be performed during the mobile working. In order to do that, it is important to determine which tasks will be carried out where.

Using the guideline on the following pages, you can consummately assess the risks attached.

The aim is to categorise the relative risk (risk class) into the one of the following categories: "non-critical", "moderate", "critical", "highly critical".

Based on this categorisation, you can choose a technical scenario.

1) Assessment of the Security Level (According to the Policy for Security and Technology in Home Office and Mobile Working from LUIS).

Guiding question: Which tasks will be performed during home office or mobile working? To what extent?

Security Level A:

- No processing of personal data that is not publically accessible
- No research data that must be protected

Examples: literature research, creating or editing online content, developing teaching and learning concepts, writing articles etc.

Will tasks of this level be performed? ☐ yes ☐ no

Notes: _____

_____

_____

_____

Security Level B:

- Contact information of third parties, in-house communication data, official data of staff
- No research data that must be protected

Examples: appointment coordination, soliciting quotations, order transactions, organisational charts etc.

Will tasks of this level be performed? ☐ yes ☐ no
Would it be possible <u>not</u> to carry out tasks of this level during mobile working?
☐ yes ☐ no

Notes: _____

_____

_____

_____

Security Level C:

- Personal data that could do damage to a person's social standing or financial circumstances if used improperly
- Administration and controlling of projects funded by third parties, research data that has not been published

Examples: Advising people interested in studying, marking course work and exams, administration of Stud.IP events, administration of personnel costs, reading access to SAP, claims for travel expenses etc.

Will tasks of this level be performed? ☐ yes ☐ no
Would it be possible not to carry out tasks of this level during mobile working?
☐ yes ☐ no

Notes: _____

_____

_____

_____

Security Level D:

- Personal data that could do severe damage to a person's social standing or financial circumstances if used improperly
- Research data that must be kept secret by contract

Examples: personnel matters, health data, professorship appointment and job application processes, information about academic achievements of students etc.

Will tasks of this level be performed? ☐ yes ☐ no
Would it be possible not to carry out tasks of this level during mobile working?
☐ yes ☐ no

Notes: _____

_____

_____

_____

There is also a security level E, which covers things like, for example, files of criminal proceedings, but this is barely relevant at Leibniz University Hannover (especially in the context of mobile working).

For the applicant's tasks during mobile working, the following security level has been determined:

☐ A ☐ B ☐ C ☐ D

2) Assessment of the Environmental Risk and the Corresponding Risk Class

Generally, the environmental risk for working with mobile devices is categorised as "medium". If the mobile device is used in a public place (public park, café, train, during a conference) without additional security measures, the environmental risk increases to "high"!

Potential threats are: hardware theft, visual access to the screen by third persons or cameras, overhearing of conversations, unsafe WLAN networks…

- For tasks of security level A and B, the risk class is "non-critical".
- For tasks of security level C, the risk class is "moderate" if the environmental risk is "medium". If the environmental risk is "high", the risk class is "critical".
- For tasks of security level D, the risk class is "critical" if the environmental risk is "medium". If the environmental risk is "high", the risk class is "highly critical".

3) Assessment of the Domain Risk

Will the applicant access LUH resources that cannot be reached via "standard VPN"? For example: institute servers, remote maintenance of measuring systems etc.

☐ yes[1] ☐ no[1]

If "yes": Will the administrator make sure that only those systems and data that are necessary for the tasks can be accessed?

☐ yes ☐ no

What will the applicant access?

_____

_____

_____

[1] If the answer is "no", the domain risk does not influence the risk class. If the answer is "yes", the risk must be assessed specifically on the basis of what data the domain contains.

For the applicant's tasks during mobile working, the following risk class has been determined:

☐ non-critical ☐ moderate ☐ critical ☐ highly critical

4) Possible technical scenarios for the "Mobile Working" application in relation to the risk class

Highly Critical:

These tasks may not be carried out during mobile working!

Critical:

The scenarios "Thinclient", "Managed Device" and "Fortrex" are allowed. All three scenarios are described in detail under section 9.1 of the Policy for Security and Technology in Home Office and Mobile Working from LUIS).

- A "Thinclient" is a mini desktop PC with direct and secure access to the switched-on PC in the office via a "tunnel". With this scenario, it is only possible to work via the "tunnel".
- A "Managed Device" is (usually) a laptop computer with access to a PC in a LUH building via device VPN. With this scenario, work takes place on the PC at LUH.
- "Fortrex" is the name for a laptop computer that is administrated via mobile device management and thus kept up-to-date and secure.

Managed devices and Fortrex laptops require an immense administrative effort that cannot be provided by LUIS. If an institute wants to use this scenario, they will have to provide it themselves.

Moderate:

In addition to the above, the technical scenarios "Road Warrior" and "Institute Laptop with VPN Access to the Institute" (*„Einrichtungs-Laptop mit VPN-Zugang zur Einrichtung"*) are allowed.

- "Road Warrior" is the name for the classic scenario in which an encrypted mobile device is used for work on the move without access to resources within the LUH network. When using this scenario, it is possible to work with local files by saving them remotely to a Seafile cloud.
- Under the "Institute Laptop" scenario, access to a local network is possible, but it requires local administration of the institute's devices.
  If it is possible to work without access to the local network, the "Road Warrior" scenario should be used preferably.

Non-critical:

All device scenarios according to the "Regulations on the Use of Private Mobile Devices at Work" are allowed.

The following technical scenario has been chosen:

☐ Thinclient ☐ Managed Device ☐ Fortrex

☐ Road Warrior ☐ Institute Laptop with VPN Access to the Institute

☐ _____

The risks of mobile working have been explained to me. I will only carry out tasks of the security level determined here, and I will only carry them out in the environment discussed here.
My laptop computer is secured by password and my device's hard drive and all additional data storage devices are encrypted.

_____

Applicant's signature