STATISTIK AUSTRIA
Die Informationsmanager

AMDC
Austrian Micro
Data Center

Technical and organisational measures (TOM) to ensure and maintain data security in the AMDC

Version 1.3 | 01.07.2023

Access point

- The access point must be located in a separate room of the research institution where physical risks such as unauthorised viewing and observation of activities as well as loss or theft are prevented. The access point must not be located in an open or public room.
- The room in which the access point is located must be lockable.
- No video or other surveillance systems may be installed in the room where the access point is located.
- If the room is not used as an access point, it may be used for other purposes. These purposes must not conflict with the use as an access point.
- Cleaning or technical maintenance of the room may only take place if it is not used as an access point.
- The access point within the room must be designed in such a way that no person other than the researcher authorised to view the data is allowed to inspect them.
- As soon as the researcher authorised to view the data leaves the access point - even for a short time - any other person must be prevented from viewing the data by appropriate technical measures on the end device (e.g. VDI logout, screen lock, turning off the end device).

End-user device to access the AMDC

The end-user device used for access must be managed by the scientific institution and must be equipped or secured with:

- maintained operating system (Windows, Linux, macOS) with current software patches,
- up-to-date and state of the art virus protection programme,
- password, biometric or other security method for activation,
- web browser whose version is currently supported by the manufacturer to ensure a secure log-in to the Virtual Desktop Infrastructure,
- stable internet connection and
- VMware Horizon Client software in the specified version.

Second, separate end-user device for two-factor authentication

The end-user device to be used for two-factor authentication (e.g. a smartphone) may only be used by the researcher authorised for access and must be equipped or secured with:

- Operating system supported by the manufacturer (e.g. Android or iOS) supported by the technology of the second factor,
- password, biometric or other security method for activation and
- Two-factor authentication app (Cisco Duo Mobile) in the version currently provided by the manufacturer.

Commitments

Institution

- Use of the access exclusively for a granted research project and not for any other than the permissible and lawful scientific purpose.
- Access only for researchers who have a valid employment relationship with the scientific institution, have undertaken in writing to comply with all confidentiality obligations (in particular statistical confidentiality in accordance with Article 17 of the Federal Statistics Act) and have undertaken in writing to keep the personal access data assigned for two-factor authentication (password and security code) secret, not to pass them on and to protect them from inspection.
- If a researcher leaves the scientific institution or the research project, or if a researcher who is eligible for admission changes, this must be demonstrably announced.
- Instructing all researchers on data security measures of the General Data Protection Regulation and all data protection requirements.
- Appointment of a Data Protection Officer.

Researcher

- Compliance with all data security measures of the General Data Protection Regulation and all legal data protection requirements.
- Obligation to maintain secrecy and absolute confidentiality with regard to all data made accessible.
- Prohibition to change or modify the configuration of the provided statistics programme for logging the procedures or the log files generated by the respective statistics programme.
- Prohibition of enabling another person to inspect or take note of data or of making data accessible to a person other than the researcher.
- Prohibition of the use of any screen recording, screen sharing, video conferencing tools or other such procedures during access.
- Prohibition of photographing, transcribing or taking a screenshot.
- Prohibition to make data available in any other way (e.g. by creating written records) outside the access point.
- Prohibition of attempting to re-identify statistical units.
- Prohibition of simultaneous use of the internet for other purposes during the access.
- Prohibition of the use of other media and information sources during access.
- As a result of the research project, the inference to affected persons must also be ruled out by way of indirect identification.
- The source code shall be written in such a way that an automated control of the maintenance of secrecy is supported by suitable routines, in particular the implementation of case counters.