SecureData Lab Access Point

Location and Physical Security

- **Separate Room:** The access point is located in a dedicated, secure room within the research institution to prevent unauthorized viewing, observation, and potential loss or theft. It should not be placed in an open or public area.
- **Lockable Room:** The room housing the access point must be lockable to ensure controlled access.
- **Surveillance:** Video recording is permitted in the room where the access point is located to maintain security and compliace with the security measures.
- **Multi-purpose Use:** When not in use as an access point, the room may serve other purposes, provided these do not conflict with its primary function.
- **Restricted Maintenance:** Cleaning or technical maintenance should only occur when the room is not being used as an access point.
- **Data Privacy:** The access point must be configured to ensure that only the authorized researcher can view the data.

Technical Security Measures

- **Session Security:** When the authorized researcher leaves the access point, even for a short period, the data must be protected from viewing by others through appropriate technical measures, such as VDI logout, screen lock, or turning off the device.

Technical and Organizational Measures (TOM) to Ensure Data Security in the SecureData Lab

End-User Device Requirements

The end-user device used to access the SecureData Lab must be managed by the scientific institution and meet the following criteria:

- **Updated OS:** A maintained operating system (Windows, Linux, macOS) with current software patches.
- **Virus Protection:** An up-to-date, state-of-the-art antivirus program.
- **Secure Activation:** Use of passwords, biometrics, or other secure methods for device activation.
- **Supported Browser:** A web browser with a version currently supported by the manufacturer to ensure secure login to the Virtual Desktop Infrastructure.
- **No Iternet Connection**

Yubico Key for Two-Factor Authentication

A separate end-user device for Yubico Key two-factor authentication must meet these requirements:

- **Secure Activation:** Password, Physical Key, or other secure methods for device activation.
- **Ubico Key:** The Yubico Key in the latest version provided by the manufacturer.

Institutional Commitments

- **Restricted Use:** The access point is exclusively for granted research projects and lawful scientific purposes.
- **Authorized Access:** Only researchers with a valid employment relationship with the institution, who have committed in writing to confidentiality obligations and the protection of personal access data, can use the access point.
- **Notification of Changes:** Any changes in researcher eligibility, employment status, or project participation must be promptly reported.
- **Training:** All researchers must be instructed on data security measures per the General Data Protection Regulation and other relevant data protection requirements.
- **Data Protection Officer:** Appointment of a Data Protection Officer is mandatory to oversee compliance and data security.