Technical and organizational measures for the internal IT systems

General measures within IEA

The employees of the organization take on a decisive role in the data processing in the IEA Hamburg, as they need access to the data in order to carry out their work. In order for the employees to be able to carry out their tasks in a secure environment, the following measures form the basis for secure data processing within the IEA Hamburg:

Commitment to confidentiality

All employees of the IEA Hamburg have signed a confidentiality agreement and are obliged to comply.

Compliance with legislation

When using the IT systems and applications in the IEA Hamburg, the employees must comply with the applicable data protection and data security regulations as well as company regulations. If employees are unsure as to whether and to what extent legislation or company regulations must be observed, they should contact their supervisor, the company Data Protection Officer or the Information Security Officer for clarification.

Raising employee awareness

Security measures can only be effectively implemented with informed and attentive employees who are able to recognize possible security incidents in time. All employees are therefore regularly trained and informed about information security in order to gain and maintain a high level of awareness and understanding of the topic.

Security organization

The IEA Hamburg has set up an information security organization according to BSI[1] protection rules and guidelines. Employees are required to immediately report security incidents to the Information Security Officer, who will take care of further coordination and handling of the incident.

Technical and organizational measures within IEA Hamburg

The collected data will be processed within the building of the IEA Hamburg. It is important to prevent unauthorized access to the data and information. In order to ensure the confidentiality of the data in the IEA Hamburg and to protect against unauthorized knowledge, the following measures are implemented:

Entrance control

The access of unauthorized persons to the building and to the data processing systems is denied through the following measures:

[1] Federal Office for Information Security

- Access Control System
- ID-Card required
- Locking system with transponder
- Security Locks
- Key control
- Checks on persons
- Designation of authorized persons
- Cleaning and maintenance staff obliged to data protection (permanent employment)
- Specified cleaning and maintenance times
- Supervision of maintenance work
- Accompanying guests and external service providers
- Subdivision into security zones
- Alarm system

Access to systems

The unauthorized use of the data processing systems is prevented by the following measures:

- Specified user account for each employee
- Authentication with password
- Authentication via directory services
- Automated screen lock
- Dedicated networks for sensitive systems
- Access restrictions by user-groups and devices
- Regulations on hiring and leaving employees

Access to data

Only authorized persons can process and use the data released to them, while unauthorized persons can neither read nor modify this data. For this purpose, the following measures are taken:

- Differentiated permissions for different transactions/ functions
- Access-rights are assigned by the IT department according to the specifications of the departments
- Restrictive assignment of administrator rights
- Role Concept
- Disk encryption
- File encryption
- Secure deletion of data
- Authorization rules
- Differentiated permissions for data objects
- Secure storage of (removable) data carriers
- Strict password policies
- Regular password changes

Authorized persons

The access to the systems is regulated by different user levels with different rights adapted to them:

- **Administrators**: The Administrators group has access to all resources. The systems are administrated exclusively by the IT department.
- **Selected Software Developers**: Selected Developers will have temporary access to the resources needed to set up and configure the web application and databases in the event of an update or necessary changes.
- **Data controller of the department**: A responsible person is defined within the project who has access to the databases to configure and monitor them.
- **Selected users**: The project staff entrusted with the further processing of the is provided with the necessary data to fulfill their work and to process the collected data.

Data separation

The separate processing of collected data for different purposes is ensured by:

- Separation of productive and test system
- Logical data separation
- Differentiated authorizations for data management
- Differentiate administrative tasks in data management

Malware protection

Each client has Antivirus-Software installed. Automatic updates are enabled and managed by the IT department. This process includes the protection of mobile devices as well.

Infected IT systems are immediately disconnected from all networks and are no longer used productively until fully cleaned up. Depending on the extent or type of infestation, reinstallation may be necessary.

The security-relevant updates and patches published for all operating systems, all installed drivers and programs are promptly installed on all IT systems. This is especially true for programs that access foreign networks (e.g. web browser).

Backup and restore

A regular data backup is guaranteed. The data is backed up on hard disks and tapes according to a planned and fixed schedule. The data recovery has been tested. The tapes are stored in secure containers separated from the IT systems.