Attachment to the main sheet: Technical and Organisational Measures

1
Access control

Guided tours for visitors
Visitors are not allowed to move freely within the office. They are to be continuously accompanied by an employee.

Record-keeping of visitors to secured areas
The date, time and duration of each visit to data processing areas are documented by:
Employees: Human Resources
Documentation: Visitors' book in the HR office

Documentation of access rights
Access rights to the data processing systems are documented by IT administrators
Document: no document, information is secured by controlled key allocation

Record-keeping of visitors to general areas
Each visit is documented by: Entry in the visitors book

List of authorized persons (server room)
A list of persons with access rights is kept. These are:
IT administrators other employees: Helmut Radtke, Marion Richter
Document: no documentation needed, secured by controlled key allocation

Harmful environmental influences for data processing
Following are dangers due to environmental influences in the data processing rooms, as well as methods of mitigation:
Fire: fire extinguishers
Power failure: UPS's for the most important servers
Overvoltage: the computer power supply system is protected against overvoltage

Protective measures for server room
The server is located in a locked room: yes, with steel core
Security window: no, server room is located on the 1st floor

Safety measures against environmental influences
Safety measures to protect against environmental influences are:
Fireproof and waterproof storage of files, data carriers, uninterruptible power supply of power via circuit breaker surge protection

Securing access (additional doors, windows)
Any additional entrances (side doors, windows) are secured by: security windows and security doors. The windows / doors are locked when leaving.

Responsibility of security
Details regarding company and location security are determined by Management

Responsibility of access
The person responsible for access to the company and offices: Managing Director

2
Admission control

Logging off devices
Employees are required to log out when leaving their workstation. Each station additionally has an automatic logout after five minutes

Authentication for IT systems
The user is authenticated via: Password

User rights
Users rights are limited to those needed to perform their specific tasks. These rights also control which software modules they have access to (e.g. purchasing, order processing, personnel) and thus which data is visible.

Unlocking of administrative accesses
If an administrative access is blocked, procedure to unlock is as follows:
Unlocking is documented via Service Desk

Logging and protocols on data processing equipment
The creation of protocols about activities on data processing systems is: automatic

Control of activity protocols on data processing equipment
The activity logs on data processing equipment automatic are controlled as follows: manual control as needed.

Protection measures for data management
The following measures are taken to protect data management:
For IT systems: assigned passwords
File logging of login data: locked filing cabinets within a locked filing room

Personal password assignment
Privacy and safety of every assigned password is guaranteed by:
Every employee has their own password witProhibition of disclosure

Guarantee of protection of administrative passwords
Information sheet for authorized persons on how to use administrative passwords.
Access granted only to selected persons
List of employees Document:

Secure storage of administrative passwords
The secure storage of administration passwords is ensured as follows: the location of storage is known only to select employees. The information is additionally stored in paper form, secured in a safe locked cabinet. Access to the encrypted document is reserved for the MA, IT

Password Security
Password security is guaranteed by: Specifications on length and complexity of passwords. (e.g. use of special characters, numbers)

Securing IT systems against unauthorised persons
The company's IT systems are secured by the following measures: dedicated line subscriber identification

User password storage
Passwords are stored with encryption

Storage of system passwords
System passwords are stored with encryption

Incorrect password procedures
A lockout for the user in case of wrong password is not activated for domain access.

Responsibility of access control
The person responsible for access control is the managing director and the IT Administrators

Group password designation
Group passwords are designated to: Interns
Note: Group passwords should be avoided if possible.

3
Access control

Place or type of storage of data carriers
Data is stored as follows: locked archive in safe locked cabinets

Distribution of access authorization
Access authorization is divided into/by:
Application programs (or individual modules of the software), Files, Data records, Data fields, Operating system, Server IT system

Logging of access authorizations
The access authorizations are logged: Document: currently not available

Access control responsibility
The person responsible for access control in is the managing director and the IT Administrators

User access to software
Employees can only access tested and approved software

Access control for employees
Employees access is controlled as follows: Users only have the rights needed to fullfill their tasks. These rights also control which software modules and data are visible (e.g. purchasing, order processing, personnel).

4
Passing control/transmission control

Organisation of data transmission
The following measures have been taken to organise data transmission: Documentation and regulation of all transmission paths and storage locations. Data is also stored on secure servers, only employees with special authorization have access

Private carriers
Bringing private data carriers is regulated as follows: general ban

Use of online banking
RS Marion
Online banking is carried out with the following program: direct banking

Arrangements with former employees
When an employee leaves the company, the user account is immediately blocked
When employees are transferred, the rights to software or data that are no longer required are deleted immediately.

Data protection during transfer
Data is protected from unauthorized persons during the transfer process by encryption

Security measures during remote maintenance
The following safety measures apply for remote maintenance: Remote maintenance is only permitted via a company-owned login server. Access is limited in time, is monitored and is logged in detail in log files

Security measures when using the Internet
The secure use of the internet is guaranteed by the following measures:
Use of anti-virus scanner (manufacturer automatic update)
Use of firewall (manufacturer automatic update)
Use of https (SSL, TLS) FTP
Use of intrusion detection system (IDS) Intrusion prevention system (IPS) VPN

Online banking security
The security of online banking is guaranteed by the following measures:
Push Tan, SMS-Tan (depending on the bank)

Email transfer security measures
The following security measures are taken when sending emails: they are always encrypted for sensitive data (S/MiME, PGB)

Security measures for external service providers
Services (e.g. repairs) are generally carried out outside the company, and the following safety measures are taken: all data is encrypted

Responsibility of remote maintenance
Permission to perform remote maintenance is granted by: Managing Director, the head of Department, or the IT Administrators

Data carrier Destroyal
Data carriers are destroyed by: magnetic data carriers, multiple overwrites via a secure procedure, physical destruction of information, external disposal companies, shredding of all in-house paper files, disposal of documents via shredder certified disposal company.
Data destruction is documented.

Encryption of data during transport
The following data is encrypted during transport: sensitive data

Safekeeping of unused data carriers
Unused data media is stored as follows: Locked cabinet in a safe Locked room

5
Input control/plausibility check/transaction control

Installation of new software
The following security measures apply when installing new software: Anti-Virus Scan, Authenticity check

Scanning intervals for antivirus software
Anti-virus software checks take place: continuously

Network documentation
Network documentation is recorded: Continuously
Storage type and location: Google Docs/DC1
Note: The minimum requirement for network documentation should be a cleaned up network. In regards to commissioned data processing, the contractor should also provide an application map with information flows of the commissioned IT environment.

Malware protection
The system is protected against malware as follows:
Antivirus software: Fortinet Antivirus Scan, MS Defender
Firewall: Fortinet 6

Data and program storage
Data and programs are stored as follows: in different directories

Foreign data carriers
The following security measures apply to the use of external data carriers: Use of foreign data carriers is excluded

Application program updates
Updates of the application programs are: automatic

Operating system updates
The installation of security-relevant updates for the operating system take place: Immediately and automatically

Malware protection updates
Malware protection is updated: automatically

6
Contract control/contract conformity control

Measures to ensure that data processing is carried out in accordance with instructions
The following measures ensure that the processing of the data is carried out in accordance with the instructions: written contract client receives data output for control purposes control on site by client possible

7
Availability control

Backup copy generation numbers
Backup copies are made according to the generation principle.
Number of generations: Grandfather-Father-Son principle

Archiving important emails
Important emails are archived as follows: automatically

Archive regulations
An archive order is available
Note: An archive order regulates, for example, which documents are archived, who is responsible for which archived data, when certain data is archived, data retention periods, deletion periods, viewing requirements, and outputting data

Archive Manager
The archive manager is: Mrs. Marion Richter

Backup media Storage
The backup media is stored: in the Vault server room

Backup methods
During a backup the following is saved:
Total backup, data stocks, altered data
Documentation of backup procedure: The backup procedure is documented regularly

Legal storage obligations
All statutory storage requirements are complied with. Compliance is monitored.

Air conditioning of the server room
The server room is air-conditioned

Backup procedure control
The backup procedure is controlled regularly by the managing IT administrators

Protective archive measures
The archive is protected by the following measures: specified room, locked access only for authorized archive administrators on site

Time interval backup
A backup is created according to the following backup plan:
https://docs.google.com/spreadsheets/d/1MYY78hlbQ41S3gDex_RwPVgOo0JaS0EkrWIeA4FcfWE/edit#gid=0

8
Audit of business organisation and accountability

Compliance with data protection in regards to data
The following organisational measures ensure compliance with data protection in regards to data: Documentation/recording of all programs, regulation protocols of any storage/archiving, pre-defined procedures for granting of access authorizations

Compliance with data protection with regard to the rights of individuals
The following organisational measures ensure compliance with data protection with regard to the rights of the persons concerned: Assertion of rights (information, deletion, etc.) is processed and documented immediately, compliance with the level of protection under Articles 44, 46 and 49 of the DS-GVO in the case of transfer to third countries

Compliance with data protection with regard to employees
The following organisational measures ensure that employees comply with data protection: Complete and up-to-date processing directory, employee training sessions on data protection, confidentiality clauses for employees, external data protection officer, a certificate of competence of data protection for the officer, Confidentiality clauses in all freelance contracts, contract with contract processor

This information refers to the server room in our office. The web application is hosted externally, which makes it professional, resulting in separately implemented security standards.