Technical and Organizational Measures

Version 4 | Valid from 2nd December 2025

Luware

1 Confidentiality

Access Control: Prevention of unauthorized access to data processing systems
Security locks; Chip card / transponder locking system; Door security (electric door closer, TV monitor); Alarm system; Intrusion detection system; Video surveillance; Visitors only when accompanied by an employee permitted; Verifiable key control; Locking of office doors in absence / outside working hours; Closing of windows in absence / outside working hours; Determination of authorized persons (employees and non-employees); Third party companies always under supervision; Visitor regulation; Security areas

Access Control: Prevention of unauthorized system use
Use of encryption routines for files and data carriers; Access to wireless network encrypted (WLAN); Controlled destruction of data media; Password policy; Clean-desk-policy; User locked in case of repeated incorrect password input; Process when an employee joins; Process when an employee leaves; Procedures for data collection templates; Audit, voting and control systems; File organization guidelines (Attachment to project folders / shares / etc.); Assignment and securing of identification keys; Non-disclosure agreements (all Employees sign a confidentiality agreement before beginning their work at Luware); Usernames / passwords for all data and programs; Differentiated access control; Locking of data terminals; Creation of a user master record per user; Use of up-to-date firewall; Use of up-to-date virus protection; Functional and/or timely limited use of terminals; Identification of a terminal on the IT system

Access Control: User control; Prevention of unauthorized reading, copying, modification or removal within the system
Encryption of laptops; Administration of user rights by system administrators; Use of an up-to-date firewall; Video surveillance; Limitation of access time; Use of up-to-date virus protection; Reduced number of administrators (need-to-know basis); Implementation of additional account without administrator privileges; Verification of authorization; Restriction of free querying possibilities of databases (query language); Use of shredders; Use of service providers for file and data destruction; Data protection compliant deletion / rewriting before reuse of a data carrier; Use of personalized administrator accounts; Use of encryption routines for files and data carriers; Process in case of an employee's entry or leave; Regulation of access on a strict need-to-know basis; Limited access possibilities to databases and functions in accordance with the tasks of employees; IT systems with up-to-date firewalls

Encryption: to ensure confidentiality of personal data
Data encrypted in transit TLS 1.2 and at rest.

Data Classification: as a security measure
Information is categorized into different levels (e.g., Internal, Confidential, etc.) to determine the appropriate security measures for each type.

Separation Control: Processing is conducted separately for data sets collected for different purposes.
Logically separated storage on different systems or data carriers; Client separation (purpose related); Separation of networks (physical / logical) by application (Production / Test / DMZ); Separation of productive and test system.

Pseudonymization: for reasons of data minimization

Pseudonymization takes place at Luware where appropriate and possible on request in which case the processing of the personal data takes place in such a way that the data can no longer be assigned to a specific person without the need for additional information.

2   Integrity

Transfer Control / Transmission Control: Prevention of unauthorized reading, copying, modification or deletion during electronic transmission
Use of an up-to-date firewall; Use of up-to-date virus protection; Data protection compliant deletion / rewriting before reuse of data carriers; Use of shredders; Use of service providers for file and data destruction (if possible with certificate) including logging of destruction; Use of encryption routines for files and data media; Use of VPNs; Email Encryption on demand; Fixed disk storage; Authorized persons identification; Secure entrance to data center for deliveries; Separated locking of confidential media; Security cabinets; Transfer of data in anonymous or pseudonymous ways

Entry Control / Data Media Control / Storage Control: Determination if and by whom personal data is entered, modified and deleted
Traceability and logging of input; Modification and deletion of data by individual users; Use of electronic signature, procedural, program, and workflow organization; Assignment of rights for input; Change and deletion of data based on an authorization concept; Cloud Customers data storage on Microsoft Azure CloudIncident Response:A formal incident response process is in place to ensure timely detection, reporting, and mitigation of any security events that may affect the integrity of data.

Backup and Recovery
Regular and secure backup procedures in place to ensure that data integrity is maintained, and business continuity is possible in the event of a disaster

Data Retention and Deletion
Defined retention policy based on purpose and legal requirements.
Change Management: Changes to systems, software, and infrastructure undergo a formal change management process to ensure integrity is maintained and risks are assessed before implementation

Security Awareness and Training
Training programs to educate employees about potential threats (e.g., phishing) that could compromise data integrity, and the importance of maintaining accurate and trustworthy data

3   Availability, Capacity, Recoverability

Business Continuity and Disaster Recovery
A documented and regularly tested Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) are in place to ensure the availability of critical systems and data during disruptive events.

Protection of accidental or intentional destruction or loss
Storage of data in a safe, separated location; Fire protection measures; Emergency plan; Backup and recovery concept; Antivirus concept; Execution of regular backups; Design of measures for property security; Fire and smoke alarm systems; Air conditioning; Use of an up-to-date virus protection; Use of an up-to-date firewall; Service and maintenance contracts for software and hardware

4   Regular Review, Valuation and Assessment

Data Protection-, Incident-Response- and Processing Management
Data processing only under direction of the data controller (Data Processing Agreements in place where applicable); Verification of availability of required systems/ data carriers/ license keys etc. to ensure the rapid recovery of data and programs (disaster recovery scenarios); Regular data and program recoverability tests; Data backup scenarios - the respective application must also be available in the version status of the data backup to ensure recovery; Appointment of a data protection officer; early involvement of the data protection officer in new projects; Data protection organization in the company; Privacy policies; Processes to optimize data protection; Regular review of data protection standards; privacy by default; Obligation of secrecy by all employees and other third parties (if applicable); Training and instruction for employees.

5   Certifications and Audit Reports

- ISO/IEC 27001
- ISO 9001
- ISO 14001
- SOC 2 Type 2 for security principles

www.luware.com