

1. Information security

1.1. The supplier/contractor protects astora's information by implementing the measures set out in this document. The implementation and compliance with these measures must be regularly checked by the supplier/contractor.¹

1.2. Employees of the supplier/contractor who are supposed to have access to astora's networks, systems or data must acknowledge their knowledge and compliance with the requirements of this document in a written statement.

1.3. The supplier must ensure that subcontractors employed by him also observe all astora's information security requirements resulting from this document in the context of their activities with reference to astora.

2. Organization of information security

2.1. The supplier/contractor appoints a competent contact person as the contact person for information security.

2.2. The supplier/contractor designs processes and performs tasks for astora in compliance with the principles of segregation of duties, need-to-know and least-privilege where it is appropriate and necessary.

3. Information security in personnel deployment

The supplier/contractor ensures that

3.1. Personnel appointed by him, which have access to astora's information, undertake to protect such information by signing a non-disclosure agreement. The non-disclosure agreement must be submitted to astora and must be valid beyond the project and the employment.²

3.2. the personnel deployed by him who no longer need access to information and systems from astora, no longer have access to this information and systems granted by the supplier.

3.3. the personnel employed by him, who leaves the supplier/contractor or no longer has any connection to astora, duly returns the computer equipment and information entrusted to him.

3.4. the staff is qualified and trained for the respective tasks (including information security).

4. Asset Management

With regard to the management of assets, the supplier/contractor shall ensure that:

4.1. information assets of astora cannot be removed from astora's premises without prior permission.³

4.2. astora's information is logically processed and stored separately from other information.

4.3. Upon completion or termination of the work of the supplier/contractor for astora, all copies of the astora information, including all backups and archiving copies, are cleaned and safely destroyed in electronic and non-electronic form (or returned to astora upon request). Exceptions are possible in the case of legal requirements. On request, astora must be provided with evidence on the safe destruction including relevant information (what, when, how, who, witnesses).

5. Access control

As part of the access control to the astora information, the supplier/contractor, in his area of responsibility, shall ensure the following:

5.1. Access to astora information always follows the principle of need-to-know and minimum right assignment (Least-Privilege).

5.2. There are reliable records of access to astora's systems and applications. The records ensure the imputability of the accesses.

5.3. Devices are connected to the astora infrastructure only after formal approval by astora.

5.4. Devices connected to the astora infrastructure are equipped with up-to-date malware protection and up-to-date functional and security updates/patches.

5.5. Before inserting any external data carrier into the astora gas storage infrastructure (e.g. USB, CD, DVD, external hard drive), the supplier/contractor must obtain written permission from astora and perform a prior check for malware.

5.6. Remote access to the astora infrastructure may only be implemented via communication channels and technologies pre-approved by astora (VPN, dedicated line, two-factor authentication).

5.7. Systems on which astora information is processed, stored, or transmitted have appropriate access and identity management. This includes at least the following security measures:

- a) Use of unique user IDs.
- b) Authorization and management of access rights.
- c) timely deletion of obsolete access rights.
- d) Regularly reviewing access rights for business needs and security requirements.
- e) Audit-proof logging of access activities related to astora information.

¹ Alternative protective measures are only permitted if they have been approved in advance by astora.

² The non-disclosure agreement may be universal

³ Information assets include data, applications, hardware, process control components, and other supporting assets.

- f) Astora password requirements or stricter requirements are applied and enforced.

6. Cryptography

6.1. Cryptographic measures must be applied in accordance with all relevant agreements, laws and regulations.

7. Physical and environmental security

7.1. Visitor passes must always be carried in a clearly visible place on the premises and in the offices/areas of the astora.

8. Operations security

In the context of services to or on astora information systems, suppliers shall apply the following measures:

8.1. astora must be informed about existing or potential availability restrictions of astora information systems, which are administrated by the supplier/contractor, unless otherwise stipulated.

8.2. Systems that are permanently connected to the astora infrastructure must meet the following security requirements:

- a) Privileged user activities are logged.
- b) Records are maintained audit-proof. At least security-related events must be logged.⁴
- c) Logs must be kept for at least 90 days and made available to astora upon request within this time.
- d) Backups must be performed and maintained in such a way to meet their agreed objective.
- e) Malware protection is active and kept up to date, wherever technically feasible.
- f) An appropriate vulnerability and patch management process is applied to ensure that the supplier's systems are updated in a timely manner.

9. Communication security

9.1. astora information at rest or transmission must be protected by appropriate security measures (e.g. encryption, firewalls, intrusion detection/prevention, etc.).

9.2. Wireless network connections from suppliers/contractors transmitting astora information must apply at least the WPA2 security standard.

10. Information security incident management

10.1. The supplier/contractor shall have processes in place that allow appropriate handling of security incidents in the context of the organization of the supplier/contractor.

10.2. Security incidents or vulnerabilities at the supplier/contractor, for which effects on astora cannot be certainly excluded, must be reported

immediately to the contact person at astora or the information security officer of astora.⁵

11. Business Continuity Management

11.1. The supplier/contractor supports the astora security organization in the annual ISMS risk management process on request by astora.

12. Compliance

12.1. Upon astora's request, the supplier/contractor must demonstrate compliance with the safety requirements described in this document by an appropriate audit by astora or its agents or in any other appropriate manner.

⁴ Security-related events are events that can affect the confidentiality, integrity, or availability of information systems.

⁵ Tel.: 0561 99858 7038 or it-security@astora.de