General requirements to the Information Security for suppliers of astora GmbH

1. Introduction

1.1. astora GmbH, hereinafter referred to as astora, is an operator of a critical infrastructure within the meaning of the §2 KRITIS direction Energy Sector. The company is obliged to comply with the security requirements of the IT security catalogue in accordance to §11 (1b) EnWG and to ensure that its suppliers who interact with company information and systems also comply with it.

This document describes basic security requirements for astora suppliers based on the ISO/IEC 27001 and 27019 standards. Suppliers are understood to be all suppliers of goods and services. Company information is primarily data and documents in written or digital form. Company systems are any hardware and software owned or operated by the company or operated by third parties on behalf of astora (e.g. computers, servers, networks, storage media, etc.).

2. Information security requirements

2.1. Suppliers shall implement the requirements set out in this document. The implementation of and compliance with these requirements are to be checked by suppliers on a regular basis. Alternative protective measures are only permissible if they have been approved by astora in advance.

2.2. Supplier employees who are given access to company information and systems must be aware of the requirements set out in this document.

2.3. Suppliers must ensure that subcontractors also observe all astora relevant information security requirements resulting from this document in the context of their activities related to astora.

3. Requirements for the organization of information security

3.1. Suppliers shall appoint a competent contact person as a partner on the information security topic, if requested.

3.2. Suppliers design processes and perform tasks for astora in compliance with the principles of segregation of duties, need-to-know and least privilege where appropriate and necessary.

4. Information security requirements for staffing

Supplier ensure that

4.1. the staff employed for astora is at least generally committed to maintain confidentiality.

4.2. access rights to information and systems of astora granted by the supplier are revoked on a timely manner when the access is no longer required.

4.3. the personnel employed for astora, properly return the IT equipment and information and delete existing copies of it, as far as the employment is terminated or no activities are performed for astora anymore.

5. Requirements for the management of assets[1]

With regard to the management of assets, suppliers shall ensure that

5.1. assets of astora may not be removed from astora's premises without prior permission.

5.2. Company information is logically processed and stored separately from third-party information.

5.3. after completion or termination of the services for astora, all copies of the company information, including all backup and archival copies, in electronic or non-electronic form, are purged or securely destroyed (or returned to astora upon request; exceptions are possible in case of legal requirements). Evidence of secure destruction must be provided upon request by astora with relevant details (what, when, how, who, witness if applicable).

6. Access control requirements

With regard to access control to company information, suppliers shall ensure within their area of responsibility that

6.1. the connection of devices to astora's infrastructure only takes place after approval by astora.

6.2. devices connected to astora's infrastructure are equipped with up-to-date malware protection and are kept up to date in terms of security and function updates.

6.3. before introducing an external data device into astora's infrastructure (e.g. USB, CD, DVD, external hard disk), a prior check for malware is carried out.

6.4. remote access to astora's infrastructure takes place exclusively via communication channels and technologies approved by astora in advance (e.g. VPN, dedicated line, two-factor authentication).

6.5. electronic systems on which company information is processed, stored or transmitted have state of the art access and identity management.

7. Physical and environmental security requirements

7.1. Suppliers shall ensure that the rules set down by astora for entering the company's premises are strictly observed.

8. Operational safety requirements

8.1. Suppliers' information systems that are permanently connected to astora's infrastructure must ensure the following:

[1] Values are data, applications, hardware, process control components, and other values that support them.

a) audit-proof logging of security-relevant user actions with a retention period of at least 90 days;
b) up-to-date malware protection;
c) vulnerability and patch management.

8.2. astora is to be informed about existing or potential availability restrictions of the information systems under the administration of the suppliers, if not otherwise regulated.

9. Communication security requirements

9.1. Company information stored, processed or transmitted on systems or data carriers must be protected according to the state of the art (e.g. encryption, use of firewalls, etc.).

9.2. Rules regarding classification and handling of information must be strictly observed. For guidance on the proper handling of classified information, see Appendix A.

10. Requirements for handling information security incidents

10.1. Suppliers shall have processes in place to adequately address security incidents in the context of their organization.

10.2. Security incidents or vulnerabilities, where an impact on astora cannot be excluded with certainty, are to be reported immediately to the contact person at astora or to it-security@astora.de without delay.

11. Compliance requirements

11.1. Upon request by astora, suppliers must demonstrate compliance with the security requirements described in this document by means of an appropriate inspection by astora or its authorized representatives or in another suitable manner.

Appendix A: Classification of information

The following rules are laid down for the classification and handling of documents in electronic, printed or other form:

Classification / Action	INTERNAL	CONFIDENTIAL	STRICTLY CONFIDENTIAL
Definition	Information on astora's internal processes which is accessible to a group of employees or contractors according to the "need-to-know" principle and which is not public.	Information about the company that is accessible to a group of employees or contractors in accordance with the "need-to-know" principle. The confidential information may include employees' personal data, information on legal processes, business and operations plans as well as financial statements and other business information related to this confidentiality class as determined by the information owners.	Information that is available to a limited number of employees according to the "need-to-know" principle. They may include all types of information (industrial, financial, commercial, etc.) that have an actual or potential value due to the confidentiality of this information to third parties.
Labelling	Implicit. Unlabeled information is always to be treated as INTERNAL.	Always to be labeled CONFIDENTIAL. Bold capital letters on each page in the header. Page number and total number of pages in the footer.	Same as CONFIDENTIAL and additionally naming all recipients of the document on the first page.
Reproduction by means of a photocopier or printer	Remove originals from the copier or printer as soon as possible. Copies, printouts and scans should not be made using publicly accessible equipment.	The process of copying, printing or scanning must be supervised. Copies, printouts and scans must not be made using publicly accessible equipment.	Same as CONFIDENTIAL. Copying or printing only with permission of the information owner of astora.
Forwarding to third parties	Only with permission of the information owner of astora.	**Prohibited**. Other regulations can be agreed with astora in individual contracts.	
Transmission by e-mail	Ensure that the recipient's e-mail address is correct.	Ensure that the recipient's address is official and correct. The recipient must be authorized to receive this information. The text and attachments of the e-mail must be encrypted.	
Postal mailing	The information can be sent in a normal envelope.	Send the information in a tamper-proof envelope and obtain an acknowledgement of receipt (use a sealed envelope labelled CONFIDENTIAL in a second, outer envelope without a label).	Same as CONFIDENTIAL and additionally send by postal service with handover to the recipient or by courier.
Transmission by fax	Ensure that the recipient's number is correct. Use a cover sheet that shows the total number of pages.	**Prohibited.**	
Destruction of information recorded on paper	Securely destroy documents using a P5 security level shredder.		
Oral dissemination	Only permissible if no unauthorized persons can listen in. Verification of the identity of the person being spoken to.		
Storing information in IT applications	Ensure the need-to-know principle. Establish measures to protect against unauthorized access.		

Classification / Action	INTERNAL	CONFIDENTIAL	STRICTLY CONFIDENTIAL
Storing information on file servers and mobile devices	Store information on available drives or in folders, taking into account access rights according to their classification; if necessary, explicitly assign access rights.	IN ADDITION, the information shall be stored in encrypted folders. Encryption must use at least the standards AES-128 or higher, RSA-2048 or higher.	
Storing information on portable storage media.	Data must be encrypted.		
Erasing electronic information from portable Storage media	Multiple overwriting of the used memory areas is possible.		
Disposal of portable Storage media	physical destruction of the storage media.		
Storage of information in cloud services	Generally prohibited. Other arrangements can be made in individual contracts with astora.		