Information security requirements for EnBW AG contractors ›

EnBW-HST-026

Document information

Scope	EnBW Group
Version	1.0.1
Classification level	Public
Summary	This document describes binding requirements for information security at EnBW AG contractors
Entry into force	05.04.2023
Last updated	03.05.2023
Competent body	CISO (C-TS)
Approved by	Markus Penn, Group ISM, C-TSM
Approved on	03.05.2023
Attachments	-

Revision history

Version	Update date	FZS/Author	Brief description
1.0	05.04.2023	CISO	Original Release
1.0.1	03.05.2023	CISO	Improvement of translation in 2.1

In case of doubt, the German version of this document shall prevail.

Contents

1 Scope of the Agreement

These information security requirements are the basis for every supplier/contractor (hereinafter referred to as "contractor") of EnBW Energie Baden-Württemberg AG (hereinafter referred to as "EnBW") who receives access to buildings or premises or access and/or access to electronic information or information systems of EnBW within the framework of the processing of a contractual relationship. The contractors are obliged to comply with the provisions of this Annex without fail, insofar as no deviating provisions have been contractually agreed.

This annex obliges all contractors, regardless of whether an IT workstation system is provided to EnBW or is accessed with its own systems or with a connection to resources in the EnBW communication network.

2 Information security requirements for contractors

Each contractor shall provide a contact person for information security on request and shall observe the following principles:

2.1 General Obligations

The contractor is aware that EnBW uses the object of performance as the operator of critical infrastructure for energy supply and is therefore subject to increased legal and regulatory requirements in the area of information security, in particular in accordance with the BSIG and the EnWG.

The contractor must have established a formal information security management system (ISMS) and must regularly further develop and update it.

The contractor must provide the deliveries and services in such a way that they meet the current legal and regulatory requirements with regard to EnBW's information security and, in particular, to protect EnBW's IT infrastructure at the time the service is provided. It is obliged to take appropriate precautions to ensure that the data it processes is protected according to the state of the art in terms of information security against attacks or other incidents with adverse effects on systems, machines, computers, networks or other infrastructure and resources due to unauthorised access, destruction, damage, publication or modification of information, "*denial of service attacks*" or other attacks.

The contractor shall provide EnBW with the IT security-relevant log data that is generated in connection with the processing of EnBW information. Where possible, this must be done automatically and in real time, for example by creating appropriate access, but in any case, without delay.

The contractor shall take sufficient detection and prevention measures against malware for its own data processing systems on which EnBW information is processed and implement suitable recovery measures.

Special backup settings, systems or other precautions on EnBW data processing systems (e.g., for protection against malware, encryption) may not be taken out of operation, circumvented or otherwise changed by the contractor, unless explicitly agreed otherwise.

The contractor shall regularly and promptly obtain information about technical vulnerabilities in the systems it uses and take appropriate measures.

The contractor shall comply with EnBW's specifications for the secure transfer of confidential information and data:

- Encryption of data during electronic transmission over unsafe networks
- Dispatch of paper documents in sealed envelopes
- Ensure that only authorised recipients receive the information.

Insofar as EnBW transmits strictly confidential information to the contractor, the parties shall conclude a separate agreement on its use. Strictly confidential information refers to information that is classified by EnBW as "strictly confidential".

The contractor must ensure that compliance with these information security requirements is an integral part of the contract of the contractor's employees.

2.2 Information obligations of the contractor

Changes to the supply chain, change of ownership and any changed basic requirements of the business relationship, in particular the withdrawal or expiry of existing certifications, must be reported to EnBW without delay.

The contractor shall establish an incident management process in order to be able to respond effectively to events, disruptions and incidents that could affect the service. Reporting channels and communication between the contractor and EnBW must be defined.

The contractor shall inform EnBW immediately of any vulnerabilities, events, disruptions, and incidents that could have an impact on the security of information and the quality of the delivery item and shall coordinate their handling with EnBW.

2.3 Availability of data

With regard to the availability of data and operational services, the contractor is obliged in coordination with EnBW to:

- regularly back up all data processed by it and store these backups in a secure location,
- have an emergency plan describing how to proceed in the event of security incidents or other emergencies and
- provide appropriate measures to ensure the protection of data in the event of emergencies, such as power outages or natural events.

2.4 Access of the contractor to EnBW systems

The contractor is obliged to have a procedure for regularly checking access rights in order to ensure that only authorised persons can access EnBW data processing systems.

The transport of EnBW's work results or IT systems from EnBW's business premises is only permitted within the scope of the contractually agreed service provision and requires the prior written approval of EnBW.

The stored authentication information (identifications and passwords) on EnBW data processing systems must be used in a personal manner. Disclosure to third parties is prohibited.

The contractor shall ensure that only those employees who are involved in the delivery performance are granted access to EnBW information.

Access to EnBW's data processing systems may only take place via the end devices, interfaces and services provided by EnBW and for the agreed purposes and tasks.

For its own systems on which EnBW information is processed, the contractor shall implement a secure login procedure in accordance with the state of the art (e.g., multi-factor authentication or use of strong passwords) to access these systems and applications. Strong passwords consist of at least fourteen (14) characters, at least three (3) character types consisting of number, lowercase letter, uppercase letter, and special character; consecutive characters are repeated no more than twice.

If remote access to EnBW data processing systems is granted, only the gateways, jump servers and services specified by EnBW may be used. Grid coupling or parallel remote access is prohibited.

2.5 Training and safety awareness of contractor's employees

The contractor must ensure that all employees who have access to EnBW information have the appropriate security awareness and the necessary knowledge and skills to process this data securely.

The contractor shall instruct its employees who are brought into the delivery service with regard to

- the information security requirements of the delivery performance,
- handling classified EnBW information and
- the detection, reporting and handling of security incidents.

2.6 Control rights and obligations

The contractor shall have a procedure for monitoring and documenting access to EnBW information and shall regularly check whether all access was authorised.

EnBW is entitled to carry out a regular review of compliance with the information security requirements to the extent required. The audit shall take place in consultation with the contractor and shall be announced with an appropriate advance notice period. Audit right includes the right to inspect any facility that processes EnBW information and also applies to subcontractors. The contractor shall contractually ensure that EnBW can also exercise its audit right with subcontractors. Expenses for this are not to be remunerated separately, unless otherwise agreed in the contract.

2.7 Return upon termination of the contractual relationship

Upon termination of the order, the contractor must return any values received from EnBW, e.g., access cards and tokens and end devices, without delay.