1 Field of application

According to the EnBW Group's General Terms and Conditions of Purchase (Section 3.3), EnBW's business partners, who are granted physical access to buildings or premises and/or logical access to EnBW's electronic information or information systems during a contractual relationship, are obliged to strictly comply with the provisions of this guidance, unless other contractual provisions have been agreed upon.

This guidance applies to all business partners connecting to resources in the EnBW communications network, regardless of them accessing EnBW information systems and information using EnBW IT equipment, or using their own systems.

2 Responsibilities

Many business partners are granted access to EnBW locations and premises or access to EnBW company information in the context of providing the service, and the use of EnBW systems and EnBW networks is made possible in this same context. This requires compliance with EnBW's security regulations, e.g. security measures to protect confidentiality, against computer viruses, hacking attempts and similar. For this purpose, it is mandatory to observe the following rules and principles.

3 General regulations of the data access

Each business partner referred to in Chapter 1 must observe the following 24 principles

1. compliance with information security (IS) regulations is an inherent part of the contract for the business partners employees.
2. the business partner trains its employees regarding the IS requirements of the provided service.
3. obligations to secrecy remain valid for the employees of the business partner beyond the end of the provided services, their participation in the services or the end of their employment with the business partner.
4. The removal of documents; working papers, notes and other work-related output; or IT systems outside the business premises of EnBW is not permitted and requires the prior written permission of EnBW.
5. Access to EnBW's IT systems may only be made using the IT equipment, gateways and services provided by EnBW and only for the agreed purposes and tasks.
6. Specific security settings, systems or other measures on EnBW's IT systems (e.g. to protect against computer viruses or encryption measures) may not be deactivated, bypassed or changed in any way unless explicitly agreed.

7. Upon termination of the contract, the business partner must return any information and documents received without being prompted and must properly delete any information that has not been returned. All assets received from EnBW, e.g. tokens and IT equipment, must be returned immediately.
8. The business partner complies with the classification of information at the provided service and ensures that it is treated properly in internal processes.
9. The business partner ensures, that only those employees who are involved in the service, are given access to EnBW information and data.
10. Secure logins (ID and passwords) used on EnBW's IT systems shall be strictly for individual use. Passing them on to third parties or disclosing them to others is not allowed.
11. For partner-owned/managed information systems in which EnBW information is processed, the Contractor must use a secure login procedure that employs strong passwords for access to these systems and applications.
12. For partner-owned/managed information systems in which EnBW information is processed, the Contractor shall implement sufficient detection, prevention and recovery measures against malware, and include appropriate instruction for its employees.
13. The Contractor shall gather information in a regular and timely manner about vulnerabilities and technical weaknesses in systems he uses and shall employ appropriate remediating measures.
14. If remote access to EnBW systems is granted, only EnBW-designated gateways, jump servers and services may be used. Alternate means of remote access is not permitted
15. The Contractor complies with EnBW requirements for the secure data and information transfer.
16. The delivery of services by sub-contractors may only take place within the agreed contractual framework. The expected transparency and security level required of the business partner by the contractual conditions with EnBW must be guaranteed along the entire supply chain.
17. Changes in the supply chain, changes in business ownership or other revisions to fundamental requirements, such as the withdrawal of existing certifications, must be reported to EnBW without delay.
18. The business partner shall establish an incident management process to respond effectively to events, incidents and malfunctions that may affect the service. Reporting procedures and communication between business partner and EnBW must be defined.
19. The business partner informs the EnBW as soon as possible about vulnerabilities, events, malfunctions and incidents that could have an influence on the information and the quality of the service and co-ordinates their management with EnBW.
20. The business partner trains its employees in the identification, reporting and handling of security incidents.
21. The business partner supports EnBW in compliance with the legal, regulatory and contractual obligations and requirements applicable to EnBW.
22. The contractor shall comply with the regulations on copyright.
23. The contractor complies with the regulations on data protection law.

24. EnBW is entitled to carry out regular audits of compliance with the IS requirements to the extent necessary. The audit will be carried out in consultation with the business partner and will be announced with a reasonable advance notice. The right to audit includes the right to inspect any facility that processes EnBW information and also applies to sub-contractors. Expenditure for this is not to be separately compensated unless otherwise agreed in the contract.