

Information leaflet - IT Security Policy external business partners of EnBW

1 Field of application

According to the General Terms of Purchase of the EnBW Group (Subclause 2.5) suppliers of EnBW who are granted access to electronic information of information systems of EnBW within the frame-work of processing a contractual relationship are obligated to strictly comply with the regulations of this information leaflet. For all cases of doubt as a supplement to this information leaflet the “luK Security Policy external business partners” of EnBW shall be available to the supplier at all times for inspection and compliance.

This information leaflet is directed at all business partners no matter whether an IT workplace sys-tem of EnBW is made available to them or they access the EnBW information systems with own systems or with a connection to resources in the EnBW communications network.

2 Responsibilities

Business partners are granted the access to company-own information of EnBW and enabled the use of EnBW systems and networks for the mutual benefit and to improve the efficiency of the business processing. This requires security measures for the protection of confidentiality, against computer vi-ruses, against hacking attacks, etc. To this end it is absolutely essential to comply with the following regulations and principles.

3 Confidentiality

Each business partner of EnBW undertakes to treat strictly confidential all information which he receives in connection with the access to the IT systems of EnBW or are accessible to him, in particular not to disclose these to any third party or to use these for other purposes than those as intended. Upon termination of the order the business partner must destroy without request or upon request re-turn any documents received. The obligation for confidentiality shall continue to exist permanently beyond the respective cooperation.

4 General regulations of the data access

Each business partner must observe the following principles when having access to the IT systems of EnBW:

- › The access may only be carried out via the respective terminals which are made available and for the agreed purposes and tasks.
- › The deposited protective mechanisms (identification codes and passwords) must be used per-person-specific. A forwarding or disclosure for third parties is to be avoided in all cases.
- › Special back-up settings, systems or other precautions (e.g. for the protection of computer vi-ruses) may not be put out of operation, circumvented or changed in any other manner.
- › The connection of own systems of the business partner to the communication network of EnBW is to be strictly avoided.
- › It is principally not permitted to take documents, work results or IT systems outside of the business premises of EnBW and requires the prior written consent of EnBW and in individual cases as business and trade secrets the coordination with the respective Security Manager.
- › The use of the e-mail configuration of EnBW requires the prior initial instructions and use by complying with the internal regulations of EnBW ("E-Mail etiquette"). In particular the automated forwarding of received e-mails to external post boxes is not permitted.
- › The business partner must moreover strictly comply with all relevant standard provisions in particular of a type under data protection law.

5 Special regulations for the data use in an individual case

- › EnBW reserves the right to stipulate a special security level in an individual case in advance when the business partner is dealing with especially sensitive data or data of EnBW which requires secrecy and to issue special protective instructions.
- › In case of suspicion of computer viruses or flow problems of the virus protection programs, which cannot be automatically identified or removed, the responsible department of EnBW is to be notified immediately.
- › Insofar as the business partner recognizes weak points and incidents with possible implications on the information security, he shall report these to the responsible department of EnBW immediately.

- › The compliance with the measures for IT security is controlled by EnBW and in particular monitored by the data protection officer and/or the group authorized agent of luK-Security of EnBW.

- › A breach of the provisions of this information leaflet can – irrespective of the other rights from the contractual relationship with the business partner – lead to the immediate withdrawal of the access authorization to the IT systems of EnBW.