



ENERPARC Group

Information Security Requirements for Provider and Supplier

Management Summary:	This guideline contains requirements relating to information security
Version:	2.0
Date of Version:	06.01.2026
Created by:	Laura Holder
Approved by:	
Confidential-Level:	C1-public

Änderungs-Historie

Date	Version	Created by	Description of Change
15.05.2025	0.1	Laura Holder	Initial creation
21.05.2025	1.0	Laura Holder	Addition of chapter 2
06.01.2026	2.0	Laura Holder	Review and addition in chapter 4

Validity notes: This document is only valid if it corresponds to the version published on the ENERPARC Group intranet.

Table of Content

1. PURPOSE, SCOPE AND USER	2
2. REFERENCE DOCUMENTS	2
3. IS SUPPLIER CHECK.....	2
4. INFORMATION SECURITY GUIDELINE	2
5. VALIDITY AND DOCUMENT MANAGEMENT	3

1. Purpose, scope and user

This guideline contains information security requirements and applies to all suppliers and service providers of the entire ENERPARC Group. It serves to maintain a high level of information security.

2. Reference documents

- ISO/IEC 27001:2022 Chapter A.5.19, A.5.20, A.5.21, A.5.22
- ISO/IEC 29019, 6.1.6 ENR, 6.1.7 ENR, 15.1.2

3. IS Supplier Check

The Contractor undertakes to complete the 'IS Supplier Check' form truthfully in advance and send it to is-gremium@enerparc.com.

4. Information Security Guideline

The Supplier undertakes to take all necessary technical and organizational measures to ensure information security in accordance with the applicable legal and contractual requirements. The Supplier shall ensure that appropriate measures are implemented to protect the confidentiality, integrity and availability of the processed data. As far as applicable, these include, but are not limited to:

- Policies and procedures regarding information security
- Encryption of sensitive data in transit and storage.
- Keep ENERPARC informed if an employee with access to ENERPARC data-exchange platforms leaves your company to disable the appropriate account.
- Regular security audits and penetration tests.
- Implementation of access controls and authentication mechanisms.
- Ensuring the physical security of the IT infrastructure.
- Vulnerability management in relation to third party libraries and own code

The Supplier must provide the Client with appropriate evidence of the implementation of these information security measures. This can be done, for example, by means of appropriate certificates (e.g. B. ISO 27001...). The Supplier undertakes to regularly check the validity and actuality of the certificates and to submit corresponding evidence to the Client.

The Supplier undertakes to regularly train its employees and to sensitize them to the importance of information security. This includes training on internal security policies as well as legal requirements.

The Client is entitled, at its own discretion, to carry out an audit annually or to have it carried out by a third party to verify compliance with the information security requirements. The Client agrees with the supplier on a specific date with at least one month's notice for the audit to be carried out. The Supplier shall provide all necessary information and access to facilitate these audits, insofar as they are relevant to the performance of this Agreement. However, the Supplier is not obliged to disclose trade secrets or other confidential information. The result of the audit is subject to confidentiality.

The Supplier undertakes to immediately report any security-related incidents affecting the availability, integrity, confidentiality and authenticity of the processed information to the Client via E-Mail at vorfall@enerparc.com.

The Supplier undertakes to pass on the above safety requirements to the subcontractors used to the extent necessary. The Supplier remains responsible for subcontractors' compliance with these requirements.

5. Validity and document management

This document is valid as of 01.02.2026

The owner of the document is the Management, who must review the document at least once a year and update it if necessary.

Management