Information Security Guideline for Suppliers

	Approval Vorwerk Gruppe	**Approval** Vorwerk Gruppe	**Apprval** Vorwerk Gruppe
Bereich	Global Director Purchasing	Global Director Quality	Informationssicherheits-Beauftragter
Name	Hr. Czayka	Hr. Schröder (QMB)	Hr. Münstermann (ISB)
Datum	01.11.2022	01.11.2022	01.11.2022
Unterschrift			

Inhalt

1. Introduction

The Vorwerk Autotec & Drivetec Group - hereinafter referred to as the Client - supplies many automotive customers with products of different requirements and functions.
In order to meet the current and future requirements of our customers and legislators as well as to safeguard the company against cybercrime, aspects of information security must be increasingly taken into account.
This Information Security Policy (ISR) forms the binding framework between client and supplier, and serves to meet the requirements for the protection of information with regard to confidentiality, integrity and availability.
This document is part of our terms and conditions of purchase and confirmation by the supplier is a prerequisite for delivery to our group of companies.

In case of contradiction, the German version shall apply.

2. Scope

These ISR apply to all suppliers and service providers of our group of companies:

Vorwerk Autotec GmbH & Co. KG - Wuppertal
Vorwerk Drivetec GmbH - Wuppertal
Vorwerk Autotec Polska Sp. z o.o. - Brodnica
Vorwerk Autotec (Suzhou) Limited
Vorwerk Drivetec (Suzhou) Limited
Vorwerk Autotec de México S.A. de C.V. – Lagos de Moreno
Vorwerk Autotec Serbia d.o.o. - Cacak
Vorwerk Drivetec Serbia d.o.o. – Cacak

3. Information security in supplier relationships

Vorwerk works exclusively with contractors who independently commit themselves to the fundamental protection of confidentiality of information and business secrets. In individual cases, if the information handed over or shared is subject to an increased need for security, special measures may also be demanded of contractors in order to take account of the increased need for security. This will mostly be done within the framework of non-disclosure agreements.

4. General requirements

4.1. Basics

The contractor is requested to expand its management system to include the principles of information security. Standards such as ISO/IEC 27001, VDA ISA catalogue or BSI IT-Grundschutz can serve as a basis. In individual cases, external certification, a passed TISAX assessment or self-assessment can become a prerequisite for certain business relationships.

4.2. Internal organisation

Policies, processes and responsibilities must be defined to implement and control information security.
information security can be implemented and controlled.
This includes in particular:

- The creation of an information security policy.
- User guidelines to define rules for the handling of applications, systems and IT end devices and behaviour when using information technology.
- The description of processes for the management of data carriers, documents and information.
- The definition of roles and responsibilities in the area of information security.
- The obligation of employees to maintain confidentiality and data secrecy.
- The regular implementation of training and awareness measures.

4.3. Physical and environmental security

The Contractor shall ensure that unauthorised access to rooms, offices and facilities in which Vorwerk's information is processed is excluded. This shall also apply to delivery and loading areas through which unauthorised persons could enter the premises.
The Contractor shall draw up guidelines regulating tidy working environments and screen locks when not in use.

4.4. Protection of information assets

The contractor is required to record its information assets, assess their need for protection and implement the necessary measures depending on the risk class.
Vorwerk uses a marking of its information assets. Documents marked "confidential" or "strictly confidential", as well as those whose content is of sensitive value in the normal business world, may only be made accessible to selected employees. Documents marked "internal" are intended for the business relationship between the contractor and the client and may be freely distributed within the company.
In principle:

- Both data and the carriers of this data must be protected against loss, destruction, manipulation and unauthorised access. Data carriers that are no longer required must be destroyed in accordance with secure procedures.
- Data may only be exchanged via data exchange channels approved by Vorwerk.
- The partner companies must ensure that no unauthorised third parties can listen in on confidential information or gain access to it. If the supplier intends to deliberately forward selected information to third parties, Vorwerk's approval must be obtained. This shall apply in particular to information on projects which are linked to a non-disclosure agreement. When sending e-mails, the distribution circle shall be limited to the necessary extent.

4.5. Incidents

Consistent and effective measures for the management of information security incidents (theft, system failure, data loss, etc.) with a potentially negative effect shall be implemented.
This includes in particular:

- The immediate reporting of information security incidents to the principal, especially when so-called cyber attacks become known.
- The logging of security incidents.
- The implementation of processes to initiate measures to prevent / repeat information security incidents.

4.6. Vulnerability and Patch Management

The exploitation of technical vulnerabilities must be prevented through the use of up-to-date virus protection software and the implementation of a regulated patch management system.
Regular checks to identify weaknesses in the IT structure must be carried out by external IT consultants if necessary.

4.7. Back ups

Measures shall be implemented to ensure that sensitive information and data / personal data are protected against accidental destruction or loss.

4.8. Kryptographie
The use of encryption procedures to ensure the proper and effective protection of the confidentiality, availability or integrity of personal data or information requiring protection. The use of cryptographic protection of communication is particularly necessary when data with a high need for protection is transmitted via public networks or networks that are not considered sufficiently secure.

4.9. Working outside the organisation
The contractor shall establish a policy for its employees that regulates working outside the organisation. The focus must be on the confidentiality of data and preventing unauthorised persons from intercepting, viewing, physically stealing or electronically tapping information.

4.10. Emergency Management
System availability must be maintained or restored as quickly as possible in difficult situations, such as crisis or damage situations. The supplier must draw up contingency plans for the critical information assets and IT systems to ensure continued business operations. These contingency plans must be regularly tested for effectiveness and optimised if necessary.

5. Requirements for organizations with access to the network

5.1. Handling log in datas
Login data must not be passed on to unauthorised persons. If there is any suspicion of compromise, the access data must be changed and the incident reported. Leaving the workplace is prohibited as long as access to the Vorwerk network exists.

5.2. Access rights
Access rights to Vorwerk systems must be requested. Access to Vorwerk data may only be made available to employees according to the need-to-know principle.

5.3. Handling information
All information is to be treated on the basic assumption that it is strictly confidential. Local storage of information and data is prohibited. Adaptations and updates to software and IT systems must be registered and approved with the Vorwerk contact persons.

6. Requirements for suppliers of software
The supplied software must not contain any functions that endanger the protection goals of the data and the software itself, in particular the undesired import and export of data and functions or the undesired modification of data or the flow logic. The supplier shall check according to the state of the art that no potentially damaging software (e.g. viruses, worms, Trojans) is supplied.

7. Changes

Date	Index	Description of changes
2022-11-01	A	creation