Information security policy for suppliers

Introduction

Kärchers business depends on its partner-network and the secure sharing of information. The weakest link in the value chain can compromise the security-status of Kärcher or his end customers. Thus, each partner shall contribute to the shared responsibility for information security and implement technical and organizational security measures. This policy provides mandatory principles for the secure transfer, storage and management of Kärcher's digital or analog information.

Scope

This policy applies to all suppliers of the Kärcher Group. They are responsible within their role and tasks for complying with this policy and its requirements.

CORE PRINCIPLES OF INFORMATION SECURITY

(1) Be aware of restricted information
Kärcher differentiates between public and restricted information. Restricted means that only a defined group of people and/or roles may have access to the information. The supplier will be informed by Kärcher when restricted information shall be involved. However, the supplier shall assess information for their criticality on its own and treat them with care.

(2) Provide or accept secure ways for communication
When Kärcher needs to share restricted information with his supplier the particular information shall not be transferred via open unprotected communication lines like open emails or chat platforms. The supplier shall use Kärcher's toolset for secure information transfer (e.g. SAP Ariba, file exchange platform, https downloads or encrypted ZIP-files etc.). Alternatively, the supplier can provide his own communication tools if he can show that they ensure the confidentiality, integrity, availability and authenticity of informationen.

(3) Protect credentials for secure communication lines
Setting up a secure communication may require the exchange and storage of credentials (e.g. encryption keys, certificates, tokens etc.). The supplier shall protect such credentials with the highest care and enforce strict access control (see principle 4) for them. The relevant credentials must be deleted if they are not needed anymore.

(4) Protect restricted information and credentials at rest
For restricted information or credentials a strict access control must be enforced. Access control means that only a defined group of people or roles with specific permissions can read, use or modify these information. Access and access attempts shall be logged and traced through technical or organisational measures.

(5) Validate if security measures are effective
Implemented information security measures shall have an impact. Thus, the supplier ensures to validate their effectiveness.

(6) Inform Kärcher if a violation of these principles occurs
If the supplier becomes aware of a violation of these principles he must inform Kärcher without delay and cooperate with Kärcher regarding the impact assessment and treatment of this violation.

By confirming, we declare to apply this policy bindingly and implement this policy.