INFORMATION SECURITY POLICY FOR SUPPLIERS

KROSCHU KROMBERG & SCHUBERT

Content

Version	Date	Creator	Reviser	Release
00	21.10.2019	M. Winkler	T.Träder B. Hoffmann-Genser	21.10.2019
01	01.09.2022		M. Winkler	Checked for actuality
02	21.08.2025	V.Sergl	M.Winkler	

0. Foreword

The core business of Kromberg & Schubert (hereinafter referred to as Kroschu) is the development and production of complex wiring systems for the automotive industry at over 40 international locations. In addition to the production of special cables, the company's range of services today also includes plastics technology.

The committed interaction of development, production and quality management has top priority at Kromberg & Schubert in order to implement every solution perfectly.

Information is an essential asset for our company, our customers and our business partners and must therefore be adequately protected. Work and business processes are increasingly based on IT-supported solutions and connections.

The security and reliability of information and communication technology is therefore becoming increasingly important.

Kroschu is certified according to TISAX. In order to ensure compliance with the standard also in cooperation with suppliers and their subcontractors, the following information security requirements are to be observed as a minimum requirement for suppliers.

With this guideline, basic regulations for ensuring information security within the business relationship between Kroschu and suppliers are agreed upon. It serves to maintain the confidentiality, integrity and availability of Kroschu's information and systems.

1. Scope

The following areas of application are explicitly affected by the regulations of this guideline:

- Suppliers from the services sector who exchange and/or process data with Kroschu such as development service providers, consulting service providers, IT service providers for the processing of data

- Suppliers who have been contracted for the outsourcing of IT and information services or who access machines, systems and IT equipment located at Kroschu by means of remote maintenance and data lines, such as data storage by means of a cloud solution, remote maintenance of production systems, use of VR glasses.

2. Use of Kroschu IT systems

The use of Kroschu's IT devices and data by employees of external suppliers requires the express consent of the responsible department. This department has the right to prevent the use at any time (e.g. in case of suspected misuse). Kroschu may prohibit the bringing of portable IT systems, cell phones, cameras, etc. or restrict them to certain areas.

The circle of authorized employees of the external supplier must be defined by name and must be kept as narrow as possible according to the "need-to-know" principle. Employees of the external supplier who gain access to Kroschu IT systems must be obligated in writing to comply with the applicable relevant laws, regulations, internal rules and the non-disclosure agreement.

This applies accordingly to employees of subcontractors.

The disclosure of information to third parties is expressly prohibited unless Kroschu expressly consents to this process.

Performing IT support:

The work performed must be documented (scope, result, time). Work concerning the operating system or system-related software may only be carried out by the external supplier in accordance with instructions.

3. Handling of Kroschu internal data

When Kroschu internal data is transferred and/or processed by the external supplier, the following points must be strictly observed:

- Kroschu internal data must be protected against any misuse and data theft, e.g. by malware. If malware is suspected, the affected devices and data carriers may no longer be used.

- The data provided by Kroschu must be secured by backup backups.

- No data or information from other customers not belonging to Kroschu may be processed on the IT equipment provided by Kroschu.

- Kroschu's data shall be separated from other customer data of the external supplier according to the rules of client separation.

- Data carriers are to be secured against loss, destruction and confusion as well as against access by unauthorized persons. Data that is no longer required must be disposed of securely.

- Care must be taken to ensure that all conversations involving sensitive information, including telephone conversations, cannot be overheard by unauthorized persons.

- When transporting data carriers or devices containing data carriers, care must be taken to ensure that all necessary and appropriate precautions are taken (e.g., encryption) to protect information from being viewed, modified or deleted by unauthorized persons.

4. Use of Kroschu IT equipment and software

The equipment provided must be handled properly and protected from loss or unauthorized modification. Devices provided by Kroschu (e.g. laptops, cell phones) may only be removed from the respective premises with Kroschu's permission. Any loss of the devices must be reported immediately.

An email account may be set up within the Kroschu domain to facilitate order-related communication. The use of the internal e-mail service is permitted exclusively in connection with the order. Likewise, the forwarding of e-mails to external recipients is only permitted in connection with the order. Automatic forwarding of e-mails to external mailboxes is expressly prohibited.

5. Information classification

Within the scope of information classification (with regard to confidentiality), the possible effects (potential damages) for Kroschu are evaluated in the event that information is unintentionally disclosed to an unauthorized group of recipients.

The Supplier shall ensure by means of an appropriate rights concept that the information transmitted by Kroschu is protected. Kroschu reserves the right to request the appropriate concepts from the supplier and to check for compliance.

6. Data protection for external operation of IT infrastructure

If the IT infrastructure (e.g. networks, servers) and/or cloud solutions are operated externally, it must be ensured that:

- external administrators do not have access to the content of the data and
- the requirements for encryption in accordance with VDA ISA Control 10.1 (Cryptography)

are complied with (reference to ISO 27002:Control 10.1.1)

7. Reporting of information security-relevant processes

The Supplier undertakes to establish and maintain a procedure to ensure traceability in the event of information security events according to criticality levels.

Occurring information security relevant events are to be reported to Kroschu immediately at the following email address:

informationsecurity@ksab.kroschu.com