Security Guide

A – General Terms

External providers of IT services and IT-related services

Scope of application:	thyssenkrupp Automotive Body Solutions GmbH
Process owner:	ISO (Information Security Officer)
Created by:	Michael Müller / ISO
Version:	13/03/2024 (V1.0)

thyssenkrupp

Revision history:

Version	Change	Page	Date	modified by
1.0	First edition	1 - 8	13/03/2024	Michael Müller

Contents

1 Description

This security guideline is mandatory for all external IT service providers operating for a tkAB affiliate. These requirements are to be understood as a minimum requirement for the provision of services within tkAB IT.

If these minimum requirements cannot be met by the external provider of IT services, tkAB will not cooperate with this external provider of IT services.

1.1 Responsibilities

The external provider of IT services shall ensure that the provision of services follows the provisions of this guideline.

The contracted external provider of IT services must at all times ensure that its actions and those of its employees do not affect the availability, integrity or confidentiality of the IT systems of tkAB companies.

Copyright and patent law provisions as well as licensing agreements must be observed.

The access data provided may not be passed on to third parties.

1.2 Access to buildings and production facilities

The external provider of IT services must inform its employees that they must register with their contact person in a company affiliated to tkAB. The external provider of IT services will also point out to its employees that a visitor's badge will be handed over to them and that they will have to wear this badge in a clearly visible manner.

1.3 Use of IT systems and IT infrastructures

1.3.1 Use basis and rights

Hardware and software used within the infrastructure shall not compromise the security and performance of the infrastructure. Therefore, the external provider of IT services may only use products and devices approved by the central IT department.

1.3.2 Use of Internet and communication infrastructure

All accesses can be logged by the central IT department for diagnostic and security purposes.

The external provider of IT services shall inform its employees that, where access to internet resources or email accounts has been provided, the use of internet and email is permitted exclusively for business purposes.

OT systems in the production environment must not be allowed access to the Internet, even during maintenance.

Only tkAB own remote support solutions may be used.

The use of "cloud solutions" always requires separate approval by the Information Security Management Department of tkAB.

1.3.3 Hardware and software management

The external provider of IT services may only provide, install, or set up IT components if they have been checked and approved by IT before they are connected to the tkAB network (LAN/WLAN/OT/IT).

To release the hardware or software, a written documentation must be available. This documentation shall include at least the following:

- Configuring network components and functions
- Function of the software interfaces
- Required permissions
- Access data

The IT components used by the external IT service providers shall support the specified IT security solutions. The external provider of IT services must request this from the central IT department.

Modifications to the hardware or software of a terminal (such as installation of hard disks, memory expansion, WLAN cards) must be coordinated with the ITM division (tkAB).

IT components shall be destroyed exclusively in coordination with the ITM division (tkAB).

When using external storage media (e.g. USB stick, external hard drive, USB devices), care must be taken that only media approved by tkAB ITM division (see guideline "Handling mobile IT equipment") may be used.

1.3.4 Network

The company's own network infrastructure is operated exclusively by the authorized agencies. Any modification not authorized by IT is prohibited.

Unrestricted network access is only permitted for own or shared terminals administered by the IT.

The use and operation of WLAN components may only be carried out after consultation with IT.

1.4 Minimum security requirements

The external IT service provider shall ensure that the hardware it uses and provides has the latest version of the anti-virus system used by tkAB with an updated virus signature database installed.

The latest updates for the operating system and software used must be installed and checked for updates at least once every quarter.

All vendor systems used for creation and configuration must also have up-to-date virus protection and all security-related system updates and patches installed.

Furthermore, the external provider of IT services must ensure that its employees have received training on IT security. If processing of personal data is necessary for the provision of the service or if access to personal data cannot be excluded, the external provider of IT services must ensure that its employees are trained and obligated in accordance with § 5 BDSG.

Transfer of data from tkAB to third parties is not permitted unless there is a separate written authorization.

All email traffic between tkAB and the external provider of IT services shall be treated confidentially.

Storing tkAB data in unencrypted form on mobile data carriers (e.g. USB sticks) is prohibited. Exceptions require separate approval from IT Security.

All data generated for tkAB as part of the processing of the order is owned by tkAB.

Upon completion of the work, any data provided shall be returned to the commissioning company, and no copies, extracts or other complete or partial reproductions shall be retained.

1.5 Dealing with technical faults

The external provider of IT services must inform its employees that if disruptions occur during operation or an IT security incident becomes known, the respective tkAB contact person must be informed immediately.

1.6 Regulation provided user accounts

The access authorizations granted and the use of personal or other business data serve exclusively for the fulfillment of the object of the contract.

The external provider of IT services must ensure that any employed person can register with the user ID requested for him. The user ID and password may not be passed on to third parties.

Upon termination of the service contract, the external provider of IT services must arrange for all identification documents and data carriers handed over by its employees to be returned to tkAB. User accounts of employees of the external IT service provider that are no longer required must be reported to IT immediately for deactivation.

1.7 Remote maintenance / remote access

Local network access is always preferable to remote access. Remote access is only possible after consultation with IT and the regulations listed below.

- Remote access for remote maintenance is only provided via tkAB own systems; any other options are not supported.
- The external provider of IT services must ensure that its employee's own network does not allow uncontrolled third-party access to the tkAB network.
- Only connections or software released by tkAB IT may be used for remote maintenance.
- No IT system shall establish a VPN connection independently.
- The external provider of IT services shall be obligated to check the remote access functionality at least once every quarter during the term of the contract.

1.8 Rendering of services

1.8.1 Software

Ensure that the source code is accessible for developed software products.

The current version of the "tkAB coding guideline for software development" must be observed in software development.

For all development work in SAP systems, the current development guideline for SAP developments of the tkAB in its current version must be applied.

The following activities are generally prohibited for the external IT service provider:

- Modifications of SAP standard objects

- Adjustments of authorization roles with external IT services
- Changes to system settings (client/system openings)
- Schedule periodic batch jobs and event-driven batch jobs
- Changes to SICF service settings
- Changes to the Switch Framework

Before being imported into productive SAP systems, complete documentation of all developments carried out must be available.

The basis for this is the valid procedure model for software changes according to the V-Model for compliance with IT governance for changes to productive systems of the tkAB.

1.8.2 Hardware

The hardware provided by the external IT service provider must be designed in accordance with the internal guidelines in consultation with the contact person at tkAB.

This includes the hardware for possible remote support.

2 Abbreviations

ITM	IT Management
tkAB	thyssenkrupp Automotive Body Solutions GmbH