

4 – Specific directives

Document Source ID

[Source Doc-ID]

Document Title

Information security guidelines for suppliers of KIRCHHOFF Automotive



Confidentiality

Public

Page 1/13

Information security guidelines for suppliers of KIRCHHOFF Automotive

Version: 9.0
Document owner Wieczorek, Waldemar
First approval: 2022-08-29, Wieczorek, Waldemar
Second approval: 2022-08-29, van Buuren, Danny
Language EN

Approved Version.

Objectives of the document

Providing guidelines for the handling of information and the use of information technology for suppliers, contractors and service providers (contractors) of KIRCHHOFF Automotive.

4 – Specific directives
Document Source ID [Source Doc-ID]
Document Title Information security guidelines for suppliers of KIRCHHOFF Automotive



Confidentiality Public	Page 2/13
---------------------------	-----------

Content

- 1 Introduction and scope 3**
 - 1.1 Preface 3
 - 1.2 Area of application 3
- 2 Protection of confidentiality of information/company secrets 3**
- 3 Forms of cooperation 4**
- 4 Requirements for contractors to maintain information security 6**
 - 4.1 Fundamentals 6
 - 4.2 Measures to implement information security depending on the form of cooperation 7
- 5 Information duties of the contractor 13**
- 6 Assessments / audits regarding the implementation of security measures 13**
- 7 Requiements for personal data processing on behalf 13**

4 – Specific directives			
Document Source ID [Source Doc-ID]			
Document Title Information security guidelines for suppliers of KIRCHHOFF Automotive		Confidentiality Public	Page 3/13

1 Introduction and scope

1.1 Preface

This guideline defines rules for the handling of information and the use of information technology that apply to suppliers, contractors and service providers (contractor) of KIRCHHOFF Automotive. The purpose of this guideline is to protect the confidentiality, integrity and availability of information as well as the rights and interests of KIRCHHOFF Automotive and all natural and legal persons who enter into a business relationship with KIRCHHOFF Automotive.

1.2 Area of application

This guideline is addressed to the management of the contractor, their employees and their vicarious agents.

2 Protection of confidentiality of information/company secrets

KIRCHHOFF Automotive works exclusively with contractors who have undertaken to maintain the confidentiality of information and business secrets within the framework of a confidentiality obligation or a non-disclosure agreement. In individual cases where the information provided is subject to an increased need for security, special measures may also be required of contractors in order to take account of the increased need for security. For example, the contractor may be prohibited from passing on, processing or storing information transmitted to third parties without the consent of KIRCHHOFF Automotive. Consent may be subject to compliance with the following safety requirements by the contractor or its subcontractors.

- (1) The contractor and his subcontractors are obliged to use the access rights granted by KIRCHHOFF Automotive (IT systems, services, data and applications) exclusively within the scope of their contractual obligations.
- (2) All information obtained through the order which is not publicly known as well as copies, records and work results created as a result of the order shall be the property of KIRCHHOFF Automotive and shall be returned to KIRCHHOFF Automotive after completion of the order.
- (3) The contractor and its subcontractors shall be obliged to keep confidential all information about the employer which has come to their knowledge in connection with the performance of the contract, to treat their business and operational matters and all work results confidentially and to protect them appropriately against unauthorised and non-contractual use, duplication or disclosure. The obligations apply beyond the termination of the contractual relationship. The contractor shall not be permitted to display, use for its own purposes or to make copies or records of any kind whatsoever of business or operational information not made public of any kind about KIRCHHOFF Automotive and/or its customers, suppliers or employees, unless this is necessary for the fulfilment of the order. Such information, copies, records or work results may not be passed on to third parties or brought to the knowledge of third parties.
- (4) Confidential information shall be disclosed only to subcontractors for which the contracting authority has given its consent and who have been required to comply with these security guidelines.
- (5) The contractor shall only employ personnel who are obliged to maintain data secrecy and information security. The obligations shall continue to exist even after termination of the activity.

3 Forms of cooperation

The use of external partners is primarily characterized by the fact that external persons are contracted to support work or business processes as well as the operation of applications and systems of the company.

There are many motivations to give external companies access to company data or company systems. Some companies need access for maintenance, service or test purposes, while others need to "operate" systems on behalf of the company. Complete services can also be outsourced to external partners, e.g. in the context of outsourcing or cloud computing.

In principle, any third-party access to KIRCHHOFF Automotive company data or the outsourced processing of data also entails a potential risk of misuse. For example, there is a risk that the access rights associated with third-party access may be used to explore the corporate network environment and access systems other than those explicitly released, or that information may be obtained from application systems that are not directly related to the company's mission.

Information that is processed or accessed are essential assets of KIRCHHOFF Automotive. The information security management system of KIRCHHOFF Automotive provides security measures to guarantee a basic protection for data, information and the underlying infrastructure. In order to achieve consistent basic protection, it is also necessary to apply the security standards within the framework of cooperation with external contractors. Depending on the type of cooperation, different requirements may arise for the security measures to be implemented. In principle, the defined security regulations apply to all internal and external employees.

Various forms of cooperation are possible in the area of cooperation with external partners. Different types of cooperation have been defined for the application of the KIRCHHOFF Automotive security targets.

Forms of cooperation Type	Description of cooperation with the contractor
Processing of non-personal data	
Type 1: External data processing	Data of KIRCHHOFF Automotive are kept on the systems of the contractor. The contractor, for example, receives the data of KIRCHHOFF Automotive within the framework of a design, development or construction contract or, for example, acts as a software developer for KIRCHHOFF Automotive. He processes the data independently on his own systems. The contractor receives the data from KIRCHHOFF Automotive via data carriers (USB media, tapes, etc.), e-mail or in another way in the context of an exchange of information (VDA / Odette communication, file transfer, download etc.).
Type 2: Data processing on systems of the contractor (excluded is the processing of personal related data on behalf of KIRCHHOFF Automotive)	The contractor undertakes the processing of non personal data / information on its own hardware and system software on behalf of KIRCHHOFF Automotive. For example, the contractor provides the operating systems, application systems and / or communication components. KIRCHHOFF Automotive is responsible for the data, the processed data is protected information / data but not personal related data. In addition to the contractor's connection based on routers / firewalls, ISDN / modem / communication servers, Internet etc., the contractor's direct involvement in the KIRCHHOFF Automotive IT infrastructures is also an option, e.g. cloud computing, SaaS etc.

4 – Specific directives

Document Source ID

[Source Doc-ID]

Document Title

Information security guidelines for suppliers of KIRCHHOFF Automotive

Confidentiality

Public

Page 5/13

Forms of cooperation Type	Description of cooperation with the contractor
Type 3: On-site-access	<p>The contractor accesses data at the KIRCHHOFF Automotive site and assumes the function of second-level support for the end user (advice, troubleshooting).</p> <p>As the operator, the contractor assumes responsibility for the operation of networks, systems and applications. As a software developer, the contractor has access to the IT infrastructure. The contractor is in case of on-site access in most cases directly integrated into the IT infrastructures of the KIRCHHOFF Automotive. No personal data or sensitive information will be processed on the contractor's systems.</p>
Type 4: Remote access or direct connection	<p>For remote access, there are two cases:</p> <ol style="list-style-type: none"> 1. The contractor has remote access to the KIRCHHOFF Automotive systems and applications via a network connection. Application examples: <ul style="list-style-type: none"> – The contractor is integrated directly into the work process as a client in a client / server application of KIRCHHOFF Automotive. – The contractor is a participant in a WEB conference, an online meeting, etc. – The contractor participates in the various forms of office communication. – The contractor performs remote maintenance on IT systems or systems of KIRCHHOFF Automotive or other network-integrated systems. 2. There are remote accesses by subcontractors, teleworkers, etc. to systems and applications at the contractor. The connection is based on router / firewall, Internet or VPN connections or ISDN / modem / communication server. No personal data or sensitive information will be processed on the Contractor's systems.
Type 5: System provision by KIRCHHOFF Automotive	<p>KIRCHHOFF Automotive provides the contractor with a system for use with which the contractor can be integrated into the KIRCHHOFF Automotive infrastructure. The security configurations and standards are defined by KIRCHHOFF Automotive.</p> <p>Example: Employees of the contractor work with systems provided by KIRCHHOFF Automotive on the premises of KIRCHHOFF Automotive or receive equipment for use.</p>
Type 6: Physical objects / information	<p>Physically protectable objects such as folders, concepts, contracts, samples, prototypes, components, tools, devices, etc. as well as accompanying information and data are processed, created or stored by the contractor, which have been classified as "confidential" or "secret" by KIRCHHOFF Automotive</p>

4 – Specific directives
Document Source ID [Source Doc-ID]
Document Title Information security guidelines for suppliers of KIRCHHOFF Automotive

Confidentiality Public	Page 6/13
---------------------------	-----------

Forms of cooperation	Description of cooperation with the contractor
Type	
Processing of personal data	
Type 7: Data processing of personal data on behalf of KIRCHHOFF Automotive	<p>The contractor processes personal data on behalf of KIRCHHOFF Automotive.</p> <ul style="list-style-type: none"> – The contractor undertakes information processing on its own hardware and system software, for example, on behalf of KIRCHHOFF Automotive. For example, the contractor provides the operating systems, application systems and / or communication components. KIRCHHOFF Automotive is responsible for the data, whereby the processing of the data is personal data. In addition to the contractor's connection based on routers / firewalls, ISDN / modem / communication servers, Internet etc., the contractor's direct involvement in the KIRCHHOFF Automotive IT infrastructures is also an option. Likewise, different types of cloud computing services can fall into this category. – The contractor accesses systems of the KIRCHHOFF Automotive t. – The data of KIRCHHOFF Automotive are kept on the systems of the contractor. – KIRCHHOFF Automotive transmits data to the contractor, who processes the data on his systems.

4 Requirements for contractors to maintain information security

4.1 Fundamentals

The contractor is requested but not obliged to implement an information security management system in accordance with the requirements of ISO 27001/27002. Furthermore, it is expected that all suppliers will comply with the legal data protection requirements.

Depending on the form of the cooperation, there are different focal points for the requirements of the security measures to be implemented. If personal data is processed, special attention is also paid to compliance with the legal data privacy regulations (e.g. appointment of a data privacy officer, if required by law; instruction of the employees in the handling of personal data etc.)

The form of cooperation may change in the course of the business relationship. In this context, the security measures to be implemented are also changing. The minimum requirements for the contractor's information security management system are set out below.

4.2 Measures to implement information security depending on the form of cooperation

Technical-organisational safety requirements depending on the form of cooperation			Forms of cooperation						
Nr	Reference ISO 27001	Technical-organizational measure	1. External data processing	2: Data processing on systems of the contractor (no personal related data)	3: On-site access	4. Remote access or direct coupling	5. System provision by the KIRCHHOFF Automotiv	6. Physical objects / information	7. personal data processing on behalf
01	A.05 A.06 A.07 A.08	<p>Organisation of Information Security</p> <p>Definition of guidelines, processes and responsibilities with which information security can be implemented and controlled.</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> Set up Information Security Policies User guidelines for the handling of devices and the behaviour when using information technology Processes for managing data media Definition of roles and responsibilities Obligation of the employees to maintain secrecy and Protection of data privacy. Regular training courses and awareness measures, including evaluation (e.g. via Employee Security Index) 	X	X	X	X		X	X
02	A.09	<p>Access control</p> <p>Implement measures to ensure that those authorised to use data processing procedures have access only to personal data subject to their right of access or to sensitive information and data.</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> Creation of an authorization concept Implementation of access restrictions Avoidance of the concentration of functions and establishment of a separation of functions Converting a Process for Assigning Authorizations Regular checking of authorizations Logging of authorization assignment and data access 	X	X	X	X			X
03	A.10	<p>Cryptography</p> <p>Use of encryption techniques to ensure the proper and effective protection of the confidentiality, authenticity or integrity of personal data or sensitive information.</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> Encryption of USB media and hard disks of PCs, Laptops, smartphones 	X	X					X

4 – Specific directives

Document Source ID [Source Doc-ID]
Document Title Information security guidelines for suppliers of KIRCHHOFF Automotive

Confidentiality Public	Page 8/13
---------------------------	-----------

Technical-organisational safety requirements depending on the form of cooperation			Forms of cooperation						
Nr	Reference ISO 27001	Technical-organizational measure	1. External data processing	2: Data processing on systems of the contractor (no personal related data)	3. On-site access	4. Remote access or direct coupling	5. System provision by the KIRCHHOFF Automotiv	6. Physical objects / information	7. personal data processing on behalf
		<ul style="list-style-type: none"> Encryption of files, data in storage systems Secure storage of data on mobile storage Wide area connections 							
04	A.11	<p>Protection of buildings</p> <p>Preventing unauthorized physical access to, damage to, or compromise of the organization's information and information processing facilities.</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> Defining Security Areas Realisation of access protection Determination of persons with access rights Administration of personal access authorizations Rules for accompanying visitors and external personnel Monitoring of rooms outside closing times Access logging 	X	X				X	X
05	A.11	<p>Protection of equipment / information values</p> <p>Prevent loss, damage, theft or deterioration of assets and interruptions to the organisation's operations.</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> Process for the safe extinguishing, disposal and destruction of operating resources Safe placement of operating resources Protection against overvoltage, power failure, water and fire Protection against theft Regular maintenance 	X	X				X	X
06	A.12	<p>Operating procedures and responsibilities</p> <p>Ensure the proper and safe operation of information processing systems and procedures.</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> Hardening of backend systems Separate processing of production and test data Multi-client capability Distribution of tasks and separation of functions that are not compatible with each other. Documentation of operating procedures. 	X	X					X

4 – Specific directives

Document Source ID

[Source Doc-ID]

Document Title

Information security guidelines for suppliers of KIRCHHOFF Automotive

Confidentiality

Public

Page 9/13

Technical-organisational safety requirements depending on the form of cooperation			Forms of cooperation						
Nr	Reference	Technical-organizational measure	1. External data processing	2: Data processing on systems of the contractor (no personal related data)	3. On-site access	4. Remote access or direct coupling	5. System provision by the KIRCHHOFF Automotiv	6. Physical objects / information	7. personal data processing on behalf
07	A.12	<p>Data backups:</p> <p>Measures to ensure that personal data or sensitive information and data are protected against accidental destruction or loss.</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> • Creation of a data protection concept • Carrying out regular data backups • Separate storage of data backup media 	X	X					X
08	A.12	<p>Malware protection and patch management</p> <p>Prevent technical vulnerabilities from being exploited by using up-to-date anti-virus software and implementing patch management. Regular checks to detect vulnerabilities.</p>	X	X	X	X			X
09	A.12	<p>Logging and monitoring</p> <p>Measures to ensure that it can be subsequently verified and established whether and by whom (personal) data have been entered, modified or removed in IT systems. (All system activities are logged; the logs are kept by the contractor for at least 3 years).</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> • Logging of authorization assignment and data access • Checking user authorizations • Logging of activities and regular evaluation of user and system activities 	X	X		X			X
10	A.13	<p>Network Security Management</p> <p>Adequate protection of the network must be implemented so that the information and infrastructure components are protected.</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> • Implementation of network management • User authentication for external connections and connections between individual systems • Protection of diagnostic and configuration ports • Security gateways at the transfer points / network boundaries • Insulation of sensitive systems 	X	X		X			X

4 – Specific directives

Document Source ID

[Source Doc-ID]

Document Title

Information security guidelines for suppliers of KIRCHHOFF Automotive

Confidentiality

Public

Page 10/13

Technical-organisational safety requirements depending on the form of cooperation			Forms of cooperation						
Nr	Reference	Technical-organizational measure	1. External data processing	2: Data processing on systems of the contractor (no personal related data)	3. On-site access	4. Remote access or direct coupling	5. System provision by the KIRCHHOFF Automotiv	6. Physical objects / information	7. personal data processing on behalf
11	A.13	<p>Transmission of information</p> <p>measures to ensure that personal data or sensitive information and data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data carriers and that it is possible to verify and establish the points to which personal data or sensitive information and data are to be transmitted by means of data transmission. (Description of the equipment and transmission protocols used, e.g. identification and authentication, state-of-the-art encryption, automatic recall, etc.)</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> Secure transport and dispatch of data / documents depending on data protection requirements Logging of data transmissions Description of interfaces between systems and external data connections 	X	X					X
12	A.13	<p>Segmentation of networks</p> <p>Groups of information services, clients, users and information systems should be kept separate in networks.</p>	X	X		X			X
13	A.14	<p>Acquisition, development and maintenance of systems</p> <p>Measures to ensure that information security is an integral part of the life cycle of information systems.</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> Establishment of security enforcing rules and requirements for the use of new information systems and for the extension of existing information systems. Establishing rules for the development and adaptation of software and systems Guidelines for safe system development Monitoring of outsourced system development activities Protection of test data 	X	X	X	X			X

4 – Specific directives

Document Source ID

[Source Doc-ID]

Document Title

Information security guidelines for suppliers of KIRCHHOFF Automotive

Confidentiality

Public

Page 11/13

Technical-organisational safety requirements depending on the form of cooperation			Forms of cooperation						
Nr	Reference ISO 27001	Technical-organizational measure	1. External data processing	2: Data processing on systems of the contractor (no personal related data)	3. On-site access	4. Remote access or direct coupling	5. System provision by the KIRCHHOFF Automotiv	6. Physical objects / information	7. personal data processing on behalf
14	A.15	<p>Supplier relationships</p> <p>Information security measures to reduce risks associated with suppliers' access to the company's assets should be agreed and documented with subcontractors.</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> Written addressing of security issues in contracts with subcontractors Security verification of subcontractors 	X	X	X	X	X	X	X
15	A.16	<p>Management of Information Security Incidents</p> <p>Consistent and effective measures must be implemented for the management of information security incidents (theft, system failure, data loss, etc.).</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> Immediate information to KIRCHHOFF Automotive Logging of security incidents 	X	X	X	X	X	X	X
16	A.17	<p>Information Security Aspects of Business Continuity Management / Emergency Management</p> <p>The maintenance of system availability in difficult situations such as crises or damage must be maintained. An emergency management system must ensure this. Information security requirements should be defined in the business continuity and disaster recovery plans.</p> <p><u>This should include:</u></p> <ul style="list-style-type: none"> Creation of redundancies Risk assessment and planning of measures to safeguard business operations Establish contingency plans Regular tests regarding the effectiveness of emergency measures Early information of KIRCHHOFF Automotiv in case of emergencies 		X					X
17	A.18	<p>Compliance with legal and contractual requirements</p> <p>Implementation of measures to avoid breaches of legal, official or contractual obligations as well as any security requirements.</p> <p><u>This should include:</u></p>	X	X	X	X	X	X	X

4 – Specific directives

Document Source ID

[Source Doc-ID]

Document Title


Information security guidelines for suppliers of KIRCHHOFF Automotive

Confidentiality

Public

Page 12/13

Technical-organisational safety requirements depending on the form of cooperation			Forms of cooperation						
Nr	Reference ISO 27001	Technical-organizational measure	1. External data processing	2: Data processing on systems of the contractor (no personal related data)	3. On-site access	4. Remote access or direct coupling	5. System provision by the KIRCHHOFF Automotiv	6. Physical objeccts / information	7. personal data processing on behalf
		<ul style="list-style-type: none"> Confidentiality obligations with employees and subcontractors Ensuring compliance with legal obligations within the framework of cooperation Return of all data, resources and information to KIRCHHOFF Automotive at the end of the contract 							
18	A.18	<p>Data privacy requirements and data privacy management</p> <p>Privacy and the protection of personal data should be ensured in accordance with the requirements of the relevant laws, regulations and, where applicable, contractual provisions.</p> <p>If the supplier processes personal data on behalf of KIRCHHOFF, the supplier has to fulfil the following requirements:</p> <ul style="list-style-type: none"> Acceptation of a data-processing agreement Establishment of a data protection emergency management system to ensure an immediate reporting of data protection incidents to KIRCHHOFF Automotive Documenting the implemented technical and organisational measurements to ensure the security of personal data 							X
19	A.18	<p>Information security audits</p> <p>It must be regularly checked whether the information processing is carried out according to the defined security measures. For this purpose, the contractor shall carry out regular checks. The contractor grants KIRCHHOFF Automotive the right to carry out regular checks at the contractor's premises.</p>	X	X	X	X	X	X	X

4 – Specific directives			
Document Source ID [Source Doc-ID]			
Document Title Information security guidelines for suppliers of KIRCHHOFF Automotive		Confidentiality Public	Page 13/13

5 Information duties of the contractor

The contractor must inform KIRCHHOFF Automotive without delay of any incidents of information security, serious disruptions to operations, suspected breaches of data protection or other irregularities in the processing of KIRCHHOFF Automotive’s data; in particular such incidents which make access by unauthorised persons possible.

If KIRCHHOFF Automotive’s data are endangered at the contractor’s by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the contractor shall inform KIRCHHOFF Automotive thereof without delay. The contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with KIRCHHOFF Automotive.

Notifications also should be sent to the central e-mail address: ISMS@kirchhoff-automotive.com

6 Assessments / audits regarding the implementation of security measures

KIRCHHOFF Automotive reserves the right to check the implementation of the safety requirements described in chapter 4.

The currently valid version of the TISAX/VDA questionnaire and/or an individual assessment is used for the review.

Alternatively, compliance with information security can also be proven by means of a TISAX assessment or security certification (e.g. ISO27001)

7 Requirements for personal data processing on behalf

In the case of the processing of personal data by the contractor on behalf of KIRCHHOFF Automotive, a contract must be concluded for the processing of data in accordance with **EU General Data Protection Regulation** (GDPR).

The contractor has to document the implementation of the technical and organisational measures (see 4.2), in particular with regard to the concrete performance of the contract, and to deliver them to KIRCHHOFF Automotive for review before starting the processing.