RONALGROUP

CORPORATE

SUPPLIER INFORMATION SECURITY GUIDELINE

RONAL GROUP: JULY 2023

Change log

Version	Date	Department	Change description
1	July 23	Information Security	Elaboration of the document

Confirmation & Signature

With this signature, you confirm your intention to comply with the requirements of the RONAL GROUP "**Supplier Information Security Guideline**" in this document and to take and implement appropriate as well as reasonable measures.

Date of approval	Company name	**Contact person: First & Last Name**	Role	Signature

Table of content

1 Scope

These instructions apply to all third parties who process sensitive information for RONAL AG, as well as for the entire RONAL GROUP (all associated subsidiaries) in accordance with the contractual agreements.

2 Purpose and definitions

This action guideline defines rules for information security to be followed by third parties when handling information and IT devices (e.g., PCs, workstations, laptops, smartphones or tablet PCs).

Third parties are defined as contractual partners who provide services to RONAL AG based on contractual relationships. Subsidiaries and brands of RONAL AG, as well as companies in which RONAL AG holds majority interests, are excluded from this definition.

3 Document structure and target group

This policy is intended for the management of the third parties, their employees, and their agents/associates. This document contains three chapters. The following table lists the document structure and the respective target group per chapter.

Chapter	Target group
4	All third parties
5.1	Third parties working in the RONAL infrastructure.
5.2	Third parties who have access to RONAL information outside the RONAL infrastructure.
5.3	Third parties who process RONAL information in connection with prototypes.

A third party can belong to several target groups at the same time, depending on the collaboration model.

4 General requirements for all third parties

The third parties undertake to ensure the implementation of common information security standards in accordance with the requirements of the VDA-ISA (see appendix, chapter 7.1.a) in its currently valid form in their company or organization.

Information security events (e.g., malfunctions occurring, violations of the information security rules and regulations) that affect data or systems of the customer must be reported immediately to the responsible office (see appendix, chapter 7.3.b).

Suspected vulnerabilities and weaknesses of the customer's IT systems must be reported immediately to the responsible entity (see appendix, chapter 7.3.b).

In the event of a suspected loss of confidential or secret information of the client, this must be reported immediately to the responsible entity (see appendix, chapter 7.3.b). General requirements for all third parties.

5 Additional requirements for third parties

Description of the additional requirements imposed on third parties working inside or outside the RONAL infrastructure and having access to RONAL information or processing RONAL information in connection with prototypes.

5.1 RONAL infrastructure (intern)

A third party operates in the RONAL infrastructure when:

- clients (physical or virtual terminals) are provided by RONAL or affiliated companies, or
- the connection is made via remote access solutions (such as Pulsecure) with access to the internal RONAL network, or
- the connection of the third party is made directly to the internal RONAL network.

This is regardless of whether the third party is located on the premises of RONAL or an affiliated company.

The following **requirements** apply to these third parties:

- Regulations of RONAL regarding the carriage of IT equipment not belonging to the client onto the company premises or into security areas must be observed.
- The equipment provided must be handled properly and protected against loss or unauthorized modification.
- The manufacturer's regulations for the protection of the equipment must be complied with.
- Equipment provided by the client (e.g., laptops, mobile phones) shall only be taken off the client's premises after approval has been granted.
- Service providers may only provide or initiate the provision or installation of hardware and software via the department of the client responsible for them.
- Regarding the use of the hardware and software provided, the regulations of RONAL shall apply (see appendix, chapter 7.3.c).
- Opening the IT device and performing changes to the hardware (e.g. installation/removal of hard disks, memory modules) as well as manual changes to the security settings (e.g. browser settings) is only permitted to the responsible departments (see Appendix, chapter 7.3).

- The use or subsequent modification of programs of the customer shall only be permitted if approved by the responsible departments (see appendix, chapter 7.3.b).
- No data from other customers not belonging to the corporation shall be processed on the IT equipment provided.
- The use of IT equipment or data of the customer by employees of the service provider requires the express consent of the customer. The client is authorized to prohibit access or use at any time (e.g., in case of misuse).
- Furthermore, the regulations, notes and information sheets on the RONAL website must be observed.

5.2 RONAL infrastructure (external)

Additional requirements for third parties who have access to RONAL information outside the RONAL infrastructure:

- Diese Dritten sind an die eigenen Regularien zur Informationssicherheit gebunden.
- The implementation of information security measures must be validated in accordance with TISAX®[1] for high protection requirements.

5.3 Prototypes

Additional requirements for third parties processing RONAL information in connection with prototypes:

- These third parties are tied to their own prototype protection regulations.
- The implementation of measures for prototype protection must be demonstrated in accordance with TISAX®[1] for high protection requirements in connection with prototype components.

6 Deviations and exceptions

Deviations from these action guidelines that lower the safety level are only permitted temporarily and after consultation with the responsible entities (see appendix, chapter 7.3.b) and the client.

[1] **T**rusted **I**nformation **S**ecurity **A**ssessment e**X**change, see www.tisax.org

7 Appendix

7.1 Applicable documents

a. Information Security Assessment of the German Association of the Automotive Industry (VDA) (download from the website of the VDA - www.vda.de/en)
b. Regulations, notes and information sheets on the RONAL website.

7.2 Validity

This information security regulation becomes effective at the time of publication. Updated contents of this regulation must be implemented within a transitional period of six months.

Next verification date: **October 31, 2023**

7.3 RONAL specific characteristics

a. RONAL Headquarter

   phone: +41 62 389 05 10
   mail: info@ronalgroup.com

b. Information security responsibility:
   infosec@ronalgroup.com

c. Each contractor is responsible for ensuring that information, programs, and IT equipment are only used and utilized properly for company purposes and within the scope of the respective task. Sending data with non-business content is not permitted. The use of the Internet for private purposes is only permitted within the framework of existing regulations within the company. The use of private software and data on IT devices provided by RONAL is prohibited.