RONALGROUP

CORPORATE

SUPPLIER INFORMATION SECURITY - CHECKLIST TISAX

RONAL GROUP: JULY 202

Change Log

Version	Date	Department	Description of change
1	October 21	Information Security	Revision of the document
2	January 23	SCM	Update of the document
3	June 23	SCM	Update of the document Deletion of chapter “3. Appraisal” 2b - adding SOC 2
4	July 23	EDA	Changing the format from Word to PDF with interactive cells

Confirmation & Signature

With this signature you confirm your intention to comply with the requirements of the RONAL GROUP document "supplier information security-checklist" and to take and implement appropriate and reasonable measures.

Date of approval	Name of company	Contact: First & last name	Role	Signature

1 Master Data (to be completed by supplier)

Supplier Name:	
DUNS No.:	
Supplier Number(s):	
Product range/range of services:	
Date of Survey:	
Author of the report:	

2 Information Security (to be completed by supplier)

	YES	NO
Does your company have a release according to TISAX?	☐	☐
If yes, which label?		
Expiration Date:		
Remarks:		

If the question <u>above</u> has been answered with a "YES", no further information is required.
Please proceed to sign the document and return it to your RONAL contact.
Additionally, please share your Scope ID in the ENX Portal with RONAL AG (P6HYRL).

If the question above has been answered with "NO" → Continue with the document and answer the questions please

	YES	NO
Does your company operate an information security management system according to a recognized standard (ISO27001, BSI IT Grundschutz, SOC 2)?	☐	☐
If yes, which standard?		
Issue Date:		
Scope of certificate:		

If the question above has been answered with "NO" → Continue with the document and answer the questions please

	YES	NO
Has your company appointed a responsible person (e.g. Information Security Officer) who takes care of the security of confidential/secret information and defines appropriate measures?	☐	☐
If yes, name?		
Direct reporting to (hierarchy level):		
Further remarks:		

In any case → Continue to answer all remaining questions please

	YES	NO
Does your company identify and classify information and are appropriate graded processing rules defined?	☐	☐
Rules defined?		
Further remarks:		

	YES	NO
Does your company use confidentiality or non-disclosure agreements for contractual purposes with subcontractors?	☐	☐
Explanation:		

	YES	NO
Does your company maintain an authorization concept for access to business premises and to electronic storage media (server, PC, ...)?	☐	☐
Explanation:		

	YES	NO
Does your company encrypt confidential information for data storage, during data exchange and on mobile devices?	☐	☐
Explanation:		

	YES	NO
Is your company protected from malware and unauthorized access?	☐	☐
Explanation:		

	YES	NO
Does your company perform regular data backups?	☐	☐
Explanation:		

	YES	NO
Has your company issued a policy, which defines in which cases and how the customer is to be informed in the event of security incidents?	☐	☐
Explanation:		

	YES	NO
Does your company ensure compliance with legal and contractual requirements?	☐	☐
Describe “how”:		

The following questions must only be answered by suppliers of production material (direct material suppliers) to RONAL:

	YES	NO
Does your service include the development of the products you are supplying to RONAL?	☐	☐
Do you manufacture own prototypes and/or do you receive prototype parts from RONAL (e.g. for testing)?	☐	☐
Are product development, manufacturing of prototypes and testing at the same location?	☐	☐
Explanation:		

Decision (to be completed by RONAL)

Approved (unconditionally) ☐

Conditionally approved ☐

Specify restrictions:
(e.g. restriction within or excluding certain countries/regions, program sourcing requires individual approval by IS Officer, exclusion from sourcing under certain conditions, …)

Rejected ☐

Explanation for rejection:

Approval / *Freigabe*	**Date** / *Datum*	**Name** / *Name*	**Signature** / *Unterschrift*
CISO			
Category Responsible			