**Supplier Information Security – Checklist
TISAX**

ronal Group

**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 documentDeletion of chapter “3. Appraisal”2b - adding SOC 2 |

**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: Click here to enter information

DUNS No.: Click here to enter information

Supplier Number(s): Click here to enter information

Product range/range of services: Click here to enter information

Date of survey: Click “button down” to enter date

Author of the report: Click here to enter information

# 2 **Information Security (to be completed by supplier)**

1. Does your company have a release according to TISAX? [ ]  Yes [ ]  No

*If Yes* *🡪 Which label?* Click here to enter information

Expiration Date: Click “button down” to enter date

Remarks: Click here to enter information

-------------------------------------------------------------------------------------------------------------------------

*If the question 2a 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).*

-------------------------------------------------------------------------------------------------------------------------

*Otherwise* *🡪 Continue with b*

1. Does your company operate an information security management system according to a recognized standard (ISO27001, BSI IT Grundschutz, SOC 2)? [ ]  Yes [ ]  No

*If Yes 🡪 Which standard?* Click here to enter information

Issue Date: Click “button down” to enter date

Scope of certificate: Click here to enter information

*If No* *🡪 Continue with c*

1. 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? [ ]  Yes [ ]  No

*If Yes* 🡪 Name: Click here to enter information

Direct reporting to (hierarchy level): Click here to enter information

Further remarks: Click here to enter information

 *In any case* *🡪 Continue with d*

1. Does your company identify and classify information and are appropriate graded processing rules defined? [ ]  Yes [ ] No

Further remarks: Click here to enter information

*In any case* *🡪 Continue with e*

1. Does your company use confidentiality or non-disclosure agreements for contractual purposes with subcontractors? [ ]  Yes [ ]  No

Explanation: Click here to enter information

*In any case* *🡪 Continue with f*

1. Does your company maintain an authorization concept for access to business premises and to electronic storage media (server, PC, ...)? [ ]  Yes [ ]  No

Explanation: Click here to enter information
*In any case* *🡪 Continue with g*

1. Does your company encrypt confidential information for data storage, during data exchange and on mobile devices? [ ]  Yes [ ]  No

Explanation: Click here to enter information
*In any case* *🡪 Continue with h*

1. Is your company protected from malware and unauthorized access?

 [ ]  Yes [ ]  No

Explanation: Click here to enter information
*In any case 🡪 Continue with i*

1. Does your company perform regular data backups? [ ]  Yes [ ]  No

Explanation: Click here to enter information
*In any case 🡪 Continue with j*

1. 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? [ ]  Yes [ ]  No

Explanation: Click here to enter information
*In any case 🡪 Continue with k*

1. Does your company ensure compliance with legal and contractual requirements?

 [ ]  Yes [ ]  No

Describe “how”: Click here to enter information

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

* Does your service include the development of the products you are supplying to RONAL? [ ]  Yes [ ]  No
* Do you manufacture own prototypes and/or do you receive prototype parts from RONAL

(e.g. for testing)? [ ]  Yes [ ]  No

* Are product development, manufacturing of prototypes and testing at the same location? [ ]  Yes [ ]  No

Explanation: Click here to enter information

# 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:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 CISO

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 Commodity Responsible