GRUPO ANTOLIN

INFORMATION SECURITY REQUISITES FOR GRUPO ANTOLIN SUPPLIERS

Document Code: I-P114-F

Review Number: 2

Review Date: March 04th 2021

Classification: Public

INDEX

I. SCOPE OF APPLICABILITY

The requisites described in this document apply to any person or company that has accepted its compliance through the signature of a contract, included an NDA contract, with **GRUPO ANTOLIN**.

This person or company signing the mentioned contract is referenced in the rest of the document as **Collaborator**.

Definitions and obligations available in the contract signed between **GRUPO ANTOLIN** and the **Collaborator** remain applicable and prevail over anything said in this document in the opposite.

II. APPLICABILITY OF REQUISITES

All **Collaborators** are obliged to ensure the implementation of Information Security standards within their organization or company as defined by the requirements of VDA-ISA in its current version, and according to the **Collaborator**'s classification and protection needs (see tables 1 and 2).

It is responsibility of the **Collaborator** to adapt the implementation of Information Security standards within their organization or company to the current VDA-ISA version. The adaptation must be done in the period of the next year after the publication of the VDA requisites.

In case of lack of compliance by the **Collaborator** regarding the adaptation to the current VDA-ISA version, it must be communicated to the point of contact in **GRUPO ANTOLIN** as soon as this situation is detected or, at least, just after the adaptation period has been exceeded.

Below is the table with the different classes of **Collaborators**. According to the class, the applicability of the VDA-ISA sections and chapters can be different.

For suppliers with access to, or handling, information owned by **GRUPO ANTOLIN** or under **GRUPO ANTOLIN**'s responsibility, in any way and format, the section Information Security is always applicable. If collaboration is limited to Suppliers' staff working at **GRUPO ANTOLIN** premises and following **GRUPO ANTOLIN** rules, normally only the chapters regarding Human Resources aspects are required and evaluated, but every case need to be analyzed according to the risks.

For Suppliers handling prototypes and/or personal data, the respective sections are applicable.

Classification must be supplied by the **Collaborator**'s point of contact in **GRUPO ANTOLIN**. In absence of this communication, **Collaborator** must ask to that point of contact about its classification and in consequence for the requisites to be met and to be demonstrated during the evaluation of compliance.

CLASS	DESCRIPTION OF COLLABORATOR'S RELATIONSHIP REGARDING INFORMATION ACCESS
1	Collaborator works at GRUPO ANTOLIN premises, without need to be escorted, but they are subject to GRUPO ANTOLIN security policies. Examples: a supplier service subcontracted and working at GRUPO ANTOLIN premises, like cleaning service, security service, etc.
2	Collaborator handles, or the opportunity to do it has been provided, information for GRUPO ANTOLIN located out of GRUPO ANTOLIN premises, independently of handle type (read, write, copies retention even encrypted with no read access, etc.). Example: a supplier access to DAXS to download files which are kept in their own premises.
3	Collaborator stores the original copies of information for GRUPO ANTOLIN. Examples: GRUPO ANTOLIN stores directly some files in a Cloud storage service provided by the Collaborator, or Collaborator stores by themselves the information associated to the contracted service (e.g. payroll externalized service).
4	Collaborator stores backup copies of information for GRUPO ANTOLIN. Example: GRUPO ANTOLIN backups the information directly in a Cloud service provided by the Collaborator.
5	Collaborator connects to GRUPO ANTOLIN systems remotely, accessing to internal GRUPO ANTOLIN network. Example: an engineering supplier perform the works in an internal GRUPO ANTOLIN system that is being accessed through a secure remote connection.
6	Collaborator connects remotely to GRUPO ANTOLIN systems with administration purposes. Example: an IT provider connects to GRUPO ANTOLIN network to solve a technical incident.
7	Collaborator manages prototype parts, components and/or vehicles out of GRUPO ANTOLIN premises.
8	Collaborator tests prototype vehicles out of GRUPO ANTOLIN premises.
9	Collaborator takes part in events and photo/film productions involving prototype parts, components and/or vehicles.
10	Collaborator, given the type of information accessed and the risks associated, is exempt from comply with more requisites beyond that defined in the NDA accepted, and therefore verification of compliance is no needed. Example: collaborator is out of GRUPO ANTOLIN premises, with no remote connections to GRUPO ANTOLIN network and information with collaborator never reaches confidential or higher levels.

Additionally to the class assigned to the **Collaborator**, information must be classified regarding its confidentiality or protection needs. Depending on the confidentiality class or impact, VDA-ISA requisites to be met are different.

Table 2 below shows the VDA-ISA requisites depending on information confidentiality class.

CONFIDENTIALITY CLASS FOR INFORMATION HANDLED	VDA ADDITIONAL REQUISITES
Internal information	Normal (must and should)
Confidential Information	High Protection needs
Highly Confidential Information	Very High Protection needs

Table 2. Confidentiality classes and protection needs according to VDA-ISA

Confidentiality classification must be supplied by the **Collaborator**'s point of contact in **GRUPO ANTOLIN**. In absence of this communication, **Collaborator** must ask to that point of contact about this classification.

Once collaboration ends between **GRUPO ANTOLIN** and the **Collaborator**'s organization or company, the **Collaborator** must ensure no data or parts belonging to **GRUPO ANTOLIN** or its customers remain in the **Collaborator**'s organization or company and that they are either returned to **GRUPO ANTOLIN** or, alternatively, and after the confirmation of **Collaborator**'s point of contact in **GRUPO ANTOLIN** for the specific collaboration, deleted or destroyed by any mean or mechanism normally regarded as secure.

III. VERIFICATION OF COMPLIANCE

Collaborator must be able to demonstrate the compliance with the requisites according to the class or classes assigned by **GRUPO ANTOLIN** and the protection needs of the information involved.

The demonstration of compliance can be supplied through one of the following ways:

(1) An adequate TISAX assessment has been approved and it is not expired or cancelled. The adequacy includes the labels equivalent to the **Collaborator** and confidentiality classes assigned to the relationship with **GRUPO ANTOLIN**.

TISAX labels are explained in the TISAX participant Handbook.

Collaborator grants access to **GRUPO ANTOLIN** to verify on TISAX portal the assessment validity.

TISAX assessment must be renewed adequately by the **Collaborator**, keeping the right for **GRUPO ANTOLIN** to verify the status in the TISAX portal.

(2) An adequate TISAX assessment is not available, but it is planned to be done along the next 9 months after the demonstration of compliance has been required from **GRUPO ANTOLIN**.

In this case, a contract with the auditor company for TISAX assessment must be provided by the **Collaborator** in the next 3 months after the demonstration of compliance has been required from **GRUPO ANTOLIN**.

GRUPO ANTOLIN will follow up this plan of assessment.

(3) There is not plan for TISAX assessment, so a specific evaluation for the **Collaborator** is required.

This evaluation is done through the binding answers to the VDA-ISA questionnaire or an equivalent one, and the **GRUPO ANTOLIN** specific questionnaires if applicable.

It is needed to show the documentation that demonstrate the truthfulness of the answers.

The evaluation can be done on-site or remotely, as agreed by **Collaborator** and **GRUPO ANTOLIN**.

In the case of prototypes involved in the relationship, GRUPO ANTOLIN has the right to demand an on-site the evaluation.

The costs associated to TISAX assessments and measures implemented to comply with the requisites are responsibility of the **Collaborator**.

In case of a specific audit (no TISAX assessment):

- If the audit is performed by an external body agreed between the **Collaborator** and **GRUPO ANTOLIN**, the costs associated to this audit are responsibility of the **Collaborator**.
- Only if **GRUPO ANTOLIN** has enough resources available, the specific assessment will be performed by **GRUPO ANTOLIN** staff.

The validity of a specific assessment is for 3 years.

In case of relevant changes (e.g. movement of Collaborator to a new building), or incidents with a significant potential impact on **GRUPO ANTOLIN**, the specific assessment can be required again for the aspects affected.

IV. ANNEXES

1. REPORTING BREACHES

Information security breaches affecting sensitive information (e.g. confidential information, business secrets) or systems owned by **GRUPO ANTOLIN** (e.g., vulnerabilities, weak points, violations of agreements) must be reported immediately, or as soon as possible, to e-mail infosec.notifications@grupoantolin.com or by phone to +34 947 47 78 00.

Alike, any suspected loss of confidential information or business secret must be reported to e-mail infosec.notifications@grupoantolin.com or by phone to +34 947 47 78 00.

2. FEEDBACK

For any kind of communication regarding information security: doubts, suggestions, events, complains or any other report, **Collaborator** can contact through infosec.ga@grupoantolin.com

3. ADDITIONAL DOCUMENTS

Documents available at the date of publication of this requisites guide.

(1) VDA-ISA questionnaire available at VDA web site.
https://www.vda.de/en/services/Publications/vda-isa-catalogue-version-5.0.html

(2) TISAX Participant Handbook and other interesting documents available at ENX web site.
https://portal.enx.com/en-US/TISAX/downloads

4. HIGH LEVEL WORKFLOW FOR THE COLLABORATOR APPROVAL PROCESS