SUMITOMO RIKO GROUP

SumiRiko AVS Germany GmbH

Security requirement information for suppliers

Dear Supplier,

Information security is a very important topic for us. For this reason, we would also like to create binding rules for the handling of information and data through our suppliers and ensure compliance with the aim to protect the confidentiality, availability and integrity of information and data, which we will highlight here.

<u>These rules for handling information and data are limited to the following:</u>

- Information and data identified as confidential and/or strictly confidential
- 2D and 3D data (drawings and data sets)
- Correspondence containing business secrets
  (e.g. prices, expertise, calculations, contracts, specifications, specification sheets and photos as well as information concerning markets, customers and products, etc.)
- Sources of supply for products, components and services
- Drafts and technical information
- Methods, practices, procedures, processes and formulas relating to the production, assembly, design or processing of the products covered by this agreement and all components or parts thereof
- Any products, including samples and prototypes, equipment and other physical forms of implementation

<u>The information below outlines our minimum requirements for accessing, transmitting and storing information and data:</u>

<u>Transmission:</u>

- For 2D and 3D data (drawings and data sets), secure (end-to-end encrypted) transmission must be guaranteed. In this regard, we would like to ask you to use the transmission options provided by us in the form of the two systems listed below as recommended tools: Seeburger Cloud (data transmission) and Jaggaer (RFQ tool).

<u>Access and security:</u>

- The "need-to-know principle" is to be followed at your company (e.g. only selected individuals who actually need access to the relevant information and data will receive it).
- Similarly, secure storage suitable for preventing access by unauthorized persons must be in place.
- Furthermore, unauthorized viewing of and access to sensitive areas (such as production and logistics) must be prevented.

Additional information concerning information security can be found in the latest versions of the international standards of the ISO/IEC 27000 series and in the VDA's minimum requirements for prototype protection.

SUMITOMO RIKO GROUP
SumiRiko AVS Germany GmbH

Should an information security incident and/or a potential risk, vulnerability or gap occur (such as theft, loss and manipulation of information and data, unauthorized entry, unauthorized access to confidential information and data, phishing and fraud etc.), a report must be immediately submitted to infosec@avs.sumiriko.com.

SumiRiko AVS reserves the right to conduct an information security audit at its suppliers.

Please contact us if you have any questions.

Our email address for the subject of information security: infosec@avs.sumiriko.com

Best regards,
SumiRiko AVS Germany GmbH

ppa. Matthias Wolthaus
Purchasing Director

ppa. Prasarth Rabindran
Director Group Compliance & IT