PUBLIC
ÖFFENTLICH

ANNEX 17

INFORMATION SECURITY GUIDELINES

December 2021

Guidelines for the tendering party

This document contains specific information that MAN provides to tendering parties for the purpose of responding to requests for proposal.

Instructions for the tendering party

1. The tendering party undertakes not to amend or modify this document in any way.
2. The tendering party's response to this request for proposal should reflect the information contained in this document and correspond to this data.
3. Any objections or issues in connection with the definitions contained in the documents do not render the requirements set out in this document or in the request for proposal invalid, nor do they result in said requirements being modified. The tendering party can only assume that the changes it proposes are accepted if MAN has expressly confirmed this to the tendering party in writing.

Ref no.	
Annex 17 - 1	**OVERVIEW**
Annex 17 - 2	Statutory provisions call for “security measures” to protect sensitive company assets, measures that are crucial in order for an organization to maintain its business operations. As digitization grows, “information assets” that have to be protected are exposed to a growing number of “threats”. Systems, their performance and functions, networks, and organizations are vulnerable as a result of cyber attacks (malware, hacking, denial-of-service attacks, phishing, etc.), sabotage, espionage, vandalism, damage caused by natural hazards like flooding and fire, as well as catastrophes and other “risks”.
Annex 17 - 3	The aim of information security management is to maintain an appropriate level of information security at MAN. To this end, a set of security policies is defined in the information security management system (ISMS) that requires compliance with both organizational and corporate requirements of MAN.
Annex 17 - 4	The main protection objectives of information security for all MAN assets are confidentiality, integrity, and availability. An expanded range of protection objectives includes authenticity, accountability, non-repudiation, and reliability.
Annex 17 - 5	The Contractor shall treat its business relationship with MAN, as well as any information exchanged as part of the said business relationship, as strictly confidential. It undertakes to protect this information carefully against third parties in accordance with these Information Security Guidelines as provided by MAN, using suitable measures. The obligation to maintain secrecy applies for a period in accordance with the IT-AEB. The obligation to maintain secrecy also applies to any knowledge obtained during the tendering phase, irrespective of whether a contract is concluded. In all other respects, the terms of the separate confidentiality declaration apply.
Annex 17 - 6	This Annex outlines the security requirements that the Contractor shall observe and / or comply with (unless otherwise specified or agreed between the parties) when rendering all services and activities as of the inception date of the contract.
Annex 17 - 7	The Contractor shall grant MAN the right, to be exercised at any time and after prior notification, to inspect and review all data relating to business transactions between MAN and the Contractor at the Contractor's premises and to review the technical and organizational measures; MAN or third parties commissioned by MAN shall be permitted to enter the Contractor's premises during normal business hours for the purpose of information security audits. If violations of the agreements of the respective order and/or the information security guidelines are identified, the Contractor shall bear the costs of the review and the implementation of risk-reducing measures, unless the violations are not the fault of the Contractor.

Ref no.	
Annex 17 - 8	For the provision of outsourced IT services by an external service provider that fall within MAN's internal control system (IFR systems) additional IT outsourcing controls are in place. In this case, the Contractor has to commission an independent auditor on an annual basis to check the control framework associated with the services and compile it's findings in an ISAE 3402 report. Depending on the IT service provided, the report may consist of several parts: 1. ISAE 3402 Type 2 Report – Basic Infrastructure Services System provided from the datacentres in Scope 2. ISAE 3402 Type 2 Add-on Report – Database and Middleware Systems for ICFR relevant applications
Annex 17 - 9	When commissioning the Contractor, MAN shall guarantee that the latter has access to the latest version of the documents forming part of the MAN Security Guidelines, as well as the relevant regulations and instructions of its parent company, Volkswagen AG, applicable in each case during the contract term. The set of rules of the MAN Group for information security (**Appendix 17-A (Protection and Security Procedures)**) is valid in principle. The regulations of the Volkswagen Group are valid when there is no explicit MAN regulation in place.
Annex 17 - 10	In the event that services performed for MAN are outsourced to subcontractors, the Contractor shall ensure that subcontractors are also placed under the same obligations and requirements as outlined in this document. Furthermore, the Contractor shall ensure that the right to audit outlined under ref. Annex 17-7 is granted to MAN also with respect to the subcontractor's premises.
Annex 17 - 11	The following additional annexes are part of Annex 17:
Annex 17 - 12	**Appendix 17-A (Protection and Security Procedures)** contains:The organizational instructions include guidelines on information security (data protection and data security)of the MAN Group.

Ref no.	
Annex 17 - 13	**Contract processing:** If the Contractor's service mainly involves the processing of information, it fulfils the term "Information processing on behalf" of MAN. The Contractor must prove its suitability for secure information processing by means of certification. If the Contractor processes information on behalf of MAN with scope of the services offered requiring a high or very high level of information security protection, it is necessary to achieve a **TISAX certification** for the relevant VDA ISA criteria at a minimum of assessment level 2. Depending on the service provision, an **ISO 27001 certification** on the scope, that includes all order processing activities, can also certify the suitability. If the Contractor cannot provide evidence of a valid information security certification, a contractual relationship can only be entered into if the Contractor commits to a **TISAX certification** within the next nine months after the start of the contract. In addition, the Contractor must provide a **gap analysis** in accordance with the TISAX methodology, including an action plan for achieving the certification level within the planned timeframe (**LINK: VDA Information Security Assessment**[1]).
Annex 17 - 14	**Appendix 17-F (Commissioned Data Processing Agreement)** describes MAN's requirements for data protection in commissioned data processing. The draft of the Order Data Processing Agreement is initially for viewing purposes only. A signed version is not yet to be submitted with the offer and will only be taken into account in the course of signing the contract.
Annex 17 - 15	

[1] Information Security - VDA