ANNEX 17

INFORMATION SECURITY GUIDELINES

November 2017

Guidelines for the tendering party

This document contains specific information 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 problems 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 becomes more widespread, “information assets” that have to be protected are exposed to a growing number of “threats”. *Systems*, networks, and organizations are vulnerable as a result of cyber attacks (malicious code, denial-of-service attacks, malware, hacker attacks, spam, etc.), sabotage, espionage, and vandalism, but also damage caused by natural hazards like flooding and fire, as well as *catastrophes* and other “risks”.
Annex 17 - 3	The aim of Safety and Information Security Management, generally known as the *Information Security Management System (ISMS)*, is to define a safety policy to comply with both organizational requirements and the *governance* requirements set by MAN.
Annex 17 - 4	The main protection objectives of information security are confidentiality, integrity, and availability. An expanded range of protection objectives includes authenticity, accountability, non-repudiation, and reliability of the “information assets”.
Annex 17 - 5	The Contractor shall treat its business relationship with MAN, as well as any information exchanged as part of said business relationship, as strictly confidential. It undertakes to protect this information against third parties in accordance with these Information Security Guidelines provided to it by MAN, using suitable measures. The obligation to maintain secrecy remains in force for a period of ten (10) years after the end or complete performance of the respective order placement. 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 to be signed by the Contractor apply.
Annex 17 - 6	This Annex outlines the security requirements the Contractor shall observe and / or comply with when rendering all *services* and activities as of the *inception date* of the contract (in the absence of any information or agreement between the Parties to the contrary). The Appendices attached to this Annex contain two self-assessments to be completed by the Contractor prior to concluding the contract, as well as specific information MAN shall make available to the Contractor.
Annex 17 - 7	The Contractor shall grant MAN the right to inspect and review all data relating to the business transactions between MAN and the Contractor at the latter’s premises, following advance notice, as well as to review information security measures, with MAN entitled to exercise said right at any time; in this respect, MAN or third parties commissioned by the latter may enter the Contractor’s premises during normal business hours as part of information security audits. The costs of reviews and of the implementation of measures to mitigate risks shall be borne by the Contractor in the event that violations against agreements concluded as part of the order placement in question and / or the Information Security Guidelines are identified, unless said violations do not involve any fault on the part of the Contractor.

Ref no.	
Annex 17 - 8	IT Outsourcing controls are planned as part of the provision of outsourced IT services that fall under the scope of the MAN internal control system. In this respect, the Contractor is to regularly commission an independent auditor to check the control framework associated with the services and compile his or her findings in an ISAE 3402 report. The report contains the following two 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 application
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. In the event that express regulations of the MAN Group are available for a specific issue, the regulations of the MAN Group are binding and take precedence over the regulation of the Volkswagen Group.
Annex 17 - 10	In the event that services performed for MAN are outsourced to subcontractors, the Contractor shall take care to ensure that subcontractors are also placed under the obligation to observe the requirements outlined in this document. Furthermore, the Contractor shall take care to ensure that the right to audit outlined under 17-7 is granted to MAN also with respect to the subcontractor's premises.

Annex 17 - 11	The following documents are attached to this Annex are and form part thereof:
Annex 17 - 12	**Appendix 17-A (Protection and Security Procedures)** contains: 1. The Organizational Instructions include existing guidelines on information security (data protection and data security), both of Volkswagen AG (parent company) and of the MAN Group. 2. The Information Security Instructions comprise the safety policy, guiding security principles, and security and implementation regulations for information security (data protection and data security) of MAN, as well as those of Volkswagen AG (parent company).
Annex 17 - 13	**Appendix 17-D (Information Security Assessment)** contains a form for recording an information security assessment and is to be completed by the Contractor.
Annex 17 - 14	**Appendix 17-E (Data Processing Checklist)** contains a form for recording a data processing assessment and is to be completed by the Contractor.
Annex 17 - 15	**Appendix 17-F (Data Processing Agreement)** outlines the requirements set by MAN with respect to data protection during data processing. A draft version of the data processing agreement is initially provided for information purposes only, hence a signed copy of the agreement does not have to be submitted when submitting the tender and is taken into account while the contract is signed.
Annex 17 - 16	**Appendix 17-G Checklist to Evidence International Norms and Certification** contains a form for recording the level of maturity with respect to conformity to international norms. These questions are to be answered with yes or no depending on the degree of conformity and supplemented with a brief comment if necessary.