MAN Energy Solutions

Information Security

- Information Security Guidelines for Suppliers -

Publisher

Group Information Technology

Status

Published

Version

1.0

Classification

Public

Date

November 26, 2020

Scope

These instructions apply to any third party that is processing sensitive data for MAN Energy Solutions SE („MAN ES“) based on contractual relationship.

I Purpose and Definitions

These Information Security Guidelines define information security regulations that 3rd parties must observe when using information and IT devices (e.g. personal computers, workstations, and smartphones or tablet computers).

3rd parties are defined as any party that is providing services to MAN ES based on a contractual relationship. Subsidiary companies, brands of MAN ES and companies that are majority owned by MAN ES are excluded from this definition.

I.I Document Structure and Target Group

These guidelines are aimed at the suppliers' management, employees and relevant sub-contractors.

The document contains three chapters. The following table lists the document structure and the target group for each chapter.

Chapter	Target group
1	All 3rd parties
2	3rd parties, using MAN ES infrastructure
3	3rd parties accessing MAN ES information and data from outside MAN ES infrastructure

A 3rd party may belong to multiple of the mentioned categories.

1 Basic requirements for all 3rd parties

- All 3rd parties are obliged to ensure implementation of current industry standards for information security within their organization or company. The information security standards as defined by the requirements of VDA-ISA (see appendix, A.1.1) in its current version should apply as a reference value.
- Information security events (e.g., vulnerabilities, violations of the Information security regulation) concerning data or systems of MAN ES must be reported immediately to the responsible unit (see appendix A.4.1).
- Suspected vulnerabilities and weak points concerning IT systems of MAN ES must be reported to the responsible unit (see appendix A.4.1).
- Any suspected loss of confidential or secret information must be reported to the responsible unit (see appendix, A.4.2) immediately.

2 Additional requirements for 3rd parties using MAN ES infrastructure

2.1 Definition

A 3rd party is using MAN ES infrastructure if:

- clients (physical or virtual endpoint devices) are provided by a MAN ES Group Company, or
- access to the internal MAN ES network is established using Remote Access solutions (e.g. ZScaler Private Access) ,or
- the 3rd party has been connected directly to the internal MAN ES network.

These suppliers may be located on the premises of the Group Company or on their own companies' premises.

2.2 Requirements

The following requirements must be observed by these 3rd parties:

- Regulations of the respective group company on bringing IT devices that are not belonging to the ordering party on premises or into security areas must be observed.
- The provided devices must be handled correctly and protected from loss or unauthorized modification.
- The manufacturer's instructions for protection of the devices must be complied with.
- Devices provided by the ordering party (e.g., laptops, cellular phones) may only be taken outside the premises of the ordering party after approval.
- Suppliers must only request or initiate procurement and installation of hardware and software via the organizational unit (business department of the ordering party) that is responsible for them.
- Usage of the provided hardware and software is subject to the regulations of the respective group company (see appendix, A.4.3).
- Only the responsible units are permitted to open the IT device, make changes to the hardware (e.g., installation/removal of hard drives and memory modules), and make manual changes to security settings (e.g., browser settings) (see appendix, A.4.4).
- Usage or subsequent modification of programs is only permissible with authorization of the responsible units (see appendix, A.4.4).
- Data of any other customer that does not belong to MAN ES must not be processed on the provided IT devices.

- The use of IT devices and data of the ordering party by employees of the supplier requires the express consent of the ordering party. The ordering party is entitled to prohibit access/use at any time (e.g., in cases of misuse).

3 Additional requirements for 3rd parties accessing MAN ES information from outside MAN ES infrastructure[1]

- These 3rd parties must observe their own regulations for information security.
- Implementation of measures for information security must be demonstrated according to TISAX®[2] or ISO 27001. This can be deviated from when accessing MAN ES information that has only a low level of protection after approval of the responsible unit (see appendix A.4.5).

II Exceptions and Deviations

This regulation must be observed by all suppliers as defined in the scope of this document. Deviations from this regulation, that reduce the security level, are only allowed temporarily and after consultation with the responsible units (see appendix A.4.5).

[1] Additional requirements apply for 3rd parties providing MAN ES information outside MAN ES infrastructure.
[2] Trusted Information Security Assessment eXchange, see www.tisax.org

A General Information

A.1 Additional documents

A.1.1 Information Security Assessment published by the Verband der Automobilindustrie e.V. (Download: VDA www.vda.de)

A.1.2 Regulations, Guidelines and Best practices on information security published by MAN ES

A.2 Validity

This information security regulation is valid immediately after publication.

A.3 Document history

Version	Name	Org. Unit	Date	Comment
1.0	Group IT	Governance	26. November 2020	Initiale Version

A.4 Company specific characteristics

A.4.1 Cyber Defense Center MAN ES - via IT ServiceDesk (Tel. +49 800 1758 1758, mail: servicedesk@man-es.com)

A.4.2 Information to Information Security, mail: infosec@man-es.com

A.4.3 Each contractor is responsible for ensuring the proper use of information, programs, and IT devices only for company purposes and within the scope of the respective assignment.

Sending data containing non business content is not permitted.

The use of the Internet for private purposes is not permitted.

The use of private software and data on IT devices provided by the company is not permitted

A.4.4 Responsibilities: To be requested from the contractor.

A.4.5 Responsibility: Information Security MAN ES, mail: infosec@man-es.com