MAN Energy Solutions

Informationssicherheit

- Handlungsleitlinien für Dienstleister -

Herausgeber

Group Information Technology

Status

veröffentlicht

Version

1.0

Klassifikation

Public

Datum

26. November 2020

Geltungsbereich

Diese Anweisungen gelten für alle Dritte, die schutzbedürftige Informationen für MAN Energy Solutions SE („MAN ES“) entsprechend vertraglicher Vereinbarungen verarbeiten.

I Zweck und Definitionen

Diese Handlungsleitlinie definiert Regeln für Informationssicherheit, die von Dritten beim Umgang mit Informationen und IT-Geräten (z. B. PCs, Arbeitsplätze, Laptops, Smartphones oder Tablet-PCs) zu befolgen sind.

Dritte sind definiert als Vertragspartner, die Dienstleistungen für MAN ES auf Basis vertraglicher Beziehungen erbringen. Tochtergesellschaften von MAN ES, sowie Gesellschaften, an denen MAN ES Mehrheitsbeteiligungen hält, sind von dieser Definition ausgeschlossen.

I.I Dokumentenstruktur und Zielgruppe

Diese Handlungsleitlinien richten sich an die Geschäftsleitung der Dritten, deren Mitarbeiter sowie deren Erfüllungs-/Verrichtungshilfen.

Dieses Dokument enthält drei Kapitel. Die folgende Tabelle führt die Dokumentenstruktur und die jeweilige Zielgruppe pro Kapitel auf.

Kapitel	**Zielgruppe**
1	Alle Dritte
2	Dritte, die in der MAN ES Infrastruktur arbeiten.
3	Dritte, die MAN ES Informationen außerhalb der MAN ES Infrastruktur im Zugriff haben.

Ein Dritter kann je nach Zusammenarbeitsmodell gleichzeitig zu mehreren Zielgruppen gehören.

1 Allgemeine Anforderungen an alle Dritten

- Die Dritten verpflichten sich, die Umsetzung gängiger Industrie-Standards zur Informationssicherheit in ihrem Unternehmen bzw. ihrer Organisation sicherzustellen. Als Referenzwert sollen die Informationssicherheitsstandards nach den Anforderungen des VDA-ISA (siehe Anhang, A.1.1) in seiner jeweils gültigen Form gelten.
- Informationssicherheitsereignisse (z. B. auftretende Störungen, Verstöße gegen das Informationssicherheits-Regelwerk), welche Daten oder Systeme der MAN ES betreffen, sind unverzüglich der zuständigen Stelle zu melden (siehe Anhang, A.4.1).
- Vermutete Verwundbarkeiten und Schwachstellen von IT-Systemen der MAN ES sind unverzüglich der zuständigen Stelle zu melden (siehe Anhang, A.4.1).
- Beim Verdacht auf Verlust von vertraulichen oder geheimen Informationen der MAN ES muss dies sofort an die zuständige Stelle gemeldet werden (siehe Anhang, A.4.2).

2 Zusätzliche Anforderungen für Dritte, die in der MAN ES Infrastruktur arbeiten

2.1 Definition

Ein Dritter arbeitet in der MAN ES Infrastruktur, wenn:

- Clients (physische oder virtuelle Endgeräte) von einer MAN ES Konzerngesellschaft zur Verfügung gestellt werden, oder
- die Anbindung über Remote-Access-Lösungen (wie z.B. ZScaler Private Access) erfolgt mit Zugriff auf das interne Konzernnetzwerk, oder
- die Anbindung des Dritten direkt an das interne Konzernnetzwerk erfolgt.

Dies ist unabhängig davon, ob sich der Dritte auf dem Gelände einer Konzerngesellschaft befindet oder nicht.

2.2 Anforderungen

Für diese Dritten gelten die folgenden Anforderungen:

- Regelungen der jeweiligen Konzerngesellschaft bezüglich des Mitbringens von nicht dem Auftraggeber gehörenden IT-Geräten auf das Firmengelände oder in Sicherheitsbereiche müssen eingehalten werden.
- Die zur Verfügung gestellten Geräte sind sachgemäß zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen.
- Die Vorschriften des Herstellers zum Schutz der Geräte sind einzuhalten.
- Durch den Auftraggeber zur Verfügung gestellte Geräte (z.B. Laptops, Mobiltelefone) dürfen nur nach erfolgter Genehmigung vom Werksgelände des Auftraggebers mitgenommen werden.
- Dienstleister dürfen die Bereitstellung oder Installation von Hardware und Software nur über den für sie zuständigen Fachbereich des Auftraggebers durchführen oder initiieren.
- Bezüglich der Nutzung der zur Verfügung gestellten Hard- und Software gelten die Regelungen der jeweiligen Konzerngesellschaft (siehe Anhang, A.4.3).
- Das Öffnen des IT-Gerätes und das Durchführen von Veränderungen an der Hardware (z. B. Ein-/Ausbau von Festplatten, Speicherbausteinen) sowie manuelle Veränderungen der Sicherheitseinstellungen (z. B. Browsereinstellungen) ist nur den zuständigen Stellen (siehe Anhang, A.4.4) gestattet.

- Der Einsatz oder das nachträgliche Verändern von Programmen des Auftraggebers ist nur zulässig, wenn diese von den zuständigen Stellen (siehe Anhang, A.4.4) genehmigt wird.
- Auf den zur Verfügung gestellten IT-Geräten sind keine Daten von weiteren Kunden, die nicht zum Konzern gehören, zu verarbeiten.
- Das Verwenden von IT-Geräten oder Daten des Auftraggebers durch Mitarbeiter des Dienstleisters erfordert die ausdrückliche Zustimmung des Auftraggebers. Der Auftraggeber ist ermächtigt, jederzeit den Zugriff oder die Benutzung zu untersagen (z.B. bei Missbrauch).

3 Zusätzliche Anforderungen für Dritte, die MAN ES Informationen außerhalb der MAN ES Infrastruktur im Zugriff haben[1]

- Diese Dritten sind an die eigenen Regularien zur Informationssicherheit gebunden.
- Die Umsetzung von Maßnahmen zur Informationssicherheit ist gemäß TISAX®[2] oder ISO 27001 nachzuweisen. Davon kann bei Zugriff auf MAN ES Informationen, die eine nur geringe Schutzhöhe haben, nach Zustimmung der zuständigen Stellen (siehe Anhang A.4.5) abgewichen werden.

II Abweichungen und Ausnahmen

Abweichungen von diesen Handlungsleitlinien, die das Sicherheitsniveau senken, sind nur temporär und nach Rücksprache mit den zuständigen Stellen (siehe Anhang A.4.5) zulässig.

[1] Für Dritte, die MAN ES Informationen außerhalb der MAN ES Infrastruktur bereitstellen, gelten zusätzliche Anforderungen.
[2] Trusted Information Security Assessment exchange, siehe www.tisax.org

A Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Information Security Assessment des Verbands der Automobilindustrie e.V. (Download von der Website des VDA www.vda.de)

A.1.2 Regelungen, Leitfäden und Merkblätter der MAN ES zur Informationssicherheit

A.2 Gültigkeit

Diese Informations-Sicherheitsregelung tritt zum Zeitpunkt der Veröffentlichung in Kraft.

A.3 Dokumenthistorie

Version	Name	Abteilung	Datum	Kommentar
1.0	Group IT	Governance	26. November 2020	Initiale Version

A.4 Gesellschaftsspezifische Ausprägungen

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

A.4.2 Information an Informationssicherheit, mail: infosec@man-es.com

A.4.3 Jeder Auftragnehmer ist dafür verantwortlich, dass Informationen, Programme und IT-Geräte nur für Unternehmenszwecke und im Rahmen der jeweiligen Aufgabenstellung ordnungsgemäß eingesetzt und genutzt werden.

Das Versenden von Daten mit nicht dienstlichem Inhalt ist unzulässig.

Die Nutzung des Internets zu privaten Zwecken ist nicht erlaubt.

Der Einsatz privater Software und Daten auf den von der Gesellschaft gestellten IT-Geräten ist verboten.

A.4.4 Verantwortlichkeit: Vom Auftragnehmer zu erfragen.

A.4.5 Verantwortlichkeit: Informationssicherheit MAN ES, mail: infosec@man-es.com