PUBLIC
ÖFFENTLICH

ANLAGE 17-A

POLICY PACK ÖFFENTLICH

Stand März 2023

Dieses Dokument enthält firmeneigene Informationen der MAN Truck & Bus. Dieses Dokument und die darin enthaltenen Informationen dürfen nur mit ausdrücklicher vorheriger schriftlicher Genehmigung der MAN Truck & Bus veröffentlicht, weitergegeben oder zu anderen Zwecken eingesetzt werden.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Informationssicherheit

Ersteller	Steven Rauwerdink Ralf Schlag	**Freigeber**	Andre Wehner	**Version**	**3.0**
Abt.	FIOS	Abt.	FI	**KSU-Klasse:**	x.x

Gültigkeitsbeginn Datum 01.02.2023	**Geltungsbereich** MAN Truck & Bus SE und deren Tochtergesellschaften	**Genehmigungen (Vorstand)** Alexander Vlaskamp, MTB Friedrich Baumann, MTB-S Murat Aksel, MTB-B Michael Kobriger, MTB-P Inka Koljonen, MTB-F Arne Puls, MTB-H Dr. Frederik Zohm, MTB-E **Abgestimmt mit**

Inhalt

Anlagen

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Zweck

Der Zweck dieser Richtlinie ist es, einen Rahmen für die Sicherung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten der MAN Truck & Bus Gruppe zu schaffen. Innerhalb dieses Rahmens müssen Strategien, Ziele und Umsetzungsverantwortlichkeiten entwickelt werden, damit jedes Unternehmen der MAN Truck & Bus Gruppe ein angemessenes Niveau an Informationssicherheit erreicht.

Diese Informationssicherheitsrichtlinie regelt die verbindlichen, verpflichtenden Ziele und Grundsätze für alle Unternehmen der MAN Truck & Bus Gruppe in Bezug auf das Informationssicherheitsmanagement, einschließlich der Rollen- und Verantwortungsverteilung zwischen der MAN Truck & Bus SE und jedem Unternehmen der MAN Truck & Bus Gruppe.

Diese Informationssicherheitsrichtlinie bildet zusammen mit der untergeordneten MTB Markenanweisung MA_13_1_01 - Standard für Informationssicherheit (im Folgenden MTB-Standard für Informationssicherheit genannt) und weiteren Markenanweisungen den Rahmen für das Informationssicherheitsmanagement innerhalb der MAN Truck & Bus Gruppe (vgl. Abschnitt 7). Diese Richtlinie bildet die Grundlage für alle weiteren Regelungen zur Informationssicherheit innerhalb der MAN Truck & Bus Gruppe.

2 Geltungsbereich

Diese Markenrichtlinie gilt weltweit für die MAN Truck & Bus SE und ihre Tochtergesellschaften sowie deren Mitarbeiter[1]. Sie gilt unmittelbar und bedarf keiner Umsetzungsrichtlinie durch einzelne Tochtergesellschaften. Für Gesellschaften, bei denen die MAN Truck & Bus SE die Geltung der Markenrichtlinie aus rechtlichen Gründen nicht unmittelbar bewirken kann, ist in Abstimmung mit dem Chief Information Security Officer (CISO) zu klären, inwieweit diese Markenrichtlinie Anwendung findet. Dies gilt beispielsweise für Gesellschaften, die sich nicht zu 100 % im Anteilsbesitz der MAN Truck & Bus SE befinden und auch nicht durch einen Beherrschungsvertrag mit der MAN Truck & Bus SE verbunden sind (wie z.B. Gesellschaften, die sich im Anteilsbesitz der MAN Finance and Holding S.A. befinden).

Diese Richtlinie hat Vorrang vor anderen internen MAN Truck & Bus Regelungen in Bezug auf die Informationssicherheit. Sofern Gesellschaften eigene Regelungen zur Informationssicherheit erlassen haben, sind diese umgehend außer Kraft zu setzen. Bis zur Außerkraftsetzung solcher Richtlinien oder Teilen von Richtlinien gilt diese Markenrichtlinie vorrangig.

Sollten Regelungen dieser Markenrichtlinie aufgrund zwingender lokaler Anforderungen nicht umgesetzt werden können, muss die betroffene Gesellschaft unverzüglich den Regelungsverantwortlichen (Chief Information Security Officer (CISO)) der MAN Truck & Bus SE informieren, um notwendige Änderungen oder Ergänzungen zu besprechen. In solchen Fällen ist das MAN Truck & Bus Unternehmen verpflichtet, eine mit dem Richtlinienverantwortlichen abzustimmende Regelung zu treffen, die unter Berücksichtigung zwingender lokaler Erfordernisse den Regelungen dieser Richtlinie möglichst nahekommt.

Sollten nationale Rechtsvorschriften ein höheres Schutzniveau oder weitergehende Anforderungen an den Umgang mit der Informationssicherheit vorschreiben als in dieser Richtlinie vorgesehen, haben diese Rechtsvorschriften Vorrang.

Diese Markenrichtlinie wird durch Markenanweisungen und Regelungen der MAN Truck & Bus SE und ihre Tochtergesellschaften ergänzt (siehe Abschnitt 7). Die einzelnen Tochtergesellschaften können ergänzende Regelungen zur Informationssicherheit erstellen. Diese Regelungen dürfen nicht im Widerspruch zu den Vorschriften in dieser Markenrichtlinie und den zusätzlichen Markenanweisungen

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

stehen. Der CISO muss über alle zusätzlichen Regelungen im Zusammenhang mit dieser Markenrichtlinie informiert werden.

Das Dokument muss mindestens alle drei Jahre überprüft und gegebenenfalls angepasst werden.

3 Begriffe und Definitionen

Ein Glossar für das gesamte Regelwerk der Informationssicherheit befindet sich in der Zusatzinformation „Begriffe und Definitionen zur Informationssicherheit“.

4 Die Ziele des Informationssicherheitsmanagements

Vorrangiges Ziel des Informationssicherheitsmanagements ist der Schutz der MAN Truck & Bus Gruppe und ihrer Interessenvertreter, Kunden und Partner vor Schäden und Risiken, die durch den Einsatz von Informations- und Kommunikationstechnologie (IKT) und im Umgang mit Informationen und Daten entstehen können. Dazu gehört die sichere Bereitstellung der Produkte und Dienstleistungen der MAN Truck & Bus Gruppe.

Auf dieser Grundlage hat die MAN Truck & Bus Gruppe folgende Informationssicherheitsziele formuliert:

- Effiziente Identifizierung und Bewertung von Risiken, die durch den Einsatz von IKT und im Umgang mit Informationen und Daten entstehen können.
- Einhaltung von Gesetzen, Vorschriften und Vereinbarungen über den Schutz von Informationen und Daten.
- Einrichtung eines funktionsfähigen und wirksamen Informationssicherheitsmanagementsystems (ISMS).
- Die Umsetzung von kosten- und aufwandswirksamen Maßnahmen zur Sicherung von Informationen und Daten entsprechend dem Risikoniveau.
- Minimale Einschränkungen der Geschäfts- und Produktionsprozesse durch die Umsetzung kritischer Sicherheitsmaßnahmen.
- Hohe Effizienz des Informationssicherheitsmanagements und des Schutzes von Informationen und Daten.

5 Grundsätze zur Einhaltung der Informationssicherheit in der MAN Truck & Bus Gruppe

Das angemessene Informationssicherheitsniveau wird dadurch erreicht, dass die Informationssicherheitsrisiken für jedes einzelne MAN Truck & Bus Unternehmen und die MAN Truck & Bus Gruppe als Ganzes auf einem akzeptablen Niveau gehalten werden. In jedem Unternehmen der MAN Truck & Bus Gruppe muss ein ISMS eingerichtet werden, das sicherstellt, dass sowohl die Ziele der Informationssicherheit als auch die Geschäftsziele von MAN Truck & Bus durch einen spezifischen risikobasierten Ansatz unter Abwägung von Kosten und Nutzen erfüllt werden.

Die genannten Anforderungen an das Informationssicherheitsmanagement müssen von allen Konzernunternehmen der MAN Truck & Bus Gruppe eingehalten werden. Diese werden durch den MAN Truck & Bus Standard für Informationssicherheit spezifiziert.

5.1 Bewusstsein der Mitarbeiter

Alle Mitarbeiter der MAN Truck & Bus Gruppe müssen von ihrem Vorgesetzten auf die Risiken im Umgang mit Informationen und Daten in der MAN Truck & Bus Gruppe aufmerksam gemacht werden. Die Mitarbeiter müssen in ihrem jeweiligen Verantwortungsbereich befähigt werden, das Unternehmen und/oder die MAN Truck & Bus Gruppe vor Informationssicherheitsvorfällen und deren Folgen zu

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

schützen. Das Bewusstsein der Mitarbeiter für die Informationssicherheit muss von der Leitung der Sparte oder des Unternehmens kontinuierlich aufrechterhalten werden.

5.2 Bestandsaufnahme und Klassifizierung von Informationen

Die Grundlage für die Klassifizierung von Informationen ist die Erstellung und Pflege eines Inventars aller relevanten immateriellen Informationsressourcen. Die für die jeweiligen Geschäftsprozesse verantwortlichen Mitarbeiter müssen den Schutzbedarf der entsprechenden Informationsressourcen entsprechend der Klassifizierung in Bezug auf die Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit bestimmen. Hierfür ist die MTB Markenanweisung MA_13_1_03 - Klassifizierung von Informationsressourcen als Grundlage zu verwenden.

5.3 Risikoidentifizierung und Risikobewertung

Die Informationssicherheitsrisiken, die mit der Nutzung, Übertragung, Verarbeitung und Speicherung von Informationen durch die MAN Truck & Bus Gruppe verbunden sind, müssen identifiziert, bewertet und so gesteuert werden, dass die Risiken für jedes einzelne Unternehmen und die MAN Truck & Bus Gruppe als Ganzes auf einem akzeptablen Niveau bleiben. Die MTB Markenanweisung MA_13_1_04 - Risikomanagement muss dabei als Grundlage verwendet werden.

5.4 Dokumentation des Informationssicherheitsmanagements

Verfahren und Ergebnisse im Zusammenhang mit dem Informationssicherheitsmanagement müssen in nachprüfbarer Form dokumentiert werden, um den Anforderungen der Rechnungsprüfung und der Prüfung etwaiger Haftungsansprüche zu genügen.

5.5 Risikogerechte Umsetzung von Schutzmaßnahmen

Die Kosten und der Aufwand für die Umsetzung der Maßnahmen müssen in einem angemessenen Verhältnis zur Höhe des Risikos stehen, gegen das sie gerichtet sind. Bei der risikogerechten Umsetzung von Maßnahmen sind folgende Grundsätze zu beachten:

- Informationen sowie Kommunikationsinfrastrukturen müssen entsprechend dem Risikoniveau für die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen während ihrer Nutzung, Übertragung, Verarbeitung und Speicherung geschützt werden (siehe MTB Markenanweisung MA_13_1_03 - Klassifizierung von Informationsressourcen).
- Der Schutz von Informationen und Daten muss in allen Phasen des Lebenszyklus von Informationsressourcen gewährleistet sein. Dazu gehören die Planung, Beschaffung, Entwicklung, Wartung und Abnahme der Produktion von IKT-Systemen.
- Der Schutz von Informationen und Daten muss in allen Phasen des Lebenszyklus des Identitätsmanagements gewährleistet sein. Dazu gehören Mitarbeiter, Lieferanten und externe Auftragnehmer.
- Der Informations- und Datenschutz muss in allen Geschäftsprozessen gewährleistet sein.
- Alle IKT-Systeme müssen vor bösartigen Angriffen und Malware geschützt werden.
- Informationen und Daten auf zentralen IKT-Systemen müssen gesichert und eine erfolgreiche Wiederherstellung muss gewährleistet werden.
- Der Informationsaustausch innerhalb der MAN Truck & Bus Gruppe und mit vertrauenswürdigen externen Partnern muss angemessen geschützt werden.
- Es müssen wirksame Verfahren und Technologien eingeführt werden, um sicherzustellen, dass Vorfälle und Schwachstellen im Bereich der Informationssicherheit erkannt, gemeldet, überwacht und durch geeignete Maßnahmen behoben werden. Es muss ein standardisierter und effektiver

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Ansatz für die Behandlung von Informationssicherheitsvorfällen und bekannten technischen Schwachstellen festgelegt werden.

- Der Zugang zu den Informationssystemen darf nur befugten Mitarbeitern nach dem Grundsatz „Kenntnis nur, wenn erforderlich“ gewährt werden. Unbefugte Benutzerzugriffe, Sicherheitsverletzungen und der Diebstahl von Informationen oder informationsverarbeitenden Einrichtungen müssen in geeigneter Weise erkannt, gemeldet, überwacht und verhindert werden.
- Das allgemeine Management der Kontinuität des Geschäftsbetriebs muss Aspekte der Informationssicherheit wie Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Daten berücksichtigen.
- Einschlägige gesetzliche Bestimmungen, Vorschriften und vertragliche Verpflichtungen zur Informationssicherheit müssen verwaltet und eingehalten werden.

5.6 Betrachtung der Norm ISO 27001

Das Management der Informationssicherheit in der MAN Truck & Bus Gruppe basiert auf der international anerkannten Norm für Informationssicherheitsmanagement, ISO 27001. Grundlage hierfür ist die MTB Markenanweisung MA_13_1_01 - Standard für Informationssicherheit (vgl. Abschnitt 7.1).

5.7 Zusammenarbeit mit Dritten

Externe Lieferanten und Partner, die im Auftrag der MAN Truck & Bus Zugang zu Informationen haben und/oder diese verarbeiten, müssen vertraglich verpflichtet werden, die Anforderungen der MAN Truck & Bus zur Informationssicherheit einzuhalten. Bitte beachten Sie die MTB Markenanweisung MA_13_1_08 - Informationssicherheit für Lieferanten (vgl. Abschnitt 7.1).

6 Verantwortlichkeiten für die Informationssicherheit in der MAN Truck & Bus Gruppe

6.1 Verantwortlichkeiten für das Informationssicherheitsmanagement innerhalb der MAN Truck & Bus Gruppe

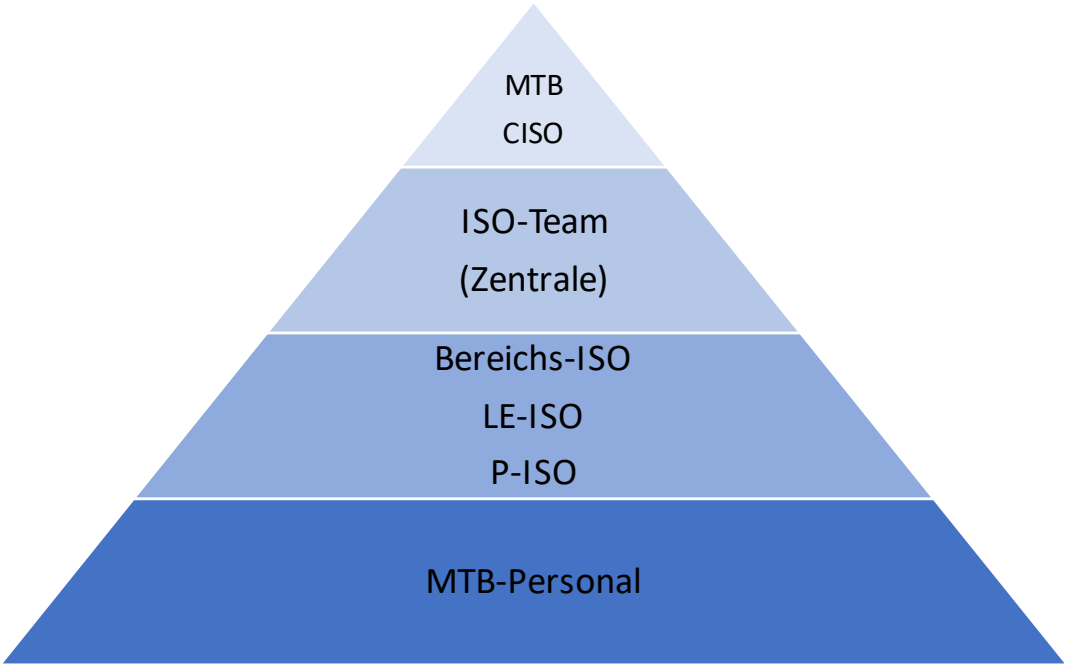


Abbildung 1 Organisation der Informationssicherheit

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Einzelheiten zu den Verantwortlichkeiten finden Sie in der MTB Markenanweisung MA_13_1_02 – Informationssicherheitsmanagement

6.1.1 Chief Information Security Officer (CISO)

Der CISO ist für die zentrale Steuerung und Verbesserung der Informationssicherheit innerhalb der MAN Truck & Bus Gruppe verantwortlich.

Der Chief Information Officer (CIO) ernennt einen qualifizierten CISO für die MAN Truck & Bus Gruppe. In enger Anlehnung an die Geschäftsstrategie der MAN Truck & Bus Gruppe entwickelt und pflegt der CISO die konzernspezifische Informationssicherheitsstrategie, den risikoorientierten Schutz der Informationsressourcen des Konzerns sowie Verfahren zur Bewertung und Darstellung des Informationssicherheitsniveaus des Konzerns. Er wird vom MAN Truck & Bus ISO-Team unterstützt.

Der CISO definiert die Grundsätze des Informationssicherheitsrahmenwerks der MAN Truck & Bus Gruppe und überwacht dessen Einhaltung.

Der CISO der MAN Truck & Bus Gruppe berichtet dem Vorstand der MAN Truck & Bus Gruppe regelmäßig über den Umsetzungsstand des Informationssicherheitsmanagements in den Sparten und im Konzernunternehmen.

Der CISO fungiert zusammen mit dem ISO-Team als Ansprechpartner für alle Belange der Informationssicherheit in der MAN Truck & Bus Gruppe.

6.1.2 ISO-Team (Zentrale)

Das ISO-Team hat die übergreifende Aufgabe, Informationssicherheit in der MAN Truck & Bus Gruppe zu etablieren. Das Team unterstützt den CISO der Gruppe bei der Erfüllung seiner Aufgaben.

6.1.3 Beauftragte für Informationssicherheit (Bereichs-ISO / LE-ISO / P-ISO)

Für Bereiche außerhalb des zentralen Organisationsbereichs der MAN Truck & Bus ist es erforderlich, Informationssicherheitsbeauftragte zu etablieren, die sich um die dezentrale Umsetzung der Informationssicherheit in der MAN Truck & Bus Gruppe kümmern, abgestimmt auf die jeweiligen Geschäftsprozesse und auf die lokalen Gegebenheiten und Anforderungen.

Die Informationssicherheitsbeauftragten der Bereiche, der Legal Entity Information Security Officer (LE-ISO) und der Production Information Security Officer (P-ISO) sind in ihrem Zuständigkeitsbereich die direkten Ansprechpartner für die zentrale MAN T&B Informationssicherheitsorganisation an der Schnittstelle zu den (lokalen) Fachabteilungen und den Abteilungen der Informationssysteme. Sie unterstützen alle mit der Informationssicherheit zusammenhängenden Themen in ihrem Bereich.

Die Führungsgremien der einzelnen Unternehmen der MAN Truck & Bus Gruppe ernennen die verantwortlichen LE-ISOs / P-ISOs.

Die Bereichs-ISOs sind in der MAN Truck & Bus SE angesiedelt (beispielsweise Finanzen, Rechnungswesen, MHR, Einkauf etc.) und sollten auf Abteilungsebene ernannt werden.

6.2 Verantwortungsvoller Umgang mit Informationen und Daten

Jeder Geschäftsprozessverantwortliche in der MAN Truck & Bus Gruppe muss die für die ordnungsgemäße Durchführung der Geschäfts- und Produktionsprozesse erforderlichen Informationen angemessen schützen. Der Geschäftsprozessverantwortliche ist mit Unterstützung der

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Informationssicherheitsbeauftragten (Bereichs-ISO / LE-ISO / P-ISO) für die Umsetzung der Informationssicherheitsmaßnahmen in seinem Verantwortungsbereich zuständig.

Alle Mitarbeiter der MAN Truck & Bus Gruppe sind verpflichtet, alle Informationen und Daten in ihrem Verantwortungsbereich gemäß den markeninternen Regelungen zu schützen. Weitere Informationen sind in der zusätzlichen MTB Markenanweisung MA_13_1_05 - Informationssicherheit für Mitarbeiter enthalten.

6.3 Verantwortungsvolle Nutzung von Systemen der Informations- und Kommunikationstechnologie (IKT)

Alle Mitarbeiter sind persönlich verpflichtet, bei ihren jeweiligen Aufgaben die Anforderungen an die Informationssicherheit einzuhalten. Jeder Mitarbeiter handelt mit den erforderlichen Systemen und Ressourcen entsprechend dem Arbeitsauftrag und in Übereinstimmung mit den Sicherheitsregelungen, Standards, Richtlinien und Verordnungen.

6.4 Verantwortungsvolle Bereitstellung von Systemen der Informations- und Kommunikationstechnologie (IKT)

Alle Mitarbeiter der MAN Truck & Bus Gruppe, die IKT-Systeme zur Nutzung entwickeln und/oder implementieren sowie mit dem Betrieb solcher Systeme befasst sind, sind für die Gewährleistung der Informationssicherheit in Übereinstimmung mit den Sicherheitsrichtlinien verantwortlich. Für alle Anwendungen und IT-Systeme müssen Ressourcenverantwortliche zugewiesen werden.

7 Weitere Regelungen zur Informationssicherheit innerhalb der MAN Truck & Bus Gruppe

Diese Richtlinie wird durch zielgruppenspezifische Anweisungen und Regelungen ergänzt.

7.1 Weitere Markenanweisungen

Diese Markenrichtlinie wird durch zusätzliche Markenanweisungen ergänzt, die die Standards für das Informationssicherheitsmanagement näher regeln. Diese Regelungen sind für alle Unternehmen des Konzerns und ihre Mitarbeiter verbindlich.

Die diese Markenrichtlinie ergänzenden Markenanweisungen sind vom oder im Auftrag des CISO der MAN Truck & Bus Gruppe zu erstellen. Der CISO ist verantwortlich für die Einhaltung der Regelungen im Hinblick auf die entsprechenden gesetzlichen Rahmenbedingungen und Anforderungen.

Der CISO leitet die Markenanweisungen an den CIO zur Validierung und Genehmigung weiter.

Nach der Genehmigung einer Markenanweisung veranlasst der CISO die Bekanntmachung für die Zielgruppe und informiert den zuständigen Richtlinienkoordinator, der die Veröffentlichung der Markenanweisungen auf dem entsprechenden Richtlinienportal vornimmt.

7.2 Weitere informationssicherheitsbezogene Anweisungen

Während die Markenanweisungen Themen der Informationssicherheit für die gesamte MAN Truck & Bus Gruppe regeln, können weitere Anweisungen, die bestimmte Fachbereiche detaillierter regeln, erstellt und in der Praxis angewendet werden.

Diese Anweisungen werden von den zuständigen Stellen der jeweiligen Fachbereiche und mit Unterstützung durch den CISO erstellt und vom CIO genehmigt.

7.3 Weitere Regelungen der Unternehmen der MAN Truck & Bus Gruppe

Neben der Markenrichtlinie MTB MR_13_1 und der Markenanweisung MA_13_1_01 - Standard für Informationssicherheit sind weitere Verordnungen zu schaffen, um die Umsetzung eines wirksamen Informationssicherheitsmanagementsystems (ISMS) im Konzernunternehmen zu gewährleisten.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Diese lokalen Regelungen müssen mit den gesetzlichen und vertraglichen Anforderungen an die Informationssicherheit übereinstimmen und regelmäßig überprüft und gegebenenfalls geändert werden. Die lokalen Regelungen müssen vom Leitungsorgan des entsprechenden Konzernunternehmens genehmigt werden.

Der CISO muss über dezentrale Regelungen informiert werden.

8 Änderungen

Version 3.0

- Änderungsprotokoll hinzugefügt
- Umetikettierung MTB
- Änderung von Rollen und Verantwortlichkeiten
- Inhaltsübernahme von AN_MTB_13_1_02
- Umbenennung der Abschnitte 6.1.2
  Streichung der Abschnitte 7.1.1, 7.1.2, 7.1.3

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

I. **Anlage 1:** Glossar – Begriffe und Definitionen der Informationssicherheit

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Anlage 1 – Glossar

Begriffe und Definitionen der Informationssicherheit

Ersteller	Steven Rauwerdink Ralf Schlag	**Freigeber**	Andre Wehner	**Version**	**3.0**
Abt.	FIOS	Abt.	FI	**KSU-Klasse:**	x.x

Gültigkeitsbeginn	**Geltungsbereich**	**Genehmigungen (Vorstand)**
Datum 01.02.2023	MAN Truck & Bus SE und deren Tochtergesellschaften	Alexander Vlaskamp, MTB Friedrich Baumann, MTB-S Murat Aksel, MTB-B Michael Kobriger, MTB-P Inka Koljonen, MTB-F Arne Puls, MTB-H Dr. Frederik Zohm, MTB-E **Abgestimmt mit**

Begriff	Definition
Eigentümer eines Systems bzw. einer Anwendung	Der Eigentümer eines Systems bzw. einer Anwendung stellt sicher, dass die Prozesse, Anwendungen, Systeme und Netze, für die er verantwortlich ist, unter Einhaltung der Sicherheitsrichtlinien eingerichtet und betrieben werden. Er berichtet darüber an den CISO bzw. die Informationssicherheitsabteilung und kümmert sich um operative Maßnahmen, z. B. die Nutzung von zentral bereitgestellten Sicherheitsdiensten (z. B. Virenschutz). Die Sicherheitsrichtlinien und Sicherheitsanweisungen geben den Standard für die Maßnahmen vor und dienen als Referenz für vertragliche Vereinbarungen mit Dienstleistern sowie für Kontrollen und Revisionen. Der Eigentümer eines Systems bzw. einer Anwendung ist verantwortlich für: Umsetzung des Rechtekonzepts (produkt-/systemabhängig) nach zentralen Vorgaben Vergabe, Verwaltung und Entzug von Zugriffsberechtigungen für Anwendungen, IT-Systeme, Netzwerke und Informationen für Berechtigte. Überprüfung von Anwendungen, Systemen und Netzwerken auf Schwachstellen Überwachung der Einhaltung von Sicherheitsrichtlinien Information der Benutzer über Sicherheitsrisiken und damit verbundene Probleme Meldung von bedeutenden Schwachstellen und schweren Sicherheitsvorfällen an die IS-Ansprechpartner oder den CISO / die Informationssicherheitsabteilung Gewährleistung des Zugangs zu und Überwachung von Anwendungen, IT-Systemen und Netzwerken Technischen Support bei Sicherheitsvorfällen
Betriebliches Kontinuitätsmanagement (BCM)	Das BCM legt fest, wie der Betrieb oder die Bereitstellung von Diensten bei Störungen oder Unterbrechungen infolge von Ereignissen wie Bränden, Überschwemmungen, Stromausfällen, Diebstahl und Vandalismus, Erdbeben und Pandemien fortgesetzt werden kann. Ganzheitlicher Managementprozess, der potenzielle Bedrohungen für ein Unternehmen und die Auswirkungen auf den Geschäftsbetrieb identifiziert, die diese Bedrohungen verursachen können, wenn sie wahr werden, und der einen Rahmen für den Aufbau von unternehmerischer Widerstandsfähigkeit mit der Fähigkeit bietet, wirksam zu reagieren und die Interessen der wichtigsten Stakeholder, den Ruf, die Marke und die wertschaffenden Aktivitäten des Unternehmens zu schützen. Das betriebliche Kontinuitätsmanagement (BCM) umfasst die Disziplinen Gefahrenabwehr, Krisenmanagement, Disaster Recovery (Technologiekontinuität) und Geschäftskontinuität (organisatorische/operative Verlagerung).

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Business Impact Analyse (BIA)	Eine Business Impact Analyse (BIA) quantifiziert Risiken in Bezug auf spezifische Geschäftsprozesse. Sie unterstützt die Bestimmung des Schutzbedarfs für Informationsressourcen.
Business Process Owner	Verantwortlich für die regelmäßige Identifizierung aller Risiken der Prozesse in seinem Verantwortungsbereich und die Sicherstellung ihrer Abdeckung durch geeignete Kontrollen. Dies umfasst die Dokumentation der Kontrollen und der damit verbundenen Tests, die Umsetzung der Maßnahmen zur Beseitigung etwaiger Schwachstellen in den Kontrollen, und die regelmäßige Überprüfung der Kontrollen auf Aktualität und vollständige Abdeckung der Prozesse.
CERT	Computer Emergency Response Team.
Chief Information Officer (CIO)	Der Corporate **Chief Information Officer** der MAN Truck & Bus Gruppe ist die höchste Stelle, die sich mit dem Management der Informations- und Kommunikationstechnologie der MAN Truck & Bus Gruppe befasst. Der CIO jeder MTB-Sparte ist die höchste Stelle, die sich mit dem Management der Informations- und Kommunikationstechnologie einer MTB-Sparte befasst.
Chief Information Security Officer (CISO)	Der **Chief Information Security Officer** der MAN Truck & Bus Gruppe ist verantwortlich für die zentralisierte, konzernweite Steuerung der Informationssicherheit und die Wahrung der unternehmensweiten strategischen Interessen der Informationssicherheit in der MAN Truck & Bus Gruppe. Der MTB-CISO wird vom Corporate CIO der MAN Truck & Bus Gruppe bestellt.
Cloud-Computing	Bezeichnet eine besondere Form des IT-Outsourcings. Eine Cloud-Anwendung ist ein Dienst, der über eine Netzwerkverbindung (z. B. Internet) bereitgestellt wird. Typische Cloud-Modelle sind Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Private und Public Cloud.
Compliance	Compliance bezieht sich auf eine Strategie, die sicherstellt, dass alle gesetzlichen, regulatorischen oder anderen relevanten Standards erfüllt werden.
Erwarteter Wert	Im Risikomanagement ist der **erwartete Wert** der Wert, der durch Multiplikation der Auswirkungen und der Wahrscheinlichkeit nach Maßnahmen erzielt wird.
Falsch negativ	Falsch negativer Zustand ist ein Versäumnis, ein böswilliges Ereignis als solches zu identifizieren. Er suggeriert, dass wir uns in einem sicheren Zustand befinden, während in Wirklichkeit ein Verstoß aufgetreten ist.
Falsch positiv	Falsch positiv ist ein Fehlalarm. Die Aktivität wurde von einem Agenten als böswillige Aktivität gemeldet, aber in einer späteren Phase als legitime Aktivität erkannt.
DSGVO	Verordnung 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung).

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

IKT-Systemkonfiguration	Unter MTB **IKT-Systemkonfiguration** sind alle Einstellungen zu verstehen, die das Verhalten eines MTB IKT-Systems in Bezug auf Verfügbarkeit, Vertraulichkeit und Integrität beeinflussen.
System der Informations- und Kommunikationstechnik (IKT-System)	Die **IKT-Systeme** von MTB umfassen alle Prozesse und Produkte (Hard- und Software), die für die sichere Verarbeitung, Übertragung/Übermittlung und Speicherung von elektronischen Informationen der MAN Truck & Bus Gruppe erforderlich sind. Zu den Produkten (Hard- und Software) gehören auch alle notwendigen passiven Infrastrukturen (Racks, Kabel, Patchpanels usw.), Immobilien (Gebäude, Räume, Flächen usw.) und die zugehörige Technologie (Stromversorgungssysteme, Kühlsysteme, Zutrittskontrollsysteme, Brandschutztechnik usw.).
Informationsressourcen	**Informationsressourcen** umfassen alle Arten von Informationen, unabhängig davon, ob sie digital verarbeitet oder als Bild, Zeichnung, gesprochenes Wort oder sichtbares Objekt dargestellt werden.
Informationseigentümer	Herausgeber, Urheber, Ersteller von Informationen.
Informationssicherheit	Ziel ist es, Informationen vor Risiken für die Vertraulichkeit (Offenlegung gegenüber unbefugten Benutzern), Integrität (unsachgemäße Änderung) und Verfügbarkeit (Nichtzugriff bei Bedarf) zu schützen.
Informationssicherheitsvorfall (IS-Vorfall)	Ein **Informationssicherheitsvorfall** (IS-Vorfall) ist ein Ereignis, das die Verfügbarkeit, Vertraulichkeit oder Integrität von MTB-Informationsressourcen beeinträchtigt und zu einem unannehmbaren Risiko für die MAN Truck & Bus Gruppe, eine Sparte oder das Konzernunternehmen führt.
Informationssicherheitsmanagementsystem (ISMS)	Das **ISMS** ist ein Managementsystem, das darauf abzielt, mit wirtschaftlich vertretbaren Maßnahmen Informationsressourcen in einer dem Risiko entsprechenden Weise zu schützen. Das Informationssicherheitsmanagement der MAN Truck & Bus Gruppe orientiert sich an der Norm ISO 27001.
Information Security Officers (Bereichs-ISO / LE-ISO und P-ISO)	Die Information Security Officers nehmen Aufgaben in ihrem Verantwortungsbereich wahr. Sie stellen den direkten Ansprechpartner für alle Themen rund um die Informationssicherheit für die ISO Organisation und alle Mitarbeiter in ihrem Verantwortungsbereich dar. Ihr Ziel ist es, die Informationssicherheit zu erhöhen und das Bewusstsein für das Thema zu schärfen.
ISO 27001	Die **ISO 27001** „Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen“ legt die Anforderungen an Entwicklung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems (ISMS) unter Berücksichtigung methodisch ermittelter Risiken innerhalb eines definierten Geltungsbereichs fest.
IT-Outsourcing	Dient als Oberbegriff und bezeichnet die Auslagerung von Unternehmensaufgaben oder Strukturen der IT an externe oder interne Dienstleister (z. B. Tochtergesellschaft, externes Rechenzentrum). Dazu gehören z. B. Managed Services, externes Hosting und Cloud-Dienste (IaaS, PaaS, SaaS)

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

IT-System	Technische Infrastruktur zur Ausführung von Softwareanwendungen, die die Ergebnisse schützen und den Berechtigten zur Verfügung stellen.
Schädlicher Code (Malware)	Ein Programm, das mit der Absicht verdeckt in ein anderes Programm eingefügt wird, Daten zu vernichten, zerstörerische oder störende Programme auszuführen oder anderweitig die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, der Anwendungen oder des Betriebssystems des Opfers zu kompromittieren. Malware-Arten • **Ransomware:** Eine Art von Malware, die eine Form der Erpressung darstellt. Sie funktioniert, indem die Festplatte eines Opfers verschlüsselt wird, um ihm den Zugriff auf Schlüsseldateien zu verweigern. Das Opfer muss dann ein Lösegeld zahlen, um die Dateien zu entschlüsseln und wieder auf sie zugreifen zu können. • **Spyware:** Software, die heimlich oder auf unlautere Weise in einem Informationssystem installiert wird, um Informationen über Einzelpersonen oder Unternehmen ohne deren Wissen zu sammeln; eine Art schädlicher Code. • **Virus:** Ein Computerprogramm, das sich ohne Erlaubnis oder Kenntnis des Benutzers selbst kopieren und einen Computer infizieren kann. Ein Virus kann Daten auf einem Cloud-Computer beschädigen oder löschen, E-Mail-Programme verwenden, um sich auf andere Computer zu verbreiten, oder sogar alle Daten auf einer Festplatte löschen. • **Wurm:** Ein Computerprogramm oder Algorithmus, der sich selbst über ein Computernetzwerk repliziert und in der Regel schädliche Aktionen ausführt.
MTB Security Incident Response Team (SIRT)	Das **Security Incident Response Team** (SIRT) innerhalb der MAN Truck & Bus Gruppe legt die Verfahren zum Umgang mit IS-Vorfällen und zur Erfüllung der Verantwortlichkeiten im gesamten Prozess fest, um die negativen Auswirkungen auf den Geschäftsbetrieb von MTB zu minimieren und den Normalbetrieb schnellstmöglich wiederherzustellen.
Maßnahme	Eine **Maßnahme** ist eine Handlung, die geeignet ist, durch Beeinflussung der Auswirkung oder der Wahrscheinlichkeit ein Risiko zu reduzieren oder eine Möglichkeit zu schaffen oder diese zu nutzen.
NDA	Vertraulichkeitsvereinbarung zwischen zwei Parteien zur Regelung des Umgangs mit vertraulichen Informationen.
Opportunity	Eine **Opportunity** ist die Möglichkeit, definierte Umsatz- und Gewinnziele zu übertreffen.
Schutzbedarf	Für jedes Sicherheitsziel kann ein erforderlicher Schutzbedarf als Maß für die Auswirkungen definiert werden, wenn das Sicherheitsziel für diesen Wert von einem Angreifer beeinträchtigt wird. Dieser Schutzbedarf wird in der Regel auf einer Skala mit vier Stufen ausgedrückt: „niedrig“, „mittel“, „hoch“ und „sehr hoch“.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Risiko	Ein Risiko entsteht, wenn eine Bedrohung ein Sicherheitsziel aufgrund einer Schwachstelle wirksam beeinträchtigen kann. Risiken werden anhand einer Risikomatrix bewertet, die die Wahrscheinlichkeit der Bedrohung auf einer Achse und den maximalen Wirkungswert des Vermögenswerts auf der zweiten Achse darstellt. Die Risikowerte aus der Risikomatrix werden in Risikokategorien eingeteilt. Je nach Risikokategorie gibt es Vorgaben zur Risikobehandlung.
Risikobewertung	Die **Bewertung** eines Risikos oder einer Opportunity ist eine Bewertung auf der Grundlage der monetären *Auswirkungen* (auf das Betriebsergebnis, falls es eintreten sollte) und der *Eintrittswahrscheinlichkeit* . Die Bruttobewertung stellt die Ausgangswerte dar, während die Nettobewertung bereits umgesetzte Maßnahmen enthält.
Risikominderung	Eine Minderungsmaßnahme (auch als Gegenmaßnahme oder Sicherheitskontrolle bezeichnet) ist eine Maßnahme zum Schutz eines Vermögenswerts vor einer Bedrohung. Die Minderung verringert entweder die Wahrscheinlichkeit einer Bedrohung (Beispiele: längere Schlüssellänge, verbesserte Zugriffskontrolle) oder die Auswirkungen (Beispiele: Netzwerksegmentierung, Partitionierung des Vermögenswert-Speichers). Folglich wird sich durch die Umsetzung von Gegenmaßnahmen der Risikowert ändern und das Risiko wird in eine andere Risikoklasse eingestuft (HOCH → MITTEL).
Risikoobjekt	Die Einheit, die mit einem Risiko verbunden ist und die einen relevanten Bereich für eine Risikobewertung darstellt. Objekte können unter anderem Systeme, Anwendungen, Prozesse oder Personen sein.
Risikoeigner	Die zuständige Person oder Rolle, die Verantwortung übernimmt und entscheiden kann, wie mit einem Risiko umzugehen ist. Der Risikoeigner ist auch für die kontinuierliche Überwachung und Neubewertung der Risikobewertung verantwortlich.
Risikobehandlung	Im Rahmen der Risikostrategie muss entschieden werden, wie mit Risiken umzugehen ist. Folgende Behandlungsmöglichkeiten gibt es: • Risikovermeidung: Beseitigung der Auswirkungen oder der Wahrscheinlichkeit eines Risikos. • Risikominderung: Umsetzung weiterer Maßnahmen zur Risikominderung auf ein vertretbares Niveau • Risikoakzeptanz: Akzeptanz des Nettorisikos (sofern im Rahmen der Risikobereitschaft) • Risikotransfer: Verlagerung des Risikos auf eine andere Instanz (z. B. Unterzeichnung einer Versicherung) • Risikoteilung: Verteilung des Risikos auf Organisationen
Run Book	Ein Run Book ist eine Zusammenstellung von Routineverfahren und -vorgängen, die der Bediener durchführt. Run Books dienen als Referenz und Anleitung und können entweder in elektronischer oder in physischer

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

	Buchform vorliegen. In der Regel enthält ein Run Book Verfahren zum Starten, Beenden und Verwalten des Prozesses und kann auch Verfahren zur Bearbeitung von Sonderanfragen beschreiben. Ein wirksames Run Book ermöglicht es anderen Teammitgliedern mit der erforderlichen Expertise, den Prozess effektiv selbst zu verwalten.
SDLC	Softwareentwicklungs-Lebenszyklus.
Sicherheitsbewertung	Eine Sicherheitsbewertung überprüft die Umsetzung der Informationssicherheitsanforderungen für ein Unternehmen. So basiert beispielsweise eine standardisierte Bewertung auf dem von der Vereinigung der Automobilindustrie (VDA) entwickelten Fragebogen „Information Security Assessment“ (ISA), der auf den Internetseiten des VDA veröffentlicht ist.
Sicherheitsvorfall	Ein Sicherheitsvorfall ist ein Ereignis, das darauf hindeuten kann, dass die Informationen oder Daten eines Unternehmens kompromittiert wurden oder dass Maßnahmen zum Schutz dieser Informationen oder Daten fehlgeschlagen sind.
Sicherheitsanforderung	Eine Sicherheitsanforderung ist eine konkrete Software- oder Unternehmensanforderung, die zu einem der Sicherheitsziele beiträgt. Beispielsweise könnte darin die Notwendigkeit einer Risikominderung aus der Entscheidung über die Risikobehandlung festgelegt werden.
Sicherheitszonen	Sicherheitszonen sind Bereiche, die Informationen oder Daten schützen, die in darin verarbeitet werden. Sie können physischer (Sicherheitszone im F&E-Bereich) oder logischer Natur (Netzwerkzonen zur Trennung des Büros von den Produktionssystemen) sein.
SLA	Ein Service Level Agreement (SLA, Dienstgütevereinbarung) legt die Erwartungen zwischen dem Dienstleister und dem Dienstleistungsempfänger fest und beschreibt die zu liefernden Produkte oder Dienstleistungen, die zentrale Anlaufstelle für Probleme und die Metriken, anhand derer die Wirksamkeit der erbrachten Dienstleistungen überwacht und genehmigt wird.
Software-Anwendung	Ein Computerprogramm, das Informationen oder Daten verarbeitet, überträgt und/oder speichert. Die Ergebnisse können zur Unterstützung von Geschäftsprozessen verwendet werden.
Fachexperte	Ein Fachexperte (auch bekannt als SME) ist eine Person mit einem umfassenden Verständnis für einen bestimmten Prozess, eine bestimmte Funktion oder Technologie oder einen bestimmten Gerätetyp. Als Fachexperten benannte Personen werden in der Regel von anderen kontaktiert, die mehr über das Thema erfahren oder deren einzigartiges Fachwissen nutzen möchten, um spezifische Probleme zu lösen oder zur Bewältigung bestimmter technischer Herausforderungen beizutragen.
Systembetreiber	Ein Systembetreiber betreibt IT-Systeme und stellt dabei ihre Verfügbarkeit und regelmäßige Wartung sicher.
Bedrohung	Eine Bedrohung ist ein Ereignis oder ein Zustand, das/der das Potenzial hat, ein oder mehrere Sicherheitsziele für Vermögenswerte zu beeinträchtigen, was unerwünschte Folgen hat. Bedrohungen werden als relevant bezeichnet, wenn sie ein oder mehrere Vermögenswerte betreffen. Bedrohungen werden nach der Wahrscheinlichkeit ihres Auftretens bewertet.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

TRATON SE Chief Information Security Officer (CISO)	Der **Chief Information Security Officer** von TRATON SE ist der Vorsitzende des TRATON CISO Boards. Dieses Gremium besteht aus CISOs aller TRATON-Marken.
Richtig positiv	Richtig positiv bezeichnet die erfolgreiche Identifizierung einer böswilligen Aktivität.
Schwachstelle	Eine Schwachstelle ist eine (meist unerwünschte) Eigenschaft eines Informationssystems, die ein oder mehrere Sicherheitsziele beeinträchtigen kann. Während die meisten Schwachstellen auf Design- oder Implementierungsfehler zurückzuführen sind, sind einige unvermeidbar, da sie der Nutzbarkeit des Systems oder der verwendeten Technologie inhärent sind. Ein Beispiel für Letzteres ist die Anfälligkeit offener Netzwerkports für DDoS-Angriffe.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Standard für Informationssicherheit

Ersteller	Steven Rauw erdink Ralf Schlag	**Freigeber**	Andre Wehner	**Version**	3.0
Abt.	FIOS	Abt..	FI	**KSU-Class:**	xx

Gültigkeitsbeginn Datum 01.02.2023	**Geltungsbereich** MAN Truck & Bus SE und deren Tochtergesellschaften	**Genehmigungen (Vorstand)*** **Abgestimmt mit**

* Nur erf orderlich, sofern eine Markenanweisung keiner übergeordneten Markenrichtlinie zuzuordnen ist.

Inhalt

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

1 Zweck

Zweck der Markenrichtlinie MR_13_1 Informationssicherheit ist es, den Standard für Informationssicherheit innerhalb der MAN Truck & Bus Gruppe zu definieren, der von allen Gesellschaften der MAN Truck & Bus Gruppe sowie aller Mitarbeiter Weltweit eingehalten werden muss.

In Anlehnung an die Markenrichtlinie MR_13_1 legt die Markenanweisung MA_13_1_01 - Standard für Informationssicherheit die Grundprinzipien für alle weiteren Regelungen, Sicherheitskonzepte und spezifischen Regelungen fest.

Sie legen die Mindestanforderungen zum Schutz der Informationsgüter der MAN Truck & Bus im Verhältnis zum Risiko fest und beziehen sich auf den Schutz und/oder die Sicherheit aller Informationen, unabhängig von der Form, die sie innerhalb des Unternehmens einnehmen.

Die Markenanweisung MA_13_1_01 berücksichtigt die Anforderungen von ISO27001:2013 Anhang A (vgl. MAN Truck & Bus MR_13_1, Abschnitt 5.6).

2 Geltungsbereich

Diese Markenanweisung gilt weltweit für die MAN Truck & Bus SE und ihre Tochtergesellschaften sowie deren Mitarbeiter[1]. Sie gilt unmittelbar und bedarf keiner Umsetzungsrichtlinie durch einzelne Tochtergesellschaften. Für Gesellschaften, bei denen die MAN Truck & Bus SE die Geltung der Markenanweisung aus rechtlichen Gründen nicht unmittelbar bewirken kann, ist in Abstimmung mit dem Chief Information Security Officer zu klären, inwieweit diese Markenanweisung Anwendung findet. Dies gilt beispielsweise für Gesellschaften, die sich nicht zu 100 % im Anteilsbesitz der MAN Truck & Bus SE befinden und auch nicht durch einen Beherrschungsvertrag mit der MAN Truck & Bus SE verbunden sind (wie z.B. Gesellschaften, die sich im Anteilsbesitz der MAN Finance and Holding S.A. befinden).

Sofern Gesellschaften eigene Regelungen zu diesem Sachverhalt erlassen haben, sind diese umgehend außer Kraft zu setzen. Bis zur Außerkraftsetzung solcher Regelungen oder Teilen von Regelungen gilt diese Markenanweisung vorrangig.

Sollten Regelungen dieser Markenanweisung aufgrund zwingender lokaler Anforderungen nicht umgesetzt werden können, muss die betroffene Gesellschaft unverzüglich den Chief Information Security Officer der MAN Truck & Bus SE informieren, um notwendige Änderungen oder Ergänzungen zu besprechen.

Das Dokument muss mindestens alle drei Jahre überprüft und ggf. angepasst werden.

3 Begriffe und Definitionen

Ein Glossar für das gesamte Regelwerk der Informationssicherheit ist in der Zusatzinformation „Begriffe und Definitionen zur Informationssicherheit“ zu finden.

4 Zielgruppe

Die Markenanweisung MA_13_1_01 - Standard für Informationssicherheit richtet sich an die Verantwortlichen für das Management der Informationssicherheit innerhalb der MAN Truck & Bus Gruppe (vgl. MAN Truck & Bus MR_13_1, Abschnitt 6.1).

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

5 Standard für Informationssicherheit

Das Regelwerk der Informationssicherheit umfasst die Markenrichtlinie MAN Truck & Bus MR_13_1, den MAN Truck & Bus Standard für Informationssicherheit sowie weitere untergeordnete zentrale und dezentrale Regelungen, die die Grundsätze des Informationssicherheitsmanagements (vgl. Markenrichtlinie MAN Truck & Bus MR_13_1) detaillierter regeln.

5.1 Informationssicherheitsmanagement

Die Funktion und der Aufbau eines Informationssicherheits-Managementsystems (ISMS) sind detailliert in der Markenanweisung MA_13_1_02 „Management der Informationssicherheit“ definiert. Dies beinhaltet die Definition der Rollen und Verantwortlichkeiten sowie der Gremien zur Überwachung und Weiterentwicklung des ISMS.

Das Management von Informationssicherheitsrisiken hat auf Basis der Markenrichtlinie MAN Truck & Bus MR_04_8 „Zentrales Risikomanagementsystem der MAN Truck & Bus Gruppe“ zu erfolgen. Dies wird in der Markenanweisung MA_13_1_04 „Informationssicherheits-Risikomanagement“ hinsichtlich der Risiken im Zusammenhang mit Informationsgütern näher definiert.

5.2 Anforderungen an den Schutz von Informationsgütern

Die folgende Tabelle definiert die gruppenspezifischen Anforderungen der MAN Truck & Bus zum Schutz von Informationsgütern. Diese Anforderungen sind auf die jeweiligen Funktionsbereiche zugeschnitten und werden durch zusätzliche Markenanweisungen der MAN Truck & Bus Gruppe konkretisiert.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 1:	Funktionsbereich Trennung von Aufgaben und Verantwortlichkeiten. Zweck Aufgaben und Verantwortlichkeiten so zu verteilen, dass der Missbrauch oder die unbefugte Veränderung von IT-Services und -Systemen so weit wie möglich beschränkt werden.	(1) Im Rahmen des Risikomanagementprozesses sind Aufgaben und Verantwortlichkeiten in Geschäftsprozessen gemeinsam mit kritischen Funktionen von jeder MAN Truck & Bus Konzerngesellschaft zu identifizieren und zu bewerten. Der Missbrauch und die Manipulation von Informationen und IT-Systemen sind durch die Aufgabentrennung weitestgehend zu verhindern.
Artikel 2:	Funktionsbereich Vertraulichkeitsvereinbarungen mit internen/externen Personen und Unternehmen. Zweck Vertraglicher Schutz der Vertraulichkeit sensibler MAN-Informationen.	(1) Jede Gesellschaft der MAN Truck & Bus Gruppe hat sicherzustellen, dass Mitarbeiter, Vertragspartner und Dritte, die im Verantwortungsbereich der MAN Truck & Bus Zugang zu sensiblen Informationen erhalten, Geheimhaltungsvereinbarungen in Bezug auf die Art der verarbeiteten Informationen unterzeichnen. (2) Für die Durchführung von Administratoraufgaben für IT-Systeme sind spezielle Geheimhaltungsvereinbarungen zu unterzeichnen.
Artikel 3:	Funktionsbereich Bedrohungen und Schwachstellen frühzeitig verhindern und erkennen. Zweck Optimiertes Vorgehen bei Sicherheitsvorfällen und Identifizierung potenzieller Gefahren.	(1) Der Umgang mit Informationssicherheitsvorfällen wird durch einen Prozess zum Security Incident Management unterstützt, der in der gesamten MAN Truck & Bus Gruppe definiert und dokumentiert ist. Der Prozess beschreibt das Verhalten von Mitarbeitern, Vertragspartnern und Dritten bei Sicherheitsschwachstellen und Sicherheitsvorfällen, einschließlich eines ggf. zu befolgenden Eskalationspfades. (2) Jede Gesellschaft der MAN Truck & Bus Gruppe hat sicherzustellen, dass das konzernweite Verfahren gemäß der Markenrichtlinie MAN Truck & Bus 13.1 Anweisung 09 „Information Security Incident Management“ umgesetzt wird. Alle Mitarbeiter müssen durch die Gesellschaften der MAN Truck & Bus Gruppe in die Vorgehensweise eingewiesen und darin geschult werden.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 4:	Funktionsbereich Sicherheit bei der Zusammenarbeit mit Lieferanten, Partnern und Kunden. Zweck Informationen, IT-Anwendungen und Infrastrukturen im Verantwortungsbereich von der MAN Truck & Bus, die von externen Parteien genutzt, kommuniziert, verwaltet oder zugänglich gemacht werden, angemessen schützen.	(1) Der Zugang zu MAN-Informationen ist Dritten zu gewähren, wenn ein konkreter Grund vorliegt, und ihr Zugang ist so zu beschränken, dass er überwacht und ordnungsgemäß nachvollzogen werden kann. (2) Die Einhaltung der Anforderungen der MAN Truck & Bus Gruppe an die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, IT-Services und IT-Systemen ist in Verträgen mit externen Dienstleistern hinsichtlich ihrer Aufgaben klar zu definieren. (3) Vereinbarungen oder Verträge mit Dritten, die den Zugang zu und die Verarbeitung von Daten regeln, müssen alle relevanten Sicherheitsanforderungen abdecken.
Artikel 5:	Funktionsbereich Business und IT Service Continuity Management. Zweck Sicherstellung eines optimierten Ansatzes in Bezug auf die IT-Servicekontinuität im Katastrophen- oder Notfall.	(1) Alle Unternehmen der MAN Truck & Bus Gruppe haben einen integrierten Business- und IT Service Continuity Management-Prozess zu etablieren. (2) Basierend auf einer Business-Impact-Analyse sind Notfallmaßnahmen, die für das ermittelte Risiko angemessen sind, zu identifizieren, regelmäßig zu prüfen und anzupassen. Der Schutz von Informationen und personenbezogenen Daten muss auch bei Katastrophen und Notfällen gewährleistet sein.
Artikel 6:	Funktionsbereich Bewertung und Verwaltung des Unternehmensvermögens in Bezug auf Informationssicherheit. Identifizierung und Klassifizierung von Informationsgütern. Zweck Erstellung von Grundlagen zur Beurteilung eines angemessenen Sicherheitsniveaus in der MAN Truck & Bus Gruppe.	(1) Informationsgüter und zugehörige Einrichtungen und Räume der Informations- und Kommunikationstechnik einschl. ihrer Software und Versorgungseinrichtungen müssen eindeutig identifiziert, klassifiziert und als Lagerbestand verwaltet werden. (2) Die Bestandsaufnahme umfasst alle notwendigen Vermögenswerte und ist regelmäßig zu überprüfen und zu verwalten. (3) Alle Informationsgüter und zugehörigen Einrichtungen der Informations- und Kommunikationstechnik einschl. ihrer Software und Versorgungseinrichtungen müssen einem verantwortlichen Daten-/Anlageneigentümer zugeordnet werden. (4) Alle bei und/oder für MAN verarbeiteten und gespeicherten Informationen sind hinsichtlich ihrer Vertraulichkeit, Verfügbarkeit und Integritätsstufe gemäß der MAN Truck & Bus Markenrichtlinie 13.1 Anweisung 03 „Klassifizierung von Informationswerten“ zu klassifizieren.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 7:	Funktionsbereich Bestellung, Anstellung und Einstellung von Personal. Zweck Sicherstellen, dass Mitarbeiter, Auftragnehmer und Drittnutzer ihre Verantwortlichkeiten im Hinblick auf den Schutz der Informationswerte der MAN Truck & Bus SE kennen. Sicherstellen, dass das Personal über die für die beabsichtigten Aufgaben und im Hinblick auf den angemessenen Schutz von Informationen erforderlichen Fähigkeiten verfügt.	(1) Vor Aufnahme einer Tätigkeit und/oder Übernahme einer Funktion in der MAN Truck & Bus Gruppe müssen sich Mitarbeiter, Vertragspartner und Dritte über die für ihre Tätigkeit/Funktionsbereiche relevanten Richtlinien und Leitsätze zur Informationssicherheit informieren. Mitarbeiter, Vertragspartner und Dritte sind verpflichtet, sich in ihren jeweiligen Verträgen zur Einhaltung dieser Regelungen zu verpflichten. (2) Personen, die Zugang zu sensiblen Bereichen mit Relevanz für die Sicherheit von Informationsgütern haben (z. B. Rechenzentrum, Entwicklungsabteilung) oder Zugang zu anderen sensiblen Informationen haben (z. B. personenbezogene Daten), müssen gesondert verpflichtet werden, sich zur Einhaltung der Informations- und Datenschutzanforderungen zu verpflichten.
Artikel 8:	Funktionsbereich Kontrolle und Management des Personals. Zweck Sicherstellen, dass Mitarbeiter, Auftragnehmer und Drittnutzer potenzielle Bedrohungen der Informationssicherheit erkennen, ihre Anforderungen in Bezug auf den Schutz von Informationswerten verstehen und die entsprechenden Richtlinien und Vorgaben einhalten.	(1) Regelmäßige Schulungen zur Informationssicherheit sind auf Arbeitsplatzebene durchzuführen und zu dokumentieren. Mitarbeiter müssen regelmäßig über Änderungen, Neuigkeiten und Bedrohungen informiert werden. (2) Personen mit Aufsichtsfunktion dürfen keine Administratorrollen im gleichen Verantwortungsbereich übernehmen. (3) Mitarbeitern, die Aufgaben mit besonderer Auswirkung auf die Informationssicherheitsinteressen wahrnehmen, ist ausreichend Zeit zur ordnungsgemäßen Erfüllung dieser Aufgaben einzuräumen. (4) Es ist sicherzustellen, dass Ansprechpartner außerhalb der normalen Arbeitszeiten für sicherheitskritische Themen zur Verfügung stehen und rechtzeitig auf beispielsweise Warnungen von z. B. sicherheitskritischen Einrichtungen reagieren. (5) Die MAN Truck & Bus Markenrichtlinie 13.1 zur Informationssicherheit, die dem MAN Truck & Bus Standard für Informationssicherheit und weiteren relevanten Regelungen zugrunde liegt, gilt als offizielles Regelungssystem der MAN Truck & Bus SE als Unternehmen und wird mit Mitarbeitern und Dienstleistern als vertragliche Verpflichtung vereinbart. Verstößen gegen diese Vorschriften sind mit geeigneten arbeitsrechtlichen Maßnahmen und/oder Vertragsstrafen zu begegnen.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 9:	Funktionsbereich Beendigung und Änderung des Beschäftigungsverhältnisses. Zweck Sicherstellung möglichst geringer Auswirkungen für MAN Truck & Bus im Hinblick auf den Schutz von Informationen im Falle, dass Mitarbeiter, Auftragnehmer und Drittnutzer die Organisation oder deren Rolle/Funktion innerhalb der Organisation ändern.	(1) Es ist sicherzustellen, dass im Falle einer Kündigung oder eines Funktionswechsels des Personals Informationen und Vermögenswerte unverzüglich an MAN Truck & Bus zurückgegeben und Zutritts- und Zugriffsrechte unverzüglich widerrufen werden. Dies gilt auch für Dienstleister, soweit diese im Rahmen ihrer Aufgaben für MAN Truck & Bus tätig werden.
Artikel 10:	Funktionsbereich Sicherheitszonen. Zweck Schutz vor unbefugtem Zugriff und Beschädigung oder Unterbrechung von IT-Infrastrukturen und Informationen, die für die Geschäfts- und Produktionsprozesse der MAN Truck & Bus erforderlich sind.	(1) Auf der Grundlage der in einer Risikoanalyse ermittelten Sicherheitsanforderungen sind geeignete Sicherheitszonen zu definieren und einzurichten, die angemessenen Schutz vor unbefugtem Zugang, Umweltbedrohungen, Feuer, Sabotage und Strom- oder Kühlsystemausfällen bieten. (2) Die Sicherheitszonen werden nach dem Zwiebelschalenprinzip eingerichtet. Bei der Verbindung von Zonen mit unterschiedlichen Schutzanforderungen muss der Zugang innerhalb der äußeren Zone beendet, kontrolliert und entsprechend den Schutzanforderungen der inneren Zone neu initiiert werden. (3) Der Zugang zu einer Sicherheitszone darf nur gewährt werden, wenn ein konkreter Bedarf besteht und der Genehmigungsprozess vollständig dokumentiert ist. Der Schutz von Zonen ist auch in Lieferbereichen zu gewährleisten.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 11:	Funktionsbereich Schutz von Einrichtungen der Informations- und Kommunikationstechnik. Zweck Angemessener Schutz der Informations- und Kommunikationstechnologien vor physischen und Umweltgefahren.	(1) Informationen und Komponenten der Informations- und Kommunikationstechnologie sind entsprechend dem erforderlichen Schutzniveau zu sichern. Sie sind unter Einsatz technischer und organisatorischer Maßnahmen vor unbefugtem Zugriff, Umweltgefahren, Stromausfall und Ausfall des Kühlsystems zu schützen. (2) Insbesondere bei der Nutzung mobiler Informations- und Kommunikationsgeräte ist sicherzustellen, dass sensible Informationen nicht gefährdet werden können. Die Notwendigkeit des Schutzes der Informationen ist im Rahmen einer Risikoanalyse zu ermitteln. (3) Strom- und Kühlkreisläufe, die am Informationstransport beteiligt sind, sind vor Beschädigungen zu schützen. (4) Daten- und Kommunikationsleitungen, die vertrauliche oder streng vertrauliche Informationen und/oder Daten transportieren, sind gegen Abfangen zu schützen, und die Verbindungen gegebenenfalls zu verschlüsseln. Daten- und Versorgungsleitungen, die kritisch für den Geschäftsbetrieb sind, sind so auszulegen, dass sie redundante Leitungen umfassen. (5) Sicherheits- und Versorgungseinrichtungen sind so zu warten und instand zu halten, dass ihre Verfügbarkeit und Integrität gewährleistet ist. (6) Für Geräte, die zur Wiederverwendung, Entsorgung oder zum Weiterverkauf bestimmt sind, müssen geeignete Verfahren eingerichtet werden, um sicherzustellen, dass alle vertraulichen oder streng vertraulichen Daten und lizenzierte Software auf den Geräten (feststehend oder mobil) entfernt oder sicher überschrieben werden. Speichermedien sind so zu entsorgen oder zu zerstören, dass eine Wiederherstellung der Daten nicht möglich ist. (7) Es ist sicherzustellen, dass Informations- und Kommunikationseinrichtungen, Software oder Informationen nicht unautorisiert aus den Sicherheitszonen entfernt werden, die für den Betrieb oder die Speicherung bestimmt sind. (8) Im Falle des ortsunabhängigen Arbeitens ist außerdem sicherzustellen, dass geeignete Sicherheitsmaßnahmen gemäß (1) - (6) getroffen werden.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 12:	Funktionsbereich Trennung von Entwicklungs-, Test- und Produktionsumgebungen. Zweck Vermeidung unbeabsichtigter und/oder nicht überwachter Änderungen an Produktionssystemumgebungen.	(1) Entwicklungs- und Testumgebungen müssen von der Produktionsumgebung getrennt werden, um unbefugte Zugriffe auf oder Änderungen an diesen Systemen zu verhindern. (2) Zusätzlich ist für Testnetzwerke ein Sicherheitskonzept zu definieren und eine verantwortliche Person zu benennen. (3) Falls zu Testzwecken auf Dateien mit Produktionsdaten oder Kopien davon zugegriffen werden muss, sind diese wie bei Produktionsprozessen zu schützen. Die Verwendung und die Gründe für die Verwendung sind zu dokumentieren. (4) Testdaten, die vertrauliche oder streng vertrauliche Informationen darstellen, sind unverzüglich nach der Verarbeitung zu löschen. (5) Für den Übergang von Entwicklungs- und Testumgebungen in die Produktion sind umfassende Prozesse zu etablieren, um Fehler in der Produktionsumgebung zu vermeiden.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 13:	Funktionsbereich Gewährleistung eines sicheren MAN Truck & Bus Netzwerks und seiner Schnittstellen. Zweck Schutz vor unbefugter Nutzung, Unterbrechung und unbefugtem Informationsfluss.	(1) Entsprechend dem erforderlichen Schutzniveau müssen die Vertraulichkeit, Verfügbarkeit und Integrität der Daten während des Transports über Netzwerke geschützt werden. Sicherheitsmaßnahmen sind entsprechend der Art und Zusammensetzung des Übertragungsweges innerhalb des Netzwerks (Wireless LAN, WAN, LAN) auszuwählen und müssen den Schutzbedarf berücksichtigen. Vertrauliche Unternehmensdaten müssen bei der Übertragung über öffentliche Netzwerke verschlüsselt werden. (2) Im Hinblick auf die funktionale Nutzung sind alle Netzwerkkomponenten so restriktiv wie möglich zu konfigurieren und vor unberechtigtem Zugriff zu schützen. Es gilt das Least-Privileg-Prinzip. (3) Für Netzwerkkomponenten, die im Zusammenhang mit kritischen Geschäftsprozessen stehen, ist die Notwendigkeit von Überwachungs- und Protokollierungsmaßnahmen zu bewerten und entsprechend einzurichten. Die daraus resultierenden Protokolldaten sind, wenn möglich, automatisch, regelmäßig zu überprüfen. (4) Für Verbindungen von Netzwerken mit unterschiedlichen Sicherheitsanforderungen ist eine Risikoanalyse durchzuführen. Auf dieser Grundlage sind geeignete Prozesse zu definieren und zu dokumentieren. Es ist ein Genehmigungsverfahren einzurichten und zu dokumentieren. (5) Der Zugang zwischen verschiedenen Netzwerken mit unterschiedlichen Sicherheitsstufen ist zu beschränken. Für die Definition der zulässigen Zugriffsmöglichkeiten auf interne Ressourcen ist ein Zonenkonzept zu entwickeln. Die Netzwerke sind entsprechend ihren Sicherheitsanforderungen logisch voneinander zu trennen. (6) Die Sicherheitsmerkmale, Service Levels und Administrationsanforderungen aller Netzwerkdienste müssen identifiziert und dokumentiert werden. Die Einhaltung der geltenden Sicherheitsanforderungen im Netzwerk muss auch Bestandteil von Verträgen mit externen Dienstleistern sein. (7) Der Fernzugriff von Benutzern auf Systeme oder Anwendungen darf nur unter Anwendung einer starken Authentifizierung erfolgen. (8) Alle mit dem MAN-Netzwerk (internes Netzwerk) verbundenen Systeme müssen eindeutig identifizierbar sein.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 14:	Funktionsbereich Schutz von Informationen auf tragbaren Medien. Zweck Verhinderung einer unbefugten Veröffentlichung, Änderung, Entfernung oder Vernichtung von MAN-Informationen.	(1) Beim Austausch von Informationen über tragbare Medien sind diese entsprechend ihrem Schutzbedarf angemessen zu schützen. (2) Wechselmedien sind entsprechend dem Schutzbedarf der gespeicherten Daten zu behandeln. (3) Ist eine Entsorgung erforderlich, ist sicherzustellen, dass vertrauliche Daten so vernichtet werden, dass sie von den Medien nicht wiederhergestellt werden können. (4) Es müssen dokumentierte Verfahren für den sicheren Umgang (Speicherung und Verteilung) mit Informationen (auf tragbaren Medien) festgelegt werden, um unbefugten Zugriff, Missbrauch oder Manipulation zu verhindern. Alle Mitarbeiter müssen auf den richtigen Umgang mit Informationen und Datenträgern gemäß MAN Truck & Bus Anweisung 03 Anlage 1 – Umgang mit klassifizierten Informationen hingewiesen werden (5) Die Mitarbeiter sind verpflichtet, Informationen und Medien beim Verlassen ihres Arbeitsplatzes auch für kurze Zeiträume vor unbefugtem Zugriff zu schützen. (6) Verschlüsselungsmechanismen müssen nach einem kryptographischen Konzept hinsichtlich Anwendung, Schlüsselverwaltung und rechtlichen Aspekten eingerichtet werden.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 15:	Funktionsbereich Schutz der internen und externen Kommunikation. Zweck Verhinderung von Datenlecks oder Offenlegung von MAN-Informationen.	(1) Die Übertragung von Daten innerhalb des MAN Truck & Bus Netzwerks oder von dort nach außen darf nur über freigegebene Schnittstellen entsprechend ihrer jeweiligen Schutzanforderungen erfolgen. Die Regelungen sind zu dokumentieren. (2) Bei der Übermittlung personenbezogener Daten sind die gesetzlichen Vorgaben und die Vorgaben der MAN Truck & Bus Datenschutzrichtlinie einzuhalten. Gegebenenfalls ist vorab die Zustimmung der Person einzuholen, die Gegenstand der übertragenen Daten ist. Gleiches gilt für automatische Aufrufverfahren. (3) Hinsichtlich der Notwendigkeit des Umgangs mit sensiblen Daten durch den Empfänger sind Regelungen und/oder vertragliche Vereinbarungen (Geheimhaltungsvereinbarungen) zu unterzeichnen. (4) Um die Risiken der elektronischen Datenübertragung abzudecken, müssen separate Vorschriften für die Übermittlung sensibler Informationen erlassen werden. Benutzer von E-Mail-Systemen müssen sich der Risiken der elektronischen Kommunikation bewusst sein. Entsprechende Schulungsmaßnahmen sind zu dokumentieren. (5) Absender und Empfänger nicht öffentlicher Daten müssen sicherstellen, dass die Vertraulichkeit der Informationen gewahrt bleibt. Werden die gespeicherten Daten nicht mehr benötigt, müssen diese gelöscht werden. Aufbewahrungspflichtige Daten sind entsprechend zu archivieren. (MAN Truck & Bus Anweisung 03 Anlage 1 – Umgang mit klassifizierten Informationen). (6) Die Speicherung von geschäftlichen E-Mails ist nur in MAN Truck & Bus Umgebungen oder für MAN Truck & Bus betriebenen Umgebungen zulässig. (7) Der Zugriff auf zentral gespeicherte E-Mails über öffentliche Netzwerke ist nur über sichere, überprüfbare Verbindungen gestattet. Es sind sichere Authentifizierungsverfahren zu verwenden. (8) Die Nutzung elektronischer Kommunikationsmittel ist nur für geschäftliche Zwecke und nur über zentral bereitgestellte Internet-Gateways oder voreingestellte Zugangswege gestattet.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 16:	Funktionsbereich Verwaltung von Berechtigungen und Authentifizierungen. Zweck Zuweisung von Zugriffsberechtigungen nach dem Least-Privileg-Prinzip, entsprechende Dokumentation und effektiver Zugriffsschutz.	(1) Es ist eine Richtlinie für Zugriffsrechte zu erstellen und regelmäßig zu überprüfen, die auf Geschäfts- und Sicherheitsanforderungen basiert. (2) Für die An- und Abmeldung von Nutzern ist ein förmliches Verfahren einzuführen. An- und Abmeldungen sind revisionssicher zu dokumentieren. Es ist sicherzustellen, dass Benutzer nur die Berechtigungen erhalten, die den von ihnen auszuführenden Aufgaben entsprechen (Least-Privileg- und Need-to-know-Prinzip). (3) Die Vergabe von administrativen Systemberechtigungen ist restriktiv durchzuführen, sorgfältig zu dokumentieren und regelmäßig zu überprüfen. (4) Privilegierte Benutzerkennungen dürfen nicht für die alltägliche Arbeit genutzt werden. (5) Die Anforderungen an die Authentifizierung sind zentral festzulegen und regelmäßig zu bewerten, und entsprechend den Anforderungen der sich entwickelnden Technologien umzusetzen. Die Authentifizierungsfaktoren sind gemäß den dokumentierten Verfahren zu verwalten. (6) Bestehende Zugangsberechtigungen sind in einem regelmäßigen Intervall zu überprüfen. Diese Intervalle richten sich nach Umfang und Kritikalität der Zugriffsrechte.
Artikel 17:	Funktionsbereich Schutz des elektronischen Geschäftsverkehrs Zweck Schutz von E-Business-Anwendungen.	(1) Die Online-Business-Dienste der MAN Truck & Bus stellen die Autorisierung und Authentifizierung sowie die Vertraulichkeit der gespeicherten oder verarbeiteten Informationen in einem dem Schutzbedarf angemessenen Umfang sicher. (2) Die Integrität von MAN-Informationen, die auf einem öffentlich zugänglichen System zur Verfügung gestellt werden, ist zu schützen, um unbefugte Änderungen zu verhindern.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 18:	Funktionsbereich Schutz von Systemnutzung und Protokollen Zweck Identifizierung der unbefugten Nutzung und Änderung von Systemen und Anwendungen.	(1) Im Falle einer gesetzlichen Nachweispflicht, vertraglicher geschäftlicher Anforderungen oder zum Zwecke der Gefahrenabwehr sind Protokolldaten zu erheben und zu speichern. Dabei ist der Grundsatz der Datensparsamkeit anzuwenden und – soweit bestimmungsgemäß – die Anonymisierung durchzuführen. (2) Es sind Rahmenbedingungen zu schaffen, um Sicherheitsvorfälle und gravierende Unterbrechungen der Geschäftsprozesse der MAN Truck & Bus über alle beteiligten Netzwerke, Systeme und Anwendungen nachvollziehen und auswerten zu können. Die Systemzeiten aller MAN Truck & Bus Systeme und Netzwerkkomponenten sind zu synchronisieren, soweit dies technisch machbar ist. (3) Protokolldaten und -dateien werden für einen bestimmten Zeitraum aufbewahrt, falls sie für künftige Untersuchungen nützlich sein könnten. Protokolle sind vor unbefugtem Zugriff und Manipulation zu schützen und nach Ablauf der festgelegten Aufbewahrungsfrist zu löschen. Personenbezogene Daten werden gelöscht, sobald sie nicht mehr benötigt werden. (4) Mitarbeiter, die an der Erstellung, Verifizierung und Auswertung von Protokolldaten beteiligt sind, müssen eine Vertraulichkeitsvereinbarung unterzeichnen. Die Auswertung personenbezogener Daten wird mit dem zuständigen Datenschutzbeauftragten und dem zuständigen Betriebsrat abgestimmt und gemeinsam durchgeführt. (5) Als Ergebnis einer Risikobewertung sind der notwendige Umfang und Inhalt der Protokollinformationen der identifizierten Systeme auf Basis der gesetzlichen und betrieblichen Anforderungen zu messen. Es müssen mindestens Informationen verfügbar sein, die eine angemessene Verfolgung von Sicherheitsvorfällen ermöglichen. (6) Privilegierte Aktivitäten innerhalb des operativen Managements von IT-Systemen müssen protokolliert und persönlich rückverfolgbar sein. Die Protokollverfahren sind zyklisch von einer unabhängigen Stelle auf Konformität mit den festgelegten Verfahren zu überprüfen. (7) Die Auswertung der Protokolldateien muss so erfolgen, dass sicherheitskritische Ereignisse zeitnah erkannt werden. Es ist darauf zu achten, dass das Personal ausreichend geschult ist, um die Protokollinformationen zu bewerten. (8) Jeder Zugriff auf Systeme, die schutzbedürftige Daten oder Funktionen enthalten, muss durch einen Zugriffsschutz gesichert werden, bei dem die Identität des Benutzers festgestellt wird. (9) IT-Systeme, die Informationen mit spezifischen Schutzanforderungen verarbeiten, müssen sich nach Möglichkeit in einer dedizierten (oder isolierten) Umgebung befinden. Die Isolierung kann physisch oder logisch erfolgen. Informationen dürfen von diesen IT-Systemen nur mit vorher festgelegten Systemen ausgetauscht werden. Für den Fall, dass IT-Systeme und/oder Anwendungen mit hohem Schutzbedarf in heterogenen Umgebungen gespeichert werden müssen, müssen die daraus resultierenden Risiken separat identifiziert und bewertet werden.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 19:	Funktionsbereich Nutzung von Informations- und Kommunikationseinrichtungen und -geräten Zweck Sichere Nutzung von Informations- und Kommunikationseinrichtungen und -geräten.	(1) Nach einer definierten Zeit der Inaktivität des Nutzers muss, soweit technisch möglich, eine automatische Sperrung erfolgen [z.B. Bildschirm, Smartphone]. (2) Der Anschluss von persönlichen Geräten an das interne LAN/WLAN oder Intranet der MAN Truck & Bus Gruppe ist untersagt.
Artikel 20:	Funktionsbereich Dokumentation der Betriebssicherheit der IT relevanten Verfahren, Systemen und Funktionen durch interne und externe IT-Dienstleister sowie Schutz der Betriebssicherheit relevanten Verfahren, Systemen und Funktionen durch interne und externe IT-Dienstleister. Zweck Die Betriebsabläufe werden so dokumentiert, dass bei Ausfall von Personal oder Störung von Systemfunktionen der normale Betriebszustand schnellstmöglich wiederhergestellt werden kann. Die Dokumentation von Betriebsabläufen, Systemkonfigurationen und Betriebsorganisation ist vor unbefugter Einsichtnahme geschützt.	(1) Alle für den ordnungsgemäßen Betrieb notwendigen Verfahren und Systeme sind so zu dokumentieren, dass eine Einschränkung des Geschäftsbetriebs oder der Sicherheit aufgrund fehlender oder fehlerhafter Dokumentation ausgeschlossen ist. (2) Bei Betriebsabläufen, bei denen regelmäßig mehrere Organisationseinheiten oder Dienstleister zusammenarbeiten, sind die Prozesse so zu definieren und zu dokumentieren, dass eine Einschränkung des Geschäftsbetriebs von der MAN oder die Sicherheit der MAN aufgrund unzureichender Definition oder Dokumentation ausgeschlossen ist. (3) Für Dokumentationen, die für betriebliche Prozesse oder die Wiederherstellung kritischer Geschäftsprozesse erforderlich sind, ist sicherzustellen, dass diese bei weitreichenden Störungen weiterhin verfügbar sind (z.B. in gedruckter Form, als verschlüsselte Notfall-CD). (4) Die Dokumentation ist entsprechend dem jeweiligen Schutzbedarf vor unberechtigtem Zugriff zu schützen.
Artikel 21:	Funktionsbereich Change Management für interne IT-Services und Dienstleistungen externer Dienstleister Zweck Möglichst geringe Auswirkungen von Änderungen auf den Geschäftsbetrieb der MAN Truck & Bus.	(1) Änderungen an IT-Services oder Teilen davon (Personal, Prozesse, Hard- und Software) sind stets nach standardisierten Change-Management-Prozessen durchzuführen. Alle Änderungen sind zu dokumentieren. (2) Bei Änderungen werden die Auswirkungen auf die entsprechenden Geschäftsprozesse im Rahmen des Risikomanagementprozesses analysiert, bewertet und dokumentiert.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 22:	Funktionsbereich Kontrollierte Bereitstellung, Überwachung und Auditierung von IT-Services durch externe Dienstleister Zweck Sicherstellung, dass die Leistungen und der Lieferumfang definiert sind und von externen Dienstleistern eingehalten werden können, dass Abweichungen vom vereinbarten Leistungs- oder Lieferumfang identifiziert und bewertet werden, und dass geeignete Gegenmaßnahmen eingeleitet werden.	(1) In mit Dritten und Partnern vereinbarten Serviceverträgen ist neben Funktionalität und Quantität auch der notwendige Schutz der Informationsgüter der MAN hinsichtlich ihrer jeweiligen Verfügbarkeit, Vertraulichkeit und Integrität klar zu regeln. Die MAN-Informationssicherheitsvorschriften sind in geeigneter Form aufzunehmen. (2) Kontrollen und regelmäßige Berichte zur Bestätigung der Einhaltung der Anforderungen zur Informationssicherheit durch Dienstleister sind zu bewerten, festzulegen und vertraglich zu vereinbaren. (3) Leistungen des Lieferanten hinsichtlich Maßnahmen zum Schutz von MAN-Informationsgütern sind durch den jeweiligen Vertragspartner auf Basis von Berichten und Protokollen vollständig zu dokumentieren und müssen zur Überprüfung der Einhaltung des vereinbarten Service Levels geeignet sein. (4) MAN Truck & Bus ist in Verträgen mit Dienstleistern das Recht einzuräumen, Audits bei den jeweiligen Dienstleistern durchzuführen. Dies muss auch für alle Subunternehmer gelten. (5) Werden Betriebsmittel, Geräte oder IT-Systeme von der MAN Truck & Bus oder dem Dienstleister zur Wartung oder Reparatur geschickt, sind alle vertraulichen oder streng vertraulichen Daten auf Datenträgern, physischen oder digitalen Datenträgern vorab zu löschen oder zu vernichten, um eine Wiederherstellung der gespeicherten Daten zu verhindern. Die mit der Reparatur beauftragten Unternehmen sind zur Einhaltung der erforderlichen Vertraulichkeitsvereinbarungen und GHVs verpflichtet. Insbesondere wird festgelegt, dass Daten, die im Rahmen der Wartungsarbeiten extern gespeichert werden, nach Abschluss der Arbeiten zu löschen und für keinen anderen Zweck zu verwenden sind.
Artikel 23:	Funktionsbereich Verwaltung von Kapazitäten für intern und von externen IT-Anbietern bereitgestellte IT-Services Zweck Rechtzeitige Erkennung und Vermeidung von Serviceengpässen.	(1) Die Auslastung aller geschäftskritischen IT-Komponenten ist regelmäßig zu dokumentieren und zu überwachen. (2) Der zukünftige Kapazitätsbedarf wird anhand von Trends und Anforderungen ermittelt, um Engpässe zu vermeiden und eine vorausschauende Planung zu ermöglichen.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 24:	Funktionsbereich Abnahme von Systemen nach definierten Kriterien Zweck Definition und Einhaltung der Systemvoraussetzungen für IT-Services	(1) Es ist sicherzustellen, dass alle neuen IT-Systeme und -Dienste die Anforderungen der MAN Truck & Bus Gruppe an die Informationssicherheit, insbesondere den Standard für Informationssicherheit, erfüllen. Ausnahmen von der Grundsystemhärtung sind zu bewerten und zu dokumentieren. Der MAN Truck & Bus Standard für Informationssicherheit und seine ergänzenden Regelungen stellen Mindestanforderungen für einen ordnungsgemäßen und sicheren Betrieb dar. (3) Im Rahmen der Systemhärtung für geschäftskritische Systeme ist eine sichere Konfiguration zu definieren. Diese dienen als Grundlage für eine sichere Installation und als Checkliste für die Überwachung.
Artikel 25:	Funktionsbereich Datensicherung und -wiederherstellung Zweck Sicherstellung der schnellstmöglichen Wiederherstellung verlorener oder beschädigter Daten sowie Auslagerung von Daten zur Abdeckung von Notfallsituationen.	(1) Für jedes System ist ein Konzept zur Datensicherung und -wiederherstellung zu definieren. In diesem Rahmenkonzept sind auch die Verantwortlichkeiten festzulegen. (2) Werden Daten über verschiedene Systeme verteilt, so ist eine übergreifende Datenkonsistenz sicherzustellen. (3) Kritische Daten werden im Falle einer lokalen oder mobilen Datenhaltung nur als Kopie und/oder nur so lange wie nötig gespeichert. Für die dauerhafte Speicherung dürfen nur zentrale Speichersysteme verwendet werden. (4) Das Datensicherheitskonzept ist mindestens einmal jährlich einer detaillierten Prüfung zu unterziehen. Das Ergebnis der Prüfung ist zu dokumentieren und als Nachweis aufzubewahren. (5) Für das Übertragungsverfahren und den Speicherort von Datensicherungen gelten die gleichen Zugriffsbeschränkungen wie für Systeme, auf denen die Originaldaten gespeichert sind. Weiterhin sind Maßnahmen zu treffen, welche die Datensicherungsmedien vor äußerlichen Einflüssen, z. B. durch Feuer, Wasser, Diebstahl oder Sabotage, schützen. (6) Datenträger zur Datensicherung sind zu katalogisieren und regelmäßig auf Vollständigkeit und Lesbarkeit zu prüfen. Diese Prüfungen sind revisionssicher zu dokumentieren. (7) Die Möglichkeit der Wiederherstellung geschäftskritischer Daten ist mindestens einmal jährlich zu testen. Alle durchgeführten Tests sind zu dokumentieren. (8) Für verschlüsselte Daten oder Datenträger sind spezielle Maßnahmen zu etablieren. (9) Nicht mehr benötigte oder ersetzte Datenträger sind zu vernichten, um die Wiederherstellung der gespeicherten Daten zu verhindern.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 26:	Funktionsbereich Schutz vor Schadsoftware und Mobile Code Zweck Verhinderung des Eindringens und der Verbreitung von Schadsoftware/-code.	(1) Der/die verantwortliche(n) Betreiber erstellt/erstellen ein Virenschutzkonzept, das eine mehrstufige Untersuchung relevanter Elemente, die von Viren befallen werden könnten, durch mindestens zwei verschiedene Produkte verschiedener Hersteller umfasst. (2) Auf jedem Arbeitsplatzrechner oder Server, auf denen Daten gespeichert sind oder über die Daten ausgetauscht werden, ist ein Virenscanner zu installieren. Der Virenscanner wird beim Systemstart automatisch gestartet, lädt Updates nach Möglichkeit automatisch herunter und ist vor einem Beenden während des Prüfvorgangs zu schützen. (3) Für Arbeitsplatzrechner und Server sind unterschiedliche Produkte unterschiedlicher Entwickler zu verwenden. (4) Der gesamte Datenverkehr aus oder innerhalb öffentlicher Netzwerke ist von einem zentralen Virenschutzsystem automatisch auf Viren zu überprüfen. Der Virenschutz muss in der Lage sein, komprimierte oder verschlüsselte Dateien zu überprüfen, soweit dies technisch möglich ist. Der interne E-Mail-Verkehr ist ebenfalls von einem Virenscanner zu überprüfen. Es ist sicherzustellen, dass der Scanner, der für die Virenscans des E-Mail-Verkehrs verwendet wird, nicht selbst Opfer eines Angriffs werden kann. Es sind geeignete Maßnahmen zum Schutz des Virenscanners zu treffen. (5) Für den korrekten Umgang mit virusanfälligen Inhalten in elektronischen Medien wie E-Mails oder Textdateien ist ein Verfahren zu entwickeln und einzuführen. Aktive Inhalte, z. B. in Downloads oder Webangeboten aus öffentlichen Netzwerken, müssen von zentralen Systemen auf systemkonformes Verhalten geprüft werden, bevor sie an das MAN Truck & Bus Netzwerk übertragen werden. (6) Auf den Systemen (Client und Server) dürfen nur die Dienste und Funktionalitäten zur Verfügung gestellt werden, die für den vorgesehenen Zweck erforderlich sind. (7) Sicherheitssoftware und -einstellungen sind so zu konfigurieren, dass keine Änderungen durch den Benutzer möglich sind und die Funktion nicht ausgeschaltet werden kann. (8) IT-Systeme in Produktionsumgebungen (z. B. Industrie-PCs) sind vor schädlicher Software zu schützen, wenn diese Systeme Zugang zum Internet bieten oder mobile Datenträger verwendet werden. Ist dies nicht möglich, müssen diese Systeme gegebenenfalls durch Trennung des Netzwerks und Deaktivierung der Ports isoliert werden. (9) Mobile Geräte mit Zugriff auf Unternehmensdaten der MAN Truck & Bus sind angemessen vor Schadsoftware und dem Ausspionieren von Unternehmensdaten zu schützen.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 27:	Funktionsbereich Beschaffung, Entwicklung und Wartung von Informationssysteme n Zweck Sicherheit bei der Beschaffung, Entwicklung und Wartung von Informationssystem en.	(1) Die Beschaffung informationsverarbeitender Komponenten (Software, Systeme, Netzwerke, Telekommunikationssysteme etc.) unterliegt einem umfassenden Freigabe- und Change-Management-Prozess, der auch ein definiertes Abnahme- und Freigabeverfahren umfasst. Vorgegebene Bestellvorschriften sind einzuhalten. (2) Die Berücksichtigung von Risiken und Schutzbedarf muss integraler Bestandteil der Prozesse zur Beschaffung und Entwicklung neuer informationsverarbeitender Komponenten (Software, Systeme, Netzwerke, Telekommunikationssysteme etc.) sein. (3) Bereits in der Vorauswahlphase ist ein Anforderungskatalog zu erstellen, in dem die Sicherheitsanforderungen formuliert werden. Die Anforderungen müssen dokumentiert und genehmigt werden. Bei Software ist zu dokumentieren, welche Versionen von ausführbaren Dateien freigegeben wurden. (4) Es ist sicherzustellen, dass Hard- und Software nach deren Freigabe nicht verändert oder manipuliert werden können. (5) Sollten trotz intensiver Abnahmeprüfungen Programmfehler im laufenden Betrieb auftreten, so sind diese im Rahmen des Incident/Problem-Managements und des Release Managements zu beheben. (6) Die Installation und/oder Nutzung von nicht freigegebener Software muss untersagt und technisch verhindert werden. Genehmigte Programme müssen regelmäßig auf Änderungen überprüft werden. (7) Die Verwendung von nicht freigegebener Software ist durch regelmäßige Kontrollen festzustellen. Die Ergebnisse dieser Prüfungen sind revisionssicher zu dokumentieren. (8) Bei Software, die intern oder extern entwickelt wird, sind im Entwicklungsprozess die Anforderungen des Standards für Informationssicherheit und weitere Leitprinzipien zu berücksichtigen.
Artikel 28:	Funktionsbereich Kontinuierliche Verbesserung Zweck Identifizierung und Bewertung von Abweichungen und Schwachstellen sowie Sicherstellung ihrer zeitnahen Behebung.	(1) Informationen zu technischen Schwachstellen in den bei der MAN Truck & Bus eingesetzten Systemen und Anwendungen müssen zeitnah eingeholt und ausgewertet werden können. (2) Das Risiko identifizierter Schwachstellen ist zu bewerten. Es sind Maßnahmen zu ergreifen, um dem damit verbundenen Risiko angemessen entgegenzuwirken. (3) Es sind Organisationsstrukturen, Rollen, Verantwortlichkeiten und Kommunikationswege festzulegen. (4) Um Angriffe und Netzwerk-Hacking-Versuche bei der MAN Truck & Bus rechtzeitig zu erkennen und zu bekämpfen, sind Systeme einzusetzen, die Angriffsmuster und Hacking-Versuche automatisch erkennen und/oder verhindern. (5) Die Einhaltung der Vorschriften und Maßnahmen zur Informationssicherheit ist regelmäßig und bei wesentlichen Änderungen mit Auswirkungen auf die Informationssicherheit von einer unabhängigen Stelle zu überprüfen. Die Audits können durch den Auditor, den Datenschutzbeauftragten von der MAN, unabhängige Qualitätsstellen und/oder externe Sachverständige durchgeführt werden.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 28:	Funktionsbereich Kontinuierliche Verbesserung Zweck Identifizierung und Bewertung von Abweichungen und Schwachstellen sowie Sicherstellung ihrer zeitnahen Behebung.	(6) Informationen zu technischen Schwachstellen in den bei der MAN Truck & Bus eingesetzten Systemen und Anwendungen müssen zeitnah eingeholt und ausgewertet werden können. (7) Das Risiko identifizierter Schwachstellen ist zu bewerten. Es sind Maßnahmen zu ergreifen, um dem damit verbundenen Risiko angemessen entgegenzuwirken. (8) Es sind Organisationsstrukturen, Rollen, Verantwortlichkeiten und Kommunikationswege festzulegen. (9) Um Angriffe und Netzwerk-Hacking-Versuche bei der MAN Truck & Bus rechtzeitig zu erkennen und zu bekämpfen, sind Systeme einzusetzen, die Angriffsmuster und Hacking-Versuche automatisch erkennen und/oder verhindern. (10) Die Einhaltung der Vorschriften und Maßnahmen zur Informationssicherheit ist regelmäßig und bei wesentlichen Änderungen mit Auswirkungen auf die Informationssicherheit von einer unabhängigen Stelle zu überprüfen. Die Audits können durch den Auditor, den Datenschutzbeauftragten von der MAN, unabhängige Qualitätsstellen und/oder externe Sachverständige durchgeführt werden.
Artikel 29:	Funktionsbereich Einhaltung der gesetzlichen Rahmenbedingungen Zweck Sicherstellung der Umsetzung gesetzlicher Vorgaben und der frühzeitigen Erkennung von Verstößen.	(1) Für MAN Truck & Bus ist zu identifizieren, welche Gesetze relevante Regelungen zur Informationssicherheit enthalten und welche relevanten Regelungen einzuhalten sind. Auch zu beachtende internationale Gesetze und Vorschriften sind hier enthalten. (2) Zum Schutz der Nutzungsrechte, z. B. proprietärer Softwareprodukte, sind Verfahren zur Einhaltung relevanter rechtlicher, behördlicher und vertraglicher Anforderungen zu implementieren. (3) Gesetzliche Anforderungen an Aufbewahrungs- und Dokumentationspflichten sind zu identifizieren. Entsprechende Anforderungen für deren Einhaltung sind umzusetzen. (4) Es ist ein Verfahren zu etablieren, das sicherstellt, dass auf MAN Truck & Bus Systemen nur Software verwendet wird, für die entsprechende Lizenzen vorliegen. (5) Im Hinblick auf den Datenschutz in der MAN Truck & Bus Gruppe sind die einschlägigen nationalen und internationalen Datenschutzbestimmungen einzuhalten. (6) Durch geeignete Verfahren ist sicherzustellen, dass kein Zugriff über das Internet auf bestimmte Daten erfolgt, der gegen Gesetze oder andere Vorschriften verstößt oder von MAN Truck & Bus Gesellschaften nicht gewünscht wird.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Artikel	Funktion und Zweck	Regelung
Artikel 30:	Funktionsbereich Einhaltung des Regelwerkes zur Informationssicherheit der MAN Truck & Bus Zweck Sicherstellung der Umsetzung und Einhaltung der Informationssicherheitsvorschriften durch die Mitarbeiter im Konzern, Feststellung von Abweichungen und Einleitung geeigneter Maßnahmen.	(1) Die Verantwortlichen für Informationssicherheit (CISO/ISO) müssen sicherstellen, dass die MAN-Informationssicherheitsvorschriften bei der MAN korrekt angewendet werden, um die Einhaltung von Sicherheitsvorschriften und -standards zu erreichen. (2) Bei Abweichungen von oder Verstößen gegen das Regelwerk der MAN Truck & Bus aus Gründen der Informationssicherheit sind Gründe zu ermitteln, Maßnahmen zur Verhinderung von Verstößen und Abweichungen zu erarbeiten und einzuführen, sowie die Wirksamkeit dieser Maßnahmen zu überprüfen. (3) Es ist ein Berichtswesen zu entwickeln, das die Transparenz der Umsetzung des Regelwerkes zur Informationssicherheit der MAN Truck & Bus innerhalb der Gruppe und bei Dienstleistern sicherstellt.
Artikel 31:	Funktionsbereich Verifikation der Informationssicherheit Zweck Erkennung von Abweichungen in der geplanten Umsetzung, Feststellung der Nichteinhaltung von Informationssicherheitsvorschriften.	(1) Alle Arbeitsprozesse, Betriebsmittel, Geräte und IT-Systeme sind durch regelmäßige Audits auf Einhaltung des Regelwerkes zur Informationssicherheit der MAN Truck & Bus zu überprüfen. (2) Diese Nachweise sind nachvollziehbar zu dokumentieren und die Ergebnisse vor unbefugter Einsichtnahme zu schützen. (3) Es ist ein Verifizierungsplan zu erstellen, um die Vollständigkeit der Verifizierungsaspekte und der Verifizierungsgegenstände sicherzustellen. (4) Die technische Informationssicherheit ist durch Maßnahmen wie regelmäßige Penetrationstests oder Sicherheitsaudits zu bewerten. (5) Die Informationssicherheit des Unternehmens ist durch regelmäßige Prozessaudits wie Selbstbewertungen, Vor-Ort-Bewertungen, Managementbewertungen oder Bewertungen durch externe Partner zu überprüfen.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

6 Änderungen

Version 3.0

- Änderungsprotokoll hinzugefügt
- Umbenennung
- Änderung von Rollen und Verantwortlichkeiten
- Angepasste Referenzen zur Berücksichtigung der neuen Richtlinienstruktur

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Klassifizierung von Informationswerten

Ersteller	Steven Rauw erdink Ralf Schlag	**Freigeber**	Andre Wehner	**Version**	3.0
Abt.	FIOS	Abt..	FI	**KSU-Class:**	xx

Gültigkeitsbeginn Datum 01.02.2023	**Geltungsbereich** MAN Truck & Bus SE und deren Tochtergesellschaften	**Genehmigungen (Vorstand)*** **Abgestimmt mit**

* Nur erforderlich, sofern eine Markenanweisung keiner übergeordneten Markenrichtlinie zuzuordnen ist.

Inhalt

Anlagen

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

1 Zweck

Alle Informationsbestände der MAN Truck & Bus Gruppe müssen vom deren Besitzer und/oder Business Owner des Prozesses unter Bezugnahme auf Vertraulichkeit, Integrität und Verfügbarkeit klassifiziert und gekennzeichnet werden. Klassifizierungen müssen so dokumentiert werden, dass die Rückverfolgbarkeit gewährleistet ist. Eine Validierung der Klassifizierung muss regelmäßig entsprechend dem Lebenszyklus des jeweiligen Informationsbestände durchgeführt werden.

Zweck dieser Markenanweisung ist es, die verbindlichen Grundsätze für die Klassifizierung von Informationswerten und den Umgang mit Informationen gemäß der MAN Truck & Bus Markenrichtlinie MR_13_1 Informationssicherheit festzulegen.

2 Geltungsbereich

Diese Markenanweisung gilt weltweit für die MAN Truck & Bus SE und ihre Tochtergesellschaften sowie deren Mitarbeiter[1]. Sie gilt unmittelbar und bedarf keiner Umsetzungsrichtlinie durch einzelne Tochtergesellschaften. Für Gesellschaften, bei denen die MAN Truck & Bus SE die Geltung der Markenanweisung aus rechtlichen Gründen nicht unmittelbar bewirken kann, ist in Abstimmung mit dem Chief Information Security Officer zu klären, inwieweit diese Markenanweisung Anwendung findet. Dies gilt beispielsweise für Gesellschaften, die sich nicht zu 100 % im Anteilsbesitz der MAN Truck & Bus SE befinden und auch nicht durch einen Beherrschungsvertrag mit der MAN Truck & Bus SE verbunden sind (wie z.B. Gesellschaften, die sich im Anteilsbesitz der MAN Finance and Holding S.A. befinden).

Sofern Gesellschaften eigene Regelungen zu diesem Sachverhalt erlassen haben, sind diese umgehend außer Kraft zu setzen. Bis zur Außerkraftsetzung solcher Regelungen oder Teilen von Regelungen gilt diese Markenanweisung vorrangig.

Sollten Regelungen dieser Markenanweisung aufgrund zwingender lokaler Anforderungen nicht umgesetzt werden können, muss die betroffene Gesellschaft unverzüglich den Chief Information Security Officer der MAN Truck & Bus SE informieren, um notwendige Änderungen oder Ergänzungen zu besprechen.

Das Dokument muss mindestens alle drei Jahre überprüft und ggf. angepasst werden.

3 Begriffe und Begriffsbestimmungen

Ein Glossar für das gesamte Regelwerk der Informationssicherheit ist in der Zusatzinformation „Begriffe und Definitionen zur Informationssicherheit“ zu finden.

4 Zielgruppe

Die MAN Truck & Bus Markenanweisung MA_13_1_03 zur Klassifizierung von Informationswerten richtet sich an die Verantwortlichen für das Management der Informationssicherheit innerhalb der MAN Truck & Bus Gruppe (vgl. MTB Markenrichtlinie MR_13_1, Abschnitt 6.1).

Die sich aus dieser Anweisung für externe Dienstleister ergebenden Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, IT-Diensten und IT-Systemen sind in den Verträgen mit externen Dienstleistern, bezogen auf deren Aufgaben, explizit zu verankern.

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

5 Allgemeine Grundsätze

Informationswerte können in unterschiedlicher Form und auf unterschiedlichen Medien zur Verfügung stehen, wie z. B.:

- elektronisch (z. B. Partnersysteme, Kundeninformationen, Bestandsdaten, E-Mails, Internet)
- auf Datenträgern (z. B. externe Festplatten, CDs, DVDs, USB-Sticks, Chipkarten)
- in Papierform (z. B. Schriftstücke, Dokumente, Fax-Ausdrucke, Zeichnungen, Veröffentlichungen)
- im menschlichen Gedächtnis (z. B. Expertenwissen über einen Geschäftsprozess)
- mündlich (z. B. persönliche Besprechungen, Telefongespräche, Mitteilungen, Sprachaufzeichnungen, Vorträge)
- visuell (z. B. Bilder, Videos)

Alle Informationen sind unabhängig von ihrer Erscheinungsform gleichermaßen und je nach ihrer Klassifizierung zu schützen.

6 Klassifizierung von Informationswerten

6.1 Allgemeine Anforderung

Informationswerte in der MAN Truck & Bus Gruppe sind angemessen, wirksam und umfassend vor den jeweils identifizierten Bedrohungen zu schützen. Die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit müssen in einer angemessenen und wirtschaftlich sinnvollen Weise gewährleistet werden.

Als Grundlage einer einheitlichen Einstufung und Bewertung bzgl. der Schutzziele werden die Schutzbedarfe für die Informationswerte der MAN Truck & Bus Gruppe anhand der nachfolgend detaillierten Sicherheitsstufen festgelegt.

Beim Umgang mit Informationen, die eine bestimmte Geheimhaltung erfordern, z. B. militärische Informationen, ist gemäß den Anforderungen lokaler Richtlinien, z. B. des Geheimschutzhandbuchs des deutschen Bundesministeriums für Wirtschaft und Technologie, zu verfahren.

Alle Informationswerte der MAN Truck & Bus Gruppe müssen vom Eigentümer der Informationen und/oder dem Verantwortlichen für den Geschäftsprozess hinsichtlich ihrer Vertraulichkeit, Integrität und Verfügbarkeit klassifiziert und gekennzeichnet werden. Die Klassifizierungen sind nachvollziehbar zu dokumentieren und dem Lebenszyklus des jeweiligen Informationswertes entsprechend in regelmäßigen Abständen zu überprüfen.

6.2 Fragen zur Hilfestellung bei der Klassifizierung

Die folgenden Fragen können bei der Klassifizierung eigener Informationen unterstützen und die Zuordnung zu den Klassifizierungsstufen erleichtern:

- Würden rechtliche, finanzielle, betriebliche, Datenschutz- und/oder Sicherheitsprobleme auftreten, wenn die Informationen in die Hände von Mitbewerbern gelangen? Wenn ja, wie würden Sie die Auswirkungen bewerten?
- Gäbe es einen möglichen Verlust oder Schaden für die Geschäftsbereiche der MAN Truck & Bus Gruppe, wenn die Informationen nicht mehr zugänglich, nicht mehr verfügbar oder vernichtet sind? Wenn ja, wie würden Sie diesen Verlust/Schaden bewerten?
- Sind Auswirkungen auf das Vertrauen der Kunden in die MAN Truck & Bus Gruppe, unser öffentliches Image oder das Verhalten unserer Aktionäre zu erwarten?

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

- Wäre der unbeabsichtigte Verlust oder die Zerstörung der Informationen mit hohen Kosten für die MAN Truck & Bus Gruppe, die Sparte oder das Konzernunternehmen verbunden?
- Könnte die Veröffentlichung dieser Informationen zu Rechtsverstößen, anderen rechtlichen Konsequenzen oder der Verletzung von sonstigen regulatorischen oder vertraglichen Verpflichtungen führen?
- Könnte der Missbrauch oder die Veröffentlichung dieser Informationen zu Ermittlungshandlungen durch Behörden führen?
- Welche Auswirkungen hätte der unbeabsichtigte Verlust oder die unbeabsichtigte Vernichtung dieser Informationen auf die Motivation der Mitarbeiter der MAN Truck & Bus Gruppe? Können die Informationen bei Vernichtung oder Verlust wiederhergestellt werden, und welcher Aufwand (zeitlich und finanziell) wäre dafür notwendig?
- Welche möglichen Folgen hätte eine Beeinträchtigung der Informationsintegrität? Wie würden Sie mögliche finanzielle, betriebliche, Datenschutz- und/oder Sicherheitsfolgen bewerten?
- Welche Auswirkungen hätte es, wenn ein Informationswert nicht oder nicht mehr verfügbar wäre? Gäbe es finanzielle, betriebliche, Datenschutz- und/oder Sicherheitsfolgen?

6.3 Vertraulichkeit

Informationen, die nicht zur allgemeinen Veröffentlichung bestimmt sind, dürfen nur Personen zugänglich gemacht werden, die entsprechend dafür berechtigt sind. Um die erforderliche Vertraulichkeit zu erreichen, muss der Zugang zu Informationen verwaltet und die Offenlegung von Informationen gegenüber nicht berechtigten Personen, Einrichtungen oder Prozessen verhindert werden, um das geistige Eigentum sowie Kunden- und Mitarbeiterinformationen von MAN Truck & Bus SE zu schützen. Dazu dienen folgende Methoden:

- Bewertung, Klassifizierung
- Authentifizierung
- Verschlüsselung

Die Vertraulichkeit von Informationen muss vom Eigentümer der Informationen und/oder vom Verantwortlichen für den Geschäftsprozess in eine der folgenden Schutzbedarfe eingestuft werden: „Öffentliche Informationen“, „Interne Informationen“, „Vertrauliche Informationen“ oder „Streng vertrauliche Informationen“.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Vertraulichkeitsstufen

Sicherheitsstufe	Bedeutung	Behandlung	Beispiele[1]
Stufe 1: **Öffentliche** **Informationen**	• Informationen werden als öffentlich eingestuft, wenn sie keinen Beschränkungen unterliegen und vom Unternehmen in den Medien veröffentlicht werden können • Öffentliche Informationswerte sind zur Verbreitung oder Nutzung im öffentlichen (z. B. Presse) oder virtuellen Raum (Internet allgemein, z. B. Foren oder Facebook) bestimmt. Dies bedarf der vorherigen Freigabe durch die zuständigen Stellen bei MAN Truck & Bus. • Öffentliche Informationen stellen bei ihrer Verbreitung oder Nutzung im öffentlichen (z. B. Presse) oder virtuellen Raum (Internet allgemein, z. B. Foren oder Facebook) kein Risiko für MAN Truck & Bus dar.	• Besondere Schutzmaßnahmen sind nicht erforderlich. • Werden Informationswerte als „öffentlich“ dokumentiert, muss sichergestellt werden, dass keine Informationen höherer Sicherheitsstufen offengelegt werden können. • Es ist mit den berechtigten Einheiten (z. B. Corporate Communications) abzustimmen, welche Informationen als öffentlich eingestuft sind, bevor sie verbreitet oder veröffentlicht werden. • Die offizielle Vorgehensweise zur Freigabe öffentlicher Daten muss eingehalten werden. • Das Wort „öffentlich“ muss als Kennzeichnung auf allen Positionen vermerkt sein.	• Pressemeldungen nach Veröffentlichung • Produktkatalog für Kunden • Werbefilme • Produktbeschreibungen • Inhalte des Internetauftritts • Werbefotos • Pressemeldungen • Publikationen in Zeitschriften und Büchern • Image-Broschüren • Präsentationen bei öffentlichen Meetings

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

[1] Die Klassifizierung eines bestimmten Informationswerts muss auf Einzelfallbasis erfolgen. Die hier genannten Beispiele sind daher nicht bindend.

Sicherheitsstufe	Bedeutung	Behandlung	Beispiele[2]
Stufe 2: **Interne** **Informationen**	• Informationen werden als intern eingestuft, wenn sie ausschließlich für den internen Gebrauch und nicht für die Öffentlichkeit bestimmt sind. • „Interne“ Informationen haben bei Offenlegung oder unberechtigter Kenntnisnahme begrenzte negative Auswirkungen auf die MAN Truck & Bus Gruppe. **„Intern“ ist die Standard-Sicherheitsstufe für alle Informationen in der MAN Truck & Bus Gruppe, die nicht anders eingestuft bzw. gekennzeichnet sind.**	• Es ist unbedingt darauf zu achten, dass keine Personen außerhalb der MAN Truck & Bus Konzernunternehmen Zugriff auf die Informationen erhält. Dies gilt für die Verarbeitung, Speicherung/Aufbewahrung, den Transport/Versand und die Entsorgung/Vernichtung. • Als intern eingestufte Informationen dürfen nur innerhalb von MAN Truck & Bus SE und der zugehörigen Mehrheitsbeteiligungsgesellschaften verbreitet werden. Externe Dienstleister müssen eine gesonderte Vertraulichkeitserklärung unterzeichnen, bevor ihnen Zugriff auf „interne“ Informationen gewährt wird. Aus dieser Erklärung müssen Nutzungsbedingungen sowie die Einstufung der Informationen als intern und ihr Schutzbedarf hervorgehen. Der Zugriff auf Systeme, die interne Daten bereitstellen, erfordert mindestens eine schwache Authentifizierung.	• Glossar • Geschäftliche E-Mail Adresse • Abteilungsvertretung • IT-Sicherheitsrichtlinien • Inhalte des Intranets • Markenrichtlinien und -anweisungen • Interne informelle Präsentationen • Mitarbeiterinformationen • Betriebsvereinbarungen

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

[2] Die Klassifizierung eines bestimmten Informationswerts muss auf Einzelfallbasis erfolgen. Die hier genannten Beispiele sind daher nicht bindend.

Sicherheitsstufe	Bedeutung	Behandlung	Beispiele[3]
Stufe 3: **Vertrauliche Informationen**	• Informationen werden als vertraulich eingestuft, wenn die Offenlegung gegenüber unberechtigten Dritten die Erreichung der Produkt- und Projektziele gefährden könnte. Diese Informationen dürfen daher nur einem begrenzten Kreis von berechtigten Personen zugänglich gemacht werden. • Vertrauliche Informationen sind nur für einen begrenzten Personenkreis, in der Regel MAN-intern, und nicht für die Öffentlichkeit bestimmt. • Vertrauliche Informationen haben bei Veröffentlichung oder Weitergabe an unberechtigte Dritte erhebliche negative Auswirkungen auf MAN Truck & Bus SE als Unternehmen (z. B. finanziell, bezüglich der Konkurrenzfähigkeit oder aus rechtlicher Sicht). Personenbezogene Daten sind stets als vertraulich einzustufen.	• Vertrauliche Informationen dürfen nur an eine vom Eigentümer der Informationen und/oder vom Geschäftsinhaber bzw. Prozessverantwortlichen benannte Gruppe von Mitarbeitern weitergegeben werden, die diese Informationen zur Erfüllung ihrer Aufgaben benötigen („Need-to-know"-Prinzip). Die Informationen dürfen nur nach Rücksprache mit dem Eigentümer der Informationen und/oder dem Geschäftsinhaber/Prozessverantwortlichen kopiert werden. • Externe Dienstleister müssen eine gesonderte Vertraulichkeitserklärung unterzeichnen, bevor ihnen Zugriff auf vertrauliche Informationen gewährt wird. Der Zugriff auf Systeme, die vertrauliche Daten bereitstellen, erfordert eine starke oder sehr starke Authentifizierung.	• Haushaltsplan • Rollen und Rechte • Wohnanschrift • Personenbezogene Daten, z. B. Gehaltsinformationen • Geschäftsberichte einzelner Konzernunternehmen • Informationen aus der Entwicklung • Daten der internen Finanzbuchhaltung • Audit-Berichte

[3] Die Klassifizierung eines bestimmten Informationswerts muss auf Einzelfallbasis erfolgen. Die hier genannten Beispiele sind daher nicht bindend.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Sicherheitsstufe	Bedeutung	Behandlung	Beispiele[4]
4. Stufe: **Streng Vertrauliche Informationen**	• Informationen werden als streng vertraulich eingestuft, wenn die Offenlegung gegenüber unberechtigten Dritten die Erreichung der Unternehmensziele langfristig gefährden könnte. Diese Informationen müssen daher auf einen äußerst eingeschränkten Verteilerkreis beschränkt werden und unterliegen strengen Kontrollen. • Streng vertrauliche Informationen sind nur für einzeln benannte Personen vorgesehen. • „Streng vertrauliche“ Informationen haben bei Offenlegung oder unberechtigter Kenntnisnahme äußerst negative Auswirkungen auf die MAN Truck & Bus Gruppe, ihre Aktionäre, Geschäftspartner oder Mitarbeiter. (z. B. ist die Existenz einer oder mehrerer MAN Truck & Bus Unternehmen gefährdet, oder es sind erhebliche rechtliche Konsequenzen für MAN Truck & Bus SE zu erwarten).	• Streng vertrauliche Informationen/Daten dürfen nur vom Eigentümer der Informationen und/oder vom Geschäftsinhaber/Prozessverantwortlichen jeweils namentlich genannten Personen zugänglich gemacht werden. Vor der Weitergabe muss sichergestellt werden, dass die Identität des Empfängers belegbar geprüft wurde. • Die Entscheidung zur Weitergabe oder Weiterverarbeitung der Informationen obliegen dem Eigentümer auf Einzelfallbasis. • Es ist die Unterzeichnung einer gesonderten Vertraulichkeitserklärung erforderlich, bevor Zugriff auf streng vertrauliche Informationen gewährt werden kann. • Informationen dieser Art dürfen nicht kopiert werden. Der Eigentümer der Informationen und/oder der Geschäftsinhaber/Prozessverantwortliche muss jede vorhandene Kopie mit einer Seriennummer für Papierdokumente und Datenträger kennzeichnen. Bei elektronischer Verbreitung kann auf diese Nummerierung verzichtet werden, wenn ein Übertragungsnachweis erbracht wird. Die Weitergabe streng vertraulicher Informationen an Dritte, z. B. Geschäftspartner, ist unzulässig. Ist dies im Einzelfall unvermeidbar, sind die Modalitäten unter Einbeziehung der Rechtsabteilung festzulegen. Der Zugriff auf Systeme, die streng vertrauliche Daten bereitstellen, erfordert eine sehr starke Authentifizierung.	• Gesundheitsdaten • Politische, religiöse und philosophische Überzeugungen von Einzelpersonen • Personenbezogene Daten zur ethnischen und kulturellen Herkunft • Sexualität • Gewerkschaftsmitgliedschaft • Designmodelle vor dem SOP • Tarninformationen bestimmter Modelle • Konzerngeschäftsberichte vor Veröffentlichung • Geschäftsgeheimnisse • Insiderinformationen • Betriebsratsprotokolle • Aufsichtsratsprotokolle

[4] Die Klassifizierung eines bestimmten Informationswerts muss auf Einzelfallbasis erfolgen. Die hier genannten Beispiele sind daher nicht bindend.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

6.4 Integrität

Die Integrität von Informationen ist wichtig, um eine fehlerfreie Verarbeitung und den Schutz vor unbefugten Änderungen zu gewährleisten. Um eine geforderte Integritätsstufe zu erreichen, müssen Änderungen von Informationen überwacht und unbemerkte Änderungen vermieden werden. Für Änderungen ist eine entsprechende Berechtigungsstufe erforderlich. Änderungen können mithilfe folgender Methoden gesteuert werden:

- Änderungsprotokoll
- Änderungsgenehmigung
- Prüfsumme

Die Integrität von Informationen wird vom Eigentümer der Informationen und/oder vom Geschäftsinhaber/Prozessverantwortlichen in eine der folgenden Sicherheitsstufen eingestuft: „Ungesicherte Integrität“, „Gesicherte Integrität“, „Prüfbare Integrität“ und „Signierte Integrität“.

Integritätsstufen

Sicherheitsstufe	Bedeutung	Behandlung	Beispiele[5]
1. Stufe: Ungesicherte Integrität	• Informationen/Daten ungesicherter Integrität sind Informationen, die nur einmalig verwendet werden oder deren Wiederherstellung ohne Aufwendungen möglich ist. • Eine nicht autorisierte Änderung hat keine Auswirkungen auf den Geschäftsbetrieb der MAN Truck & Bus Gruppe.	• Bei Informationen/Daten der Einstufung „ungesicherte Integrität“ sind keine besonderen Maßnahmen zur Wahrung der Integrität oder Verbindlichkeit vorzusehen.	• Speisepläne • Kopien öffentlicher Informationen

[5] Die Klassifizierung eines bestimmten Informationswerts muss auf Einzelfallbasis erfolgen. Die hier genannten Beispiele sind daher nicht bindend.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Sicherheitsstufe	Bedeutung	Behandlung	Beispiele[6]
2. Stufe: Gesicherte Integrität	• Informationen/Daten gesicherter Integrität sind Informationen, die mehrfach verwendet werden oder deren Wiederherstellung bei nicht autorisierter Änderung mit moderaten Aufwendungen möglich ist. • Eine nicht autorisierte Änderung der Informationen/Daten hat begrenzte negative Auswirkungen auf eine Sparte oder ein Konzernunternehmen der MAN Truck & Bus Gruppe und nur sehr geringe Auswirkungen auf MAN Truck & Bus SE. **„Gesicherte Integrität" ist die Standard-Sicherheitsstufe für alle Informationen in der MAN Truck & Bus Gruppe, die nicht anders eingestuft bzw. gekennzeichnet sind.**	• Informationen/Daten der Einstufung „gesicherte Integrität" müssen mit Vorsichtsmaßnahmen zum Schutz vor Änderungen durch Unbefugte ausgestattet sein. • Dies gilt für die Verarbeitung, Speicherung/Aufbewahrung und den Transport/Versand. • Die Sicherstellung der Integrität und Verbindlichkeit von Informationen erfolgt in dieser Stufe in der Regel durch die eingesetzten Systeme bzw. Anwendungen. • Änderungen dürfen nur von einem festgelegten Personenkreis vorgenommen werden.	• Projektarbeitsdateien • Besprechungsprotokolle
3. Stufe: Prüfbare Integrität	• Informationen/Daten mit prüfbarer Integrität sind Informationen, die vielfach verwendet werden oder deren Wiederherstellung bei nicht autorisierter Änderung nur mit sehr erheblichem Aufwand möglich ist. • Eine nicht autorisierte Änderung der Informationen/Daten hat erhebliche negative Auswirkungen auf MAN Truck & Bus SE.	• Informationen/Daten der Einstufung „prüfbare Integrität" müssen mit Vorsichtsmaßnahmen zum Schutz vor Änderungen durch Unbefugte ausgestattet sein. • Bei Informationen/Daten der Einstufung „prüfbare Integrität" muss es möglich sein, Verletzungen der Integrität festzustellen. • Die Verbindlichkeit wird über die prüfbare Dokumentation einer eindeutigen Kennung sichergestellt. • Änderungen werden nachvollziehbar dokumentiert und dürfen nur von einem begrenzten, berechtigten und eindeutig identifizierbaren Personenkreis durchgeführt werden.	• Arbeitsanweisungen • Prüfberichte • Sicherheitsanweisungen • Sitzungsprotokolle des Betriebsrats • Produktbeschreibungen • Inhalte des Internetauftritts • Pressemeldungen • Image-Broschüren • E-Mails

[6] Die Klassifizierung eines bestimmten Informationswerts muss auf Einzelfallbasis erfolgen. Die hier genannten Beispiele sind daher nicht bindend.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Sicherheitsstufe	Bedeutung	Behandlung	Beispiele[7]
4. Stufe: Signierte Integrität	• Informationen/Daten signierter Integrität sind Informationen, die vielfach verwendet werden oder deren Wiederherstellung bei nicht autorisierter Änderung nicht mehr möglich ist. • Eine nicht autorisierte Änderung von Informationen/Daten hat äußerst negative Auswirkungen auf die MAN Truck & Bus Gruppe, ihre Aktionäre, Geschäftspartner oder Mitarbeiter (z. B. wenn die Existenz einer oder mehrerer MAN Truck & Bus Unternehmen gefährdet ist, oder es sind erhebliche rechtliche Konsequenzen für MAN Truck & Bus SE zu erwarten).	• Diese Informationen/Daten müssen mit Vorsichtsmaßnahmen zum Schutz vor Änderungen durch Unbefugte ausgestattet sein. • Die Informationen/Daten müssen mit einer persönlichen oder digitalen Signatur zur Integritätsprüfung versehen werden. • Aktivitäten wie Entwurf, Prüfung, Genehmigung, Versand oder Eigentum von Informationen müssen eindeutig dokumentiert werden. • Jede Änderung muss nach einem eindeutig dokumentierten Verfahren nachvollziehbar und prüfbar sein und darf nur namentlich benannten und eindeutig identifizierbaren Personen möglich sein.	• Markenrichtlinien • Markenrichtlinienanweisungen • Betriebsvereinbarungen • Geschäftsberichte • Bilanzen • Dokumentierte Entwicklungsstände

6.5 Verfügbarkeit

Informationen müssen innerhalb eines vereinbarten Zeitrahmens verfügbar gemacht werden können. Die Informationen müssen von ihrem Eigentümer und/oder vom Geschäftsinhaber/Prozessverantwortlichen in eine der folgenden Schutzbedarfe eingestuft werden: „Anforderung nicht definiert“, „Verfügbar“ und „Hochverfügbar“.

Um eine hohe Verfügbarkeitsstufe zu erreichen, sollte die Verfügbarkeit überwacht werden. Die rechtzeitige Wiederherstellung nach Ausfällen kann entscheidend sein. Dabei helfen folgende Methoden:

- Serviceüberwachung

[7] Die Klassifizierung eines bestimmten Informationswerts muss auf Einzelfallbasis erfolgen. Die hier genannten Beispiele sind daher nicht bindend.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

- Service-Level-Agreement (SLA)
- Failover-Plan

Der Informationsverantwortliche (Eigentümer der Informationen) muss die Kritikalität der Verfügbarkeit von Informationen ermitteln und dokumentieren. Informationen jeder Vertraulichkeitsstufe können verfügbarkeitskritisch sein.

Verfügbarkeitsstufen

Sicherheitsstufe	Bedeutung	Behandlungs-	Beispiele[8]
1. Stufe: Anforderung nicht definiert	• Die Nichtverfügbarkeit der Informationen hat keine Auswirkungen auf den Geschäftsbetrieb eines MAN Truck & Bus Unternehmens oder der MAN Truck & Bus SE.	• Informationen/Daten, IT-Systeme und IT-Dienste der Stufe 1 unterliegen keinen besonderen Anforderungen an die Verfügbarkeit. • Die Verfahren richten sich nach der sinnvollen und wirtschaftlich angemessenen Umsetzung von Maßnahmen und Prozessen.	• Offlinedaten aus dem Internet • Arbeitskopien
Stufe 2: Verfügbar	• Die Nichtverfügbarkeit der Informationen hat Auswirkungen auf den Geschäftsbetrieb eines MAN Truck & Bus Unternehmens, jedoch ohne dessen Existenz zu gefährden, und wirkt sich nur begrenzt negativ auf MAN Truck & Bus SE aus. **„Verfügbar“ ist die Standard-Verfügbarkeitsstufe für alle Informationen in der MAN Truck & Bus Gruppe, die nicht anders eingestuft bzw. gekennzeichnet sind.**	• Informationen/Daten, IT-Systeme und IT-Dienste der Einstufung „verfügbar“ müssen innerhalb eines eindeutig festgelegten Zeitraums wiederhergestellt oder ersetzt werden können. • Es muss ein Wiederherstellungskonzept vorhanden sein, mit dem bei einem IT-Ausfall sichergestellt werden kann, dass Funktionen und Informationen nach dem eindeutig festgelegten Zeitraum wieder zur Verfügung stehen. • Das Verfügbarkeitskonzept ist zu dokumentieren.	• Internetauftritt • Markenrichtlinien • Markenrichtlinienanweisungen • Intranet • Image-Broschüren • Publikationen • Zeitaufwendige Präsentationen • Entwicklungsunterlagen • IT-Systeme, z. B. Server

[8] Die Klassifizierung eines bestimmten Informationswerts muss auf Einzelfallbasis erfolgen. Die hier genannten Beispiele sind daher nicht bindend.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Sicherheitsstufe	Bedeutung	Behandlungs-	Beispiele[9]
3. Stufe: Hoch verfügbar	• Die Nichtverfügbarkeit der Informationen hat erhebliche negative Auswirkungen auf die MAN Truck & Bus Gruppe, ihre Aktionäre, Geschäftspartner oder Mitarbeiter (z. B. wenn die Existenz einer oder mehrerer MAN Truck & Bus Unternehmen gefährdet ist, oder es sind erhebliche rechtliche Konsequenzen für MAN Truck & Bus zu erwarten).	• Es müssen Mindestverfügbarkeitsstufen von Informationen/Daten, IT-Systemen und IT-Diensten sowohl für den Normalfall als auch für den Notfall angegeben werden. • Die Informationen sind redundant zu handhaben, sodass die Beeinträchtigung der Geschäftsprozesse bei Ausfall oder Vernichtung von Informationen und Systemen ein akzeptables Niveau nicht überschreitet. • Das Verfügbarkeitskonzept ist detailliert zu dokumentieren und regelmäßig zu prüfen. • Ein Disaster-Recovery-Konzept ist detailliert zu dokumentieren und regelmäßig zu prüfen.	• Informationen der Produktionssteuerung • Finanzberichterstattung

6.6 Authentizität

Die Authentizität der Informationen belegt ihre Unverfälschtheit. Mit diesem Ziel wird sichergestellt, dass die Informationen im Zuge der Übermittlung nicht geändert wurden und der Empfänger die Quelle der Nachricht überprüfen kann. Zur Nachverfolgung von Informationsänderungen müssen manipulationssichere Technologien eingerichtet werden. Methoden zur Gewährleistung der Authentizität sind die Implementierung von Prüfsummen und die Verwendung digitaler Signaturen.

[9] Die Klassifizierung eines bestimmten Informationswerts muss auf Einzelfallbasis erfolgen. Die hier genannten Beispiele sind daher nicht bindend.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

7 Änderungen

Version 3.0

- Änderungsprotokoll hinzugefügt
- Neue Kennzeichnung: MAN Truck & Bus
- Änderung von Rollen und Verantwortlichkeiten
- Verweis auf Entsorgungsrichtlinie hinzugefügt
- Anforderungen für Authentifizierung gemäß Passwortrichtlinie hinzugefügt
- Deutsche Gesetzgebung nur als Beispiel angeführt
- Tabellenformat für Vertraulichkeit in Fließtext geändert
- Kurze Tabelle für Vertraulichkeit im Anhang hinzugefügt
- Übernahme des entsprechenden Level-3-Dokuments AN_MTB_13_1_02 „Umgang mit Informationen“
- Regelmäßige Überprüfung
- Aktualisierung der Verantwortlichkeiten
- Neues Kapitel / neue Tabelle – 6.2 Vertraulichkeit
- Neues Kapitel – 6.2.1 Entsorgung, Vernichtung und Löschung
- Neu geordnet – 6.2.2 Fragen zur Hilfestellung bei der Ermittlung der Vertraulichkeitsstufe
- Aktualisierung Kapitel – 6.3 Integrität
- Aktualisierung Kapitel – 6.4 Verfügbarkeit
- Neues Kapitel – 6.5 Authentizität
- Die zugewiesene neue Dokumentennummer "MA_13_1_03" - war "MAN 13.1 Anweisung 4 – Klassifizierung von Informationswerten"
- Der "MAN 13.1 Anweisung 3 - Management von Informationssicherheitsvorfällen" wurde eine neue Dokumentennummer zugewiesen "MA_13_1_09".

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Anlage 1 : Umgang mit klassifizierten Informationen

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Anlage 1 - Umgang mit klassifizierten Informationen

Ersteller	Steven Rauwerdink Ralf Schlag	**Freigeber**	Andre Wehner	**Version**	1.0
Abt.	FIOS	Abt..	FI	**KSU-Class:**	XX

Gültigkeitsbeginn Datum 01.02.2023	**Geltungsbereich** MAN Truck & Bus SE und deren Tochtergesellschaften	**Genehmigungen (Vorstand)*** **Abgestimmt mit**

* Nur erforderlich, sofern eine Markenanweisung keiner übergeordneten Markenrichtlinie zuzuordnen ist.

Inhalt

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

1 Zweck

Der Zweck dieses Anhangs besteht darin, die Anforderungen an den Umgang mit Informationen in Bezug auf ihre Klassifizierung gemäß MTB Markenrichtlinie MR_13_1 Information Security und Markenanweisung MA_13_1_03 – Klassifizierung von Informationswerten detailliert zu definieren und zu beschreiben.

Das Dokument enthält detaillierte Anweisungen für alle Mitarbeiter von MAN Truck & Bus und externe Auftragnehmer zu den Anforderungen an die sichere Ablage, den Austausch, die Präsentation, die Kennzeichnung, den Druck und die Entsorgung von Informationen und Informationsbeständen entsprechend ihrer Vertraulichkeit, Integrität und Verfügbarkeit. Darüber hinaus werden die Anforderungen an den sicheren Umgang mit Informationen in der Cloud und bei der Fernarbeit bereitgestellt.

2 Schutz von Informationswerten

2.1 Allgemeine Anforderungen

Unabhängig vom Vertraulichkeitsgrad der Informationen ist stets das Need-to-know-Prinzip anzuwenden. Das bedeutet: Einzelpersonen erhalten nur Zugriff auf die Informationen, die sie zur Erfüllung ihrer Aufgaben benötigen.

- Alle Daten- und Informationssysteme erfordern einen verantwortungsvollen Umgang und dürfen nur bestimmungsgemäß verwendet werden. Darüber hinaus dürfen Informationen und Informationssysteme nur so verwendet werden, dass MAN Truck & Bus SE rechtlich nicht haftbar gemacht werden kann.
- Nutzer von Informationssystemen müssen Urheberrechts- und Lizenzvereinbarungen einhalten.
- Von MAN Truck & Bus SE bereitgestellte Informationen dürfen nicht zum persönlichen Vorteil genutzt werden.
- Mündliche Kommunikation, ob persönlich oder telefonisch, hat so zu erfolgen, dass die Vertraulichkeit der Informationen gewährleistet ist und diese für unbefugte Dritte nicht zugänglich sind.
- Der Umgang mit elektronischen Datenträgern wie CDs und USB-Sticks muss verantwortungsvoll und entsprechend ihrer jeweiligen Klassifizierung erfolgen.
- Werden unbeaufsichtigte, als vertraulich oder streng vertraulich gekennzeichnete Dokumente gefunden, sind diese in Verwahrung zu nehmen und direkt an den für die Informationen Verantwortlichen oder den Eigentümer der Informationen zurückzugeben. Kann diese Person nicht kontaktiert werden, müssen die Dokumente an den lokalen Informationssicherheitsbeauftragten (IS-Manager) oder an lokale oder globale Sicherheitsbeauftragte übergeben werden. Alternativ können die Dokumente entsprechend ihrer Klassifizierung vernichtet werden.
- Werden unbeaufsichtigte Dokumente mit personenbezogenen Daten gefunden, sind diese in Verwahrung zu nehmen und direkt an den zuständigen Datenschutzbeauftragten auszuhändigen.
- Vertrauliche Informationen der MAN Truck & Bus Gruppe dürfen nicht auf privaten Systemen oder Datenträgern gespeichert werden. Eine Übermittlung an Anbieter

öffentlicher Dienstleistungen (z. B. zur Übersetzung in andere Sprachen oder an Kommunikationsdienstleister) ist nur unter Anwendung geeigneter Sicherheitsmaßnahmen (z. B. verschlüsselte Übertragung, Versand per Einschreiben) und Geheimhaltungsvereinbarungen zulässig.

2.2 Schutzziele der Informationssicherheit

Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sind die wichtigsten Schutzziele im Kontext der Informationssicherheit. Spezifische technische und organisatorische Maßnahmen gewährleisten die Erreichung dieser Schutzziele.

2.3 Vertraulichkeit

Wie werden Informationen gekennzeichnet?

Zur Angabe der Vertraulichkeitsklasse von Informationen werden Kennzeichnungen verwendet. Sie sollen dem Leser zeigen und ihn daran erinnern, dass er sorgsam mit den Informationen umgehen muss.

PUBLIC	INTERNAL	CONFIDENTIAL	STRICTLY CONFIDENTIAL
ÖFFENTLICH	INTERN	VERTRAULICH	STRENG VERTRAULICH

Beispiel: Die Kennzeichnungen geben die englische Klassifizierung und ihre Übersetzung in die lokale Sprache wieder.

Wenn die Vertraulichkeitsklasse auch in den Dateinamen eines Dokuments aufgenommen wird, trägt dies dazu bei, Fehler bei der Speicherung oder Übermittlung dieser Informationen zu vermeiden.

Beispiel: ***2022–03_F10-Produktionsplan_vertraulich.xlsx***

Wie wird Vertraulichkeit erreicht?

Informationen, die nicht zur allgemeinen Veröffentlichung bestimmt sind, dürfen nur Personen zugänglich gemacht werden, die entsprechend berechtigt sind.

Ziele

- Zugriff auf Informationen verwalten,
- Schäden durch die Offenlegung von Informationen gegenüber nicht berechtigten Personen, Einrichtungen oder Prozessen vermeiden,
- Die geistigen Eigentumsrechte von MAN sowie Kunden- und Mitarbeiterinformationen schützen

Methoden

- Bewertung, Klassifizierung
- Authentifizierung
- Verschlüsselung

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

2.4 Integrität

Wie wird Integrität sichergestellt?

Sicherstellung einer fehlerfreien Verarbeitung von Informationen und Schutz vor unbefugten Änderungen.

Ziele

- Änderungen von Informationen überwachen, unbemerkte Änderungen verhindern,
- Änderungen nur mit entsprechender Berechtigungsstufe – Zugriffsrechte regelmäßig überprüfen

Methoden

- Änderungsprotokoll
- Änderungsgenehmigung
- Prüfsumme

2.5 Verfügbarkeit

Wie wird die Verfügbarkeit von Informationen gewährleistet?

Informationen müssen innerhalb eines vereinbarten Zeitrahmens verfügbar sein.

Ziele

- Verfügbarkeit überwachen, rechtzeitige Wiederherstellung nach Ausfällen,
- Umgang mit Erwartungen

Methoden

- Serviceüberwachung
- Service-Level-Agreement
- Failover-Plan

2.6 Authentizität

Wie wird die Authentizität von Informationen sichergestellt?

Die Informationen wurden im Zuge der Übermittlung nicht geändert, und der Empfänger kann die Quelle der Nachricht überprüfen.

Ziele

- Änderungen an Informationen verfolgen,
- manipulationssichere Technologien (z. B. Dokumentenhistorie) einsetzen

Methoden

- Prüfsumme
- Digitale Signaturen

3 Wie müssen Informationen je nach Klassifizierung behandelt werden?

3.1 Vertraulichkeit

	STRICTLY CONFIDENTIAL STRENG VERTRAULICH	CONFIDENTIAL VERTRAULICH	INTERNAL INTERN
Speichern			
Filesharing	Ja, bei klassifiziert freigegebener MTB-Speicherung		OK, ohne besondere Vorsichtsmaßnahmen
Outlook-Postfach	OK, wenn Nachrichtenverschlüsselung aktiv	OK, wenn Tag „vertraulich“ aktiv	
MS Teams / SharePoint Online	Nein	OK, wenn von TEAMS-/SP-Eigentümer verwaltet	
Physische Informationen	Niemals unbeaufsichtigt lassen, in einem Tresor aufbewahren	Niemals offen zugänglich lassen, verschlossen aufbewahren	Niemals in öffentlichen Bereichen lassen
Austauschen			
E-Mail (extern)	Keine direkte E-Mail, Links zu vertraulichem Austausch	Keine direkte E-Mail, nur verschlüsselt	Intern keine Vorsichtsmaßnahmen, extern mit Geheimhaltungsvereinbarung
Brief	Intern – persönlich extern – genehmigter Kurier	Intern – Verteilungstasche extern – Einschreiben	Firmenpost oder Standardpost
Präsentieren			
Sorgfaltspflicht des Präsentierenden	Nur genehmigtes und bestätigtes Publikum Gesicherter Ort Keine Fotos oder Aufnahmen Unternehmensausstattung	Nur genehmigtes und bestätigtes Publikum Geheimhaltungsverpflichtung Unternehmensausstattung	Interne Zielgruppe, keine Vorsichtsmaßnahmen Externe Zielgruppe, mit Geheimhaltungsvereinbarung

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

	STRICTLY CONFIDENTIAL STRENG VERTRAULICH	CONFIDENTIAL VERTRAULICH	INTERNAL INTERN
Kennzeichnen			
Dokumente	Auf jeder Seite		Auf der ersten Seite des Dokuments
Bilder	Wasserzeichen – streng vertraulich	Wasserzeichen – vertraulich	Keine Kennzeichnung erforderlich
Drucken			
Direktdruck	Nein, nur print2me	OK, ohne besondere Vorsichtsmaßnahmen	
Entsorgen			
Physische Informationen	Physisch vernichtet vor Ort geschreddert oder Datenentsorgungsbehälter		Abfallbehälter vor Ort
Digital gespeicherte Informationen	HDD zuverlässig überschrieben USB-Sticks, CD/DVD, vor Ort geschreddert oder in Datenentsorgungsbehälter entsorgt Datenentsorgungsnachweis		Zuverlässiges Löschen von Daten Entsorgung in Abfallbehälter vor Ort
Mobiles Arbeiten / Remote Work			
Sorgfaltspflicht des Mitarbeiters	Informationen dürfen die Räumlichkeiten nicht ohne ausdrückliche Genehmigung verlassen	Mit einem gesicherten Netzwerk verbinden Zugriff nur über Unternehmensausstattung Den Datenschutz wahren, den Bildschirm schützen und Dokumente verschlossen aufbewahren	

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Cloud		
Sorgfaltspflicht des Kontoinhabers	Nutzung generell nicht zulässig Einzelfallbewertung durch Informationssicherheit Schlüsselmanagement im Eigentum von MAN	Verschlüsselte Übermittlung und Speicherung Starke Authentifizierung Cloud-Anbieter mit bestandener Cloud-Anbieterbewertung

3.2 Integrität

	Stufe 2 Gesicherte Integrität	**Stufe 3** Prüfbare Integrität	**Stufe 4** Signierte Integrität
Speichern			
Digitale/physische Informationen	Informationen müssen an einem Ort gespeichert werden, an dem Änderungen erkennbar sind (z. B. Änderungsprotokolle sind implementiert)		Änderungen müssen erkennbar sein und bedürfen einer Signatur (z.B. physische oder digitale Signatur eines Dokuments)
Austauschen			
Digitale Informationen	Übermittlung von Informationen über vertrauenswürdige Kanäle und vertrauenswürdige Routen (z. B. TLS, sichere Dateiübertragung)	Nachweise führen, um die Integrität der übermittelten Informationen überprüfen zu können (z. B. Datum der letzten Änderung, letzte Änderung durch Benutzer-ID)	Ausgetauschte Informationen beinhalten eine digitale Signatur des Urhebers (z. B. der letzten Person, die die Informationen geändert hat)
Physische Informationen	Physische Informationen in einem Umschlag über einen vertrauenswürdigen Zusteller versenden (z. B. Brief per Post)	Physische Informationen in einem Umschlag über einen vertrauenswürdigen Zusteller mit Lieferbestätigung versenden (z. B. per Einschreiben)	Versiegelter Umschlag, der dem Empfänger persönlich übergeben wird und durch Unterschriften bestätigt ist (z. B. Einschreiben mit Rückschein)
Drucken			
Direktdruck	Persönlich prüfen, ob der Ausdruck korrekt ist		

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

3.3 Verfügbarkeit

	Stufe 2 Verfügbar	**Stufe 3** Hoch verfügbar
Speichern		
Digitale Informationen	Informationen nicht lokal speichern. Informationen an einen zuverlässigen, zentral verwalteten Speicher (Dateiserver oder Cloudspeicher) übermitteln. Dort werden Informationen gesichert und können bei Fehlern innerhalb der geforderten Zeit bis zu einem bestimmten Alter der Daten wiederhergestellt werden.	Nur zertifizierte Speicher verwenden, die den Zielen der Hochverfügbarkeit sowie Technologien für rechenzentrumsübergreifende Spiegelung entsprechen, geprüfte Disaster-Recovery-Pläne sowie zertifizierte Archivierungslösungen nutzen.
Physische Informationen	Dokumente an sicheren Orten aufbewahren, die vor Gefahren wie Feuer, Überschwemmung und Feuchtigkeit geschützt sind.	Mit Kopien eines Dokuments arbeiten und das Original an einem besonders sicheren Ort wie einem Tresor oder einem zertifizierten Dokumentenarchiv aufbewahren.
Präsentieren		
Sorgfaltspflicht des Präsentierenden	Zum Schutz Ihrer Präsentation mögliche technische Ausfälle berücksichtigen und sich auf diese vorbereiten (z. B. mittels lokaler Kopien, Cloud-Kopie, alternativen Präsentationsgeräts oder Papierausdrucks).	
Mobiles Arbeiten / Remote Work		
Sorgfaltspflicht des Mitarbeiters	Die Verwendung der bereitgestellten Unternehmensausstattung gewährleistet die Erfüllung des Standard-Verfügbarkeitsziels für den Zugriff auf Informationen in der Telearbeit.	Für höhere Anforderungen an die Verfügbarkeit von Informationen kann eine lokale Kopie auf einem sicherheitszertifizierten verschlüsselten Gerät (z. B. sichere Festplatte) erstellt werden.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

4 Änderungen

Version 1.0

- Erstellung

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Informationssicherheit für Systembetrieb und Administration

Ersteller	Steven Rauw erdink	**Freigeber**	Andre Wehner	**Version**	3.0
Abt.	FIOS	Abt..	FI	**KSU-Class:**	xx

Gültigkeitsbeginn	**Geltungsbereich**	**Genehmigungen (Vorstand)***
Datum 01.02.2023	MAN Truck & Bus SE und deren Tochtergesellschaften	**Abgestimmt mit**

* Nur erf orderlich, sofern eine Markenanweisung keiner übergeordneten Markenrichtlinie zuzuordnen ist.

Inhalt

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

1 Zweck

Diese Markenanweisung ist abgeleitet von der Markenrichtlinie MTB MR_13_1 Informationssicherheit und der MTB Markenanweisung MA_13_1_01 - Standard für Informationssicherheit. Sie definiert die Informationssicherheitsvorschriften, die von allen Mitarbeitern der MAN Truck & Bus oder externen Partnern zu beachten sind, die für Systeme der Informations- und Kommunikationstechnik (IKT-Systeme) sowie Infrastrukturbetrieb, -verwaltung und -architektur verantwortlich sind. Das Dokument definiert die Verantwortlichkeiten und Vorschriften für den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von IKT-Systemen und -Netzen in ihrer Entwurfsphase sowie während ihres Betriebs. Darüber hinaus werden in dieser Anweisung die Anforderungen an die Kennwortkomplexität für Administratorkonten beschrieben.

2 Geltungsbereich

Diese Markenanweisung gilt weltweit für die MAN Truck & Bus SE und ihre Tochtergesellschaften sowie deren Mitarbeiter[1]. Sie gilt unmittelbar und bedarf keiner Umsetzungsrichtlinie durch einzelne Tochtergesellschaften. Für Gesellschaften, bei denen die MAN Truck & Bus SE die Geltung der Markenanweisung aus rechtlichen Gründen nicht unmittelbar bewirken kann, ist in Abstimmung mit dem Chief Information Security Officer zu klären, inwieweit diese Markenanweisung Anwendung findet. Dies gilt beispielsweise für Gesellschaften, die sich nicht zu 100 % im Anteilsbesitz der MAN Truck & Bus SE befinden und auch nicht durch einen Beherrschungsvertrag mit der MAN Truck & Bus SE verbunden sind (wie z.B. Gesellschaften, die sich im Anteilsbesitz der MAN Finance and Holding S.A. befinden).

Sofern Gesellschaften eigene Regelungen zu diesem Sachverhalt erlassen haben, sind diese umgehend außer Kraft zu setzen. Bis zur Außerkraftsetzung solcher Regelungen oder Teilen von Regelungen gilt diese Markenanweisung vorrangig.

Sollten Regelungen dieser Markenanweisung aufgrund zwingender lokaler Anforderungen nicht umgesetzt werden können, muss die betroffene Gesellschaft unverzüglich den Chief Information Security Officer der MAN Truck & Bus SE informieren, um notwendige Änderungen oder Ergänzungen zu besprechen.

Das Dokument muss mindestens alle drei Jahre überprüft und gegebenenfalls angepasst werden.

3 Begriffe und Definitionen

Ein Glossar für das gesamte Regelwerk der Informationssicherheit ist in der Zusatzinformation „Begriffe und Definitionen zur Informationssicherheit“ zu finden.

4 Zielgruppe

Dieses Dokument richtet sich an Mitarbeiter der MAN Truck & Bus oder an externe Partner, die für Entwicklung, Installation, Betrieb und Konfiguration von Systemen der Informations- und Kommunikationstechnik (IKT-Systemen) verantwortlich sind, sowie an deren Führungskräfte.

Zu diesen Mitarbeitern der MAN Truck & Bus gehören IT-Manager, Systemarchitekten, Betriebsverantwortliche sowie alle Mitarbeiter oder externen Partner, die mit der Konfiguration von IKT-Systemen betraut sind.

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

5 Informationssicherheit für IKT-Systeme

Da IKT-Systeme ständig einer Vielzahl von Bedrohungen ausgesetzt sind, ist ein wirksamer Schutz dieser Systeme für die Erreichung der Geschäftsziele von MAN Truck & Bus unerlässlich.

Diese Bedrohungen sind:

- Informationsverlust durch Verstöße
- Ungewollte Veröffentlichung
- Offenlegung gegenüber Wettbewerbern
- Manipulation
- Zuwiderhandlung
- Verlust der Lieferfähigkeit

5.1 Verantwortung für die Informationssicherheit der IKT-Systeme

Der Eigentümer eines Systems bzw. einer Anwendung ist verantwortlich für die Umsetzung des risikoorientierten Ansatzes im Hinblick auf den Schutz der Informationssicherheitsziele der MAN Truck & Bus Gruppe. Ein wirksamer Schutz kann nur durch eine Kombination geeigneter Maßnahmen erreicht werden. Zu diesen Maßnahmen gehören:

- Integration unserer Mitarbeiter in die Unternehmenskultur
- Sicherheitsbewusstsein für das gesamte Unternehmen
- Einhaltung der festgelegten Prozesse und Verfahren
- Angemessener Schutz von Informations- und Kommunikationsgeräten und -Software

Alle Mitarbeiter der MAN Truck & Bus Gruppe oder externen Partner, die mit der Konfiguration von IKT-Systemen betraut sind, sind für die Einhaltung der relevanten MAN Truck & Bus Vorschriften verantwortlich.

Alle Anwendungsentwickler und Systemarchitekten der MAN Truck & Bus Gruppe sind dafür verantwortlich, dass Design, Spezifikationen, Prüfung und Migration der IKT-Systeme den relevanten Markenanweisungen und Vorschriften der MAN Truck & Bus entsprechen.

Alle für den Betrieb verantwortlichen Personen müssen die Betriebssicherheit der IKT-Systeme in ihrem Verantwortungsbereich gemäß den relevanten Anforderungen von MAN Truck & Bus sicherstellen. Dabei müssen die Betreffenden sehr aufmerksam auf Bedrohungen der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen achten.

5.2 Anforderungen an die Gestaltung von IKT-Systemen

Bei der Gestaltung von IKT-Systemen sind die Markenrichtlinie MTB MR_13_1 Informationssicherheit und die MTB Markenanweisung MA_13_1_01 – Standard für Informationssicherheit zu beachten. Darüber hinaus gilt Folgendes:

- Als Teil der Entwicklungs- und Spezifikationsphase eines IKT-Systems muss eine Risikoanalyse auf der Grundlage der ISi-Bewertungsmethode durchgeführt werden.
- Bei der Planung zukünftiger Kapazitätsbedarfe sind neue Geschäfts- und Systemanforderungen sowie aktuelle und absehbare Trends zu berücksichtigen.
- Konzepte zur Umsetzung, Integration und Erprobung müssen die Ergebnisse der Risikoanalyse und die daraus resultierenden Maßnahmenpläne berücksichtigen. Hierbei ist

darauf zu achten, dass unabhängige Tester zugewiesen werden, die nicht im Rahmen der Entwicklungs- und Spezifikationsphase der jeweiligen IKT-Systeme involviert waren.

- Für jedes IKT-System muss ein akzeptables Nutzungskonzept definiert werden.
- Bei der Gestaltung von IKT-Systemen ist in Abhängigkeit von den risikoorientierten Anforderungen an die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen die physische und Umgebungssicherheit des Entwicklungsortes sicherzustellen (vgl. MTB Markenanweisung MA_13_1_01 – Standard für Informationssicherheit, Artikel 10 und 11).

  Diese umfasst:

  - Zugriffsschutz und Zugriffsverwaltung – administrative und technische Kontrolle und Verfolgung des physischen Zugangs zu den Systemen der Informations- und Kommunikationstechnik, einschl. Anlieferungsbereiche, Sicherheitspersonal, Zäune, Tore und Sicherheitsbereiche
  - Eindringungserkennung/-schutz – Maßnahmen zur Erkennung und Verhinderung von unbefugtem Zugriff auf und Sabotage von Systemen der Informations- und Kommunikationstechnik einschließlich Überwachung.
  - Brandschutz – Maßnahmen zur Erkennung und Verhinderung der Ausbreitung eines Brandes und der schädlichen Auswirkungen von Dämpfen (Rauch), einschl. Brandmeldeanlagen, Feuerschutztüren und Eingrenzungsbereiche, Löscheinrichtungen und Rauchabzugsanlagen
  - Schutz vor Umweltgefahren – Erdbeben, Überschwemmungen usw.
  - Umgebungsklimatisierung – Luftwechselraten, Temperatursteuerung, Feuchtigkeitssteuerung und -überwachung
  - Schutz gegen Ausfall von Versorgungseinrichtungen (Strom- und Kühlsysteme) für Systeme der Informations- und Kommunikationstechnik, einschl. Management der Versorgungskapazität, unterbrechungsfreie Stromversorgung und Notstromaggregate
  - Baulicher Schutz – Tragfähigkeit der Decken/Böden, Eignung der Liefer- und Verkehrswege
  - Schutz von Kabeln und Leitungen – verschlossene Schränke gegen Abhören und Beschädigung sowie eindeutige Beschriftung für eine schnelle Fehlerbehebung
  - Vom Hersteller der technischen Komponenten geforderte Betriebsbedingungen
- Um Informationen angemessen zu schützen und unannehmbare Risiken für die Geschäftsprozesse von MAN Truck & Bus zu vermeiden, sind neben der MTB Markenanweisung MA_13_1_07 – Informationssicherheitsanforderungen zur Entwicklung sicherer Anwendungen und der Anlage 1 zur Markenanweisung MA_13_1_07 – Anforderungen zur Entwicklung sicherer Anwendungen folgende Punkte zu beachten:
  - Die Produktions-, Test- und Entwicklungsumgebungen müssen getrennt werden, um Interferenzen zu vermeiden (z. B. auf unterschiedlichen Systemen oder Prozessoren und in unterschiedlichen Domänen oder Verzeichnissen laufen).
  - Die Regeln für den Übergang der Software aus der Entwicklungs- in die Produktionsphase müssen definiert und dokumentiert werden

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

- Compiler, Editoren und sonstige Entwicklungswerkzeuge oder System-Dienstprogramme dürfen nicht von Produktionssystemen aus zugänglich sein, wenn dies nicht erforderlich ist
- Die Testsystemumgebung muss die Produktionssystemumgebung so genau wie möglich nachstellen
- Benutzer müssen unterschiedliche Authentifizierungen für Produktions- und Testsysteme verwenden
- Test- und Entwicklungssysteme müssen eindeutig gekennzeichnet sein, damit eine ordnungsgemäße Identifizierung des Systems zur Vermeidung von Benutzerfehlern gewährleistet ist
- Vertrauliche oder streng vertrauliche Informationen und Daten aus den Produktionssystemen dürfen in den Testsystemumgebungen nicht verwendet werden. Wenn dies nicht vermieden werden kann, müssen die Informationen gemäß den Anforderungen für Produktionsdaten geschützt werden.

- Der Einsatz neuer Geräteklassen und Softwaretechnologien für die MAN Truck & Bus Gruppe darf erst nach erfolgreichem Abschluss von Implementierungs- und Integrationstests und der Freigabe durch die zuständigen Gremien von MAN Truck & Bus erfolgen.
- Bei übergreifenden Architekturen ist die Freigabe des CIO und IT-Vorstands der MAN Truck & Bus Gruppe einzuholen.
- Die Akzeptanz von verbleibenden Informationssicherheitsrisiken muss formell durch den/die verantwortlichen Eigentümer (Prozess, Anwendung oder System) bestätigt werden.
- Die nach außen gerichteten Systeme müssen besonders widerstandsfähig gegen Cyberangriffe wie DDoS-Angriffe (Distributed Denial of Service), schädlichen Code, unbefugten Zugriff usw. ausgelegt sein.
- Für IKT-Systeme, die Informationen mit hohem oder sehr hohem Schutzbedarf verarbeiten, muss eine End-to-End-Verschlüsselung gewährleistet werden.
- Bei der Gestaltung von Geschäftsanwendungen und -systemen sind neben den in der MTB Markenanweisung MR_13_1_01 – Informationssicherheitsanforderungen zur Entwicklung sicherer Anwendungen definierten allgemeinen Anforderungen mindestens folgende Kriterien zu beachten:
  - Sicherstellen, dass geeignete Authentifizierungs- und Autorisierungsmethoden in Übereinstimmung mit den Vertraulichkeits- und Integritätsstufen der Informationen implementiert und mit Geschäftspartnern geteilt werden
  - Gewährleisten, dass die Handelspartner von ihren erteilten Berechtigungen Kenntnis haben
  - Definition und Erfüllung der Anforderungen an Vertraulichkeit, Integrität, Versandnachweis und Erhalt wichtiger Dokumente sowie Nicht-Ablehnung von Verträgen, z. B. in Verbindung mit Angebotsabgabe- und Vertragsprozessen.
  - Vermeidung von Verlust oder Vervielfältigung von Transaktionsinformationen
  - Haftungsverhältnisse in Bezug auf das Eigentum an Informationen

- Einhaltung der relevanten gesetzlichen Anforderungen in Bezug auf das Land und die Nutzung der Geschäftsanwendung oder des Geschäftssystems

- Für alle IKT-Systeme von MAN Truck & Bus sind Berechtigungskonzepte zu definieren. In die Berechtigungskonzepte müssen mindestens folgende Aspekte einfließen:
  - Sicherheitsanforderungen des zugrundeliegenden Geschäftsprozesses
  - Rechtliche und vertragliche Verpflichtungen in Bezug auf den Zugriff auf Informationen oder Dienste
  - Prozess und Verfahren bei der Zugriffs- und Rechteverwaltung, einschl. Freigaben, Zuweisung, Änderung und Widerruf
  - Revisionssichere Dokumentation der aktuellen Berechtigungen (Auditbericht) und der Rechtevergabe-/Rechtewiderrufsverfahren (Auditprotokoll)
  - Ein Prüfungsverfahren zur Feststellung der Richtigkeit der aktuellen Berechtigungen
  - Verwaltung kritischer Berechtigungen (privilegierter Zugriff)

5.3 Anforderungen an die Gestaltung von Netzwerken

Netzwerke von MAN Truck & Bus sind so auszulegen, dass die Netzwerke je nach Risiko in verschiedene Klassen/Bereiche (DMZ, Geschäftsanwendungen, IT-Infrastrukturanwendungen, Cloud-Anwendungen, Engineering-Anwendungen, HR-Anwendungen, Facility-Management-Anwendungen, Produktions- und Logistikanwendungen usw.) unterteilt sind.

Netzwerk-Gateways dürfen nur den erforderlichen Netzwerkverkehr zulassen und müssen speziell gegen Manipulation oder unbefugten Zugriff geschützt werden.

Der Fernzugriff auf interne Netzwerke von MAN Truck & Bus erfordert eine starke Authentifizierung und End-to-End-Verschlüsselung.

Für alle Netzwerke von MAN Truck & Bus sind Berechtigungskonzepte zu definieren. In die Berechtigungskonzepte müssen mindestens folgende Aspekte einfließen:

- Sicherheitsanforderungen des zugrundeliegenden Geschäftsprozesses
- Prozess und Verfahren der Sicherheitskonformitätsprüfung von Geräten vor der Anbindung an interne Netzwerke der MAN Truck & Bus
- Prozess und Verfahren für die Sicherheitskonformitätsprüfung und Freigabe von Netzwerkmanagement-Tools
- Verwaltung kritischer Berechtigungen (privilegierter Zugriff auf Netzwerkkomponenten)
- Prozess und Verfahren bei der Zugriffs- und Rechteverwaltung zur Verwaltung von Netzwerken und Netzwerkdiensten, einschl. Freigaben, Zuweisung, Änderung und Widerruf
- Verwaltungsverfahren und technische Maßnahmen zum Schutz des Zugriffs auf Netzwerkverbindungen und Netzwerkdienste
- Verwaltungsverfahren und technische Maßnahmen zum Schutz des Zugriffs auf Diagnose- oder Konfigurations-Ports

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

5.4 Anforderungen an den Betrieb von IKT-Systemen

Bei dem Betrieb der IKT-Systeme von MAN Truck & Bus sind die Markenrichtlinie MTB MR_13_1 Informationssicherheit und die MTB Markenanweisung MA_13_1_01 – Standard für Informationssicherheit zu beachten. Darüber hinaus gilt Folgendes:

- Es müssen Prozesse und Verfahren für die Stilllegung und sichere Entsorgung von IKT-Systemen vorhanden sein. Bei IKT-Systemen, die interne, vertrauliche oder streng vertrauliche Informationen enthalten (vgl. MTB Markenanweisung MA_13_1_03 – Klassifizierung von Informationsressourcen) sind die Datenträger entweder physisch zu zerstören oder die auf diesen Systemen gespeicherten Informationen unwiederbringlich zu löschen. Diese Maßnahme muss angemessen dokumentiert und Aufzeichnungen müssen aufbewahrt werden.
- Bei Personalausfall oder der Systemfunktionsstörungen müssen für alle in der MAN Truck & Bus Gruppe eingesetzten IKT-Systeme ein Betriebsablauf und eine Dokumentation zur Verfügung stehen, damit der Normalbetrieb schnellstmöglich wieder aufgenommen werden kann. Dazu gehören:
    - Datenverarbeitung
    - Backup und Wiederherstellung
    - Betriebsplanung
    - Schnittstellen und Abhängigkeiten zu anderen IKT-Systemen
    - Anweisungen für die Fehlerbehandlung oder den Umgang mit sonstigen Ausnahmebedingungen einschließlich Einschränkungen in der Nutzung von Tools
    - Für den Fehlerfall sollte eine Kontaktliste für den technischen und betrieblichen Support vorhanden sein
    - Neustart- und Reboot-Verfahren für das System
    - Management von Prüfspuren (Audit Trails) und Systemprotokoll-Informationen
    - Systemspezifische Änderungsverfahren
    - Beschreibung von Rollen und Zuständigkeiten
- Die Dokumentation der Systemkonfigurationen muss vor unbefugtem Zugriff und Offenlegung geschützt werden.
- Um die Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit verarbeiteter Informationen zu minimieren, müssen Änderungen an IKT-Systemen gemäß dem dokumentierten, standardisierten Änderungsmanagementprozess implementiert werden. Der Änderungsprozess muss folgende Punkte umfassen:
    - Feststellung und Dokumentation bedeutender Änderungen
    - Planung von Änderungen und Durchführung entsprechender Prüfungen
    - Bewertung potenzieller Risiken im Zusammenhang mit diesen Änderungen, einschließlich der Auswirkungen auf die Geschäftsprozesse von MAN Truck & Bus SE
    - Formales Freigabeverfahren für vorgeschlagene Änderungen

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

- Mitteilung der Einzelheiten der vorgeschlagenen Änderungen an alle relevanten Stakeholder
- Verfahren und Verantwortliche für die Stornierung einer Änderung:
- Rollback-Plan nach fehlgeschlagenen Änderungsversuchen oder nicht vorhersehbaren Ereignissen
- Verfahren für Notfalländerungen

- Die Leistungsfähigkeit der Systeme der Informations- und Kommunikationstechnik ist zu überwachen und auf die Zielwerte abzustimmen.
- Neue Informationssysteme, Upgrades und neue Versionen dürfen erst nach Erhalt einer formalen Freigabe in die Produktionsumgebung implementiert werden. Dabei sind mindestens folgende Punkte zu berücksichtigen:
  - Vollständigkeit und Angemessenheit der Sicherheitsmaßnahmen
  - Vorfallmanagementverfahren
  - Vollständigkeit und Angemessenheit der Betriebsabläufe
  - Kontinuitätsmanagement und Notfallpläne
  - Betriebsschulungen für die neuen Systeme wurden durchgeführt
- Die Anforderungen der MTB Markenanweisung MA_13_1_01 – Standard für Informationssicherheit, Artikel 26, sind umzusetzen, um das Eindringen und Verbreiten von Schadsoftware und -codes zu verhindern.
- Für die Identifizierung und Bewertung von Schwachstellen und deren Behebung müssen Informationen über technische Schwachstellen der eingesetzten Systeme und Anwendungen rechtzeitig ermittelt und bewertet werden. Für jedes System der Informations- und Kommunikationstechnik von MAN Truck & Bus muss ein Verfahren zur ordnungsgemäßen und Notfallinstallation von Sicherheitspatches zur Verfügung stehen. Folgende Aspekte sind zu berücksichtigen:
  - Die Quellen für Informationen über Schwachstellen sind zu ermitteln und zu dokumentieren
  - Schwachstellen müssen hinsichtlich des Risikos bewertet werden.
  - Abhängig von der Risikobewertung einer Schwachstelle muss ein Aktionsplan definiert und priorisiert werden
  - Patches sind aus vertrauenswürdigen Quellen zu beziehen
  - Es muss ein Verfahren vorhanden sein, mit dem kritische Patches rechtzeitig außerhalb der regulären Wartungsfenster bereitgestellt werden können
  - Ein Patchverfahren muss in den Änderungsmanagementprozess integriert werden
- Für jedes bei der MAN Truck & Bus Gruppe eingesetzte IKT-System ist ein Backup- und Wiederherstellungsverfahren zu implementieren. Dieses Verfahren muss den Anforderungen der MTB Markenanweisung MA_13_1_01 – Standard für Informationssicherheit, Artikel 25 entsprechen. Die Backupstrategie ist abhängig von dem Risiko für die Geschäftsprozesse der MAN Truck & Bus Gruppe und ergibt sich aus der Klassifizierung der Informationswerte (vgl. Markenanweisung MA_13_1_03 –

Klassifizierung, Abschnitt 6). Darüber hinaus muss das Backup- und Wiederherstellungskonzept folgende Punkte berücksichtigen:

- Die Backups müssen rückverfolgbar und die Backup-Medien eindeutig beschriftet sein
- Backup- und Wiederherstellungskonzepte müssen auf die Anforderungen des betrieblichen Kontinuitätsmanagements (BCM) abgestimmt werden. Dazu gehört auch die Aufbewahrung von Backup-Medien in ausreichender physischer Entfernung zum Hauptstandort, an dem die Informationen gespeichert werden. Es muss sichergestellt werden, dass der Backup-Aufbewahrungsort nicht von derselben Katastrophe betroffen ist.
- Backup-Medien müssen am Remote-Aufbewahrungsort gemäß der Klassifizierung der darin enthaltenen Informationen geschützt werden.
- Backup-Medien müssen während des Transports zwischen Standorten (Übergabeverfahren, Verpackung, Transportmittel, zuverlässiger Kurierdienst) gemäß ihrer Klassifizierung nach MTB Markenanweisung MA_13_1_03 – Klassifizierung von Informationsressourcen, Anlage 1 – Umgang mit Verschlusssachen geschützt werden.
- Die Entsorgung von Datenträgern hat gemäß ihrer Klassifizierung nach MTB-Markenanweisung MA_13_1_03 – Klassifizierung von Informationsressourcen, Anlage 1 – Umgang mit Verschlusssachen zu erfolgen.

- Die IKT-Systeme von MAN Truck & Bus müssen gemäß den globalen Standards und anerkannten Best Practices für die Sicherung von IT-Systemen konfiguriert werden (vgl. CIS-Sicherheitsbenchmarks).
- Die Uhren in allen Systemen der MAN Truck & Bus Gruppe sind auf eine vereinbarte Referenzzeit eines zentralen Zeitservers zu synchronisieren.
- Für alle Informationssysteme und -dienste müssen rückverfolgbare Verfahren zur An- und Abmeldung regelmäßiger und privilegierter Benutzer vorhanden sein. Dies gilt auch für den gesamten Lebenszyklus von Berechtigungen. Alle Änderungen der Berechtigungen müssen erfasst werden.
- Allen Benutzern der IKT-Systeme von MAN Truck & Bus muss eine eindeutige persönliche Benutzerkennung zugewiesen werden.
- Es muss eine geeignete Authentifizierungsmethode ausgewählt werden, mit der die Identität des angegebenen Benutzers bestätigt wird.
- Die IKT-Systeme von MAN Truck & Bus sind für regelmäßige Benutzer, soweit technisch möglich, so zu konfigurieren, dass sie nur Passwörter mit mindestens 12 Zeichen akzeptieren (weitere Einzelheiten siehe MTB Markenanweisung MA_13_1_05 – Informationssicherheit für Mitarbeiter), die mindestens einmal jährlich zu ändern sind und aus einer Kombination von 3 der folgenden 4 Attribute bestehen:
  - Kleinbuchstaben (a-z)
  - Großbuchstaben (A-Z)
  - Ziffern/Zahlen (0–9)
  - Sonderzeichen (!,@,#,%,$,+)

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

- Erteilte Berechtigungen sind in regelmäßigen Abständen zu überprüfen. Diese Abstände sind entsprechend dem Umfang und der Kritikalität der Zugriffsrechte festzulegen, die Überprüfungen sind jedoch nicht seltener als einmal jährlich durchzuführen. Die durchgeführten Kontrollen sind eindeutig und nachvollziehbar zu dokumentieren und diese Dokumentation ist zu Nachweiszwecken sicher aufzubewahren.
- Bei allen IKT-Systeme von MAN Truck & Bus muss der Zugriff auf Betriebssysteme durch ein sicheres Anmeldeverfahren geschützt werden. Folgende Punkte sind dabei sicherzustellen:
    - Es werden keine System- oder Anwendungskennungen angezeigt, bevor der Anmeldevorgang erfolgreich abgeschlossen wurde.
    - IKT-Systeme mit hohem Schutzbedarf müssen die Vertraulichkeitsstufe der verarbeiteten Informationen deutlich anzeigen (d. h. als Label im GUI)
    - Die Anmeldeinformationen werden erst bestätigt, wenn alle Eingabedaten eingegeben wurden. Wenn ein Fehler auftritt, zeigt das System nicht an, welcher Teil der Daten korrekt oder falsch ist.
    - Die Anzahl der erlaubten erfolglosen Anmeldeversuche sowie die erlaubten maximalen und minimalen Zeiträume sind begrenzt.
    - Passwörter dürfen nicht im Klartext über das Netzwerk übertragen werden.
    - Vorzugsweise sollten Passwortverwaltungssysteme verwendet werden, um die Verwendung sicherer Passwörter zu erzwingen.
- Die Verwendung von System-Dienstprogrammen, die System- und Anwendungseinstellungen überschreiben können, muss Benutzern mit privilegierten Berechtigungen vorbehalten sein. Ihre Verwendung muss protokolliert und sie müssen vor der Verwendung durch andere Benutzer geschützt werden.
- Die IKT-Systeme von MAN Truck & Bus müssen so konfiguriert sein, dass inaktive Sitzungen nach einer festgelegten Zeit der Inaktivität beendet werden.

5.5 Anforderungen an den Betrieb der Netzwerkinfrastruktur

Der Schutz der internen und externen Kommunikation muss den Anforderungen der MTB Markenanweisung MA_13_1_01 – Standard für Informationssicherheit, Artikel 15 entsprechen. Zusätzlich gilt:

- Das Management von Gateway-Konfigurationen muss einem definierten Änderungsmanagementprozess folgen, einschließlich der Freigabe, der regelmäßigen Überprüfungen und des Ablaufs solcher Regeln.
- Der privilegierte Zugriff auf die Konfiguration von Netzwerkgeräten muss ausreichend protokolliert werden. Protokolle müssen vor unbefugter Änderung oder Löschung geschützt werden.
- Es müssen die Sicherheitsmaßnahmen festgelegt werden, die für einen bestimmten Dienst erforderlich sind. Es ist sicherzustellen, dass die jeweiligen Netzbetreiber diese Maßnahmen umsetzen.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

5.6 Anforderungen an Administratoren

Aufgrund ihrer Verantwortlichkeiten (siehe MTB Markenanweisung MA_13_1_01 – Standard für Informationssicherheit, Artikel 16) in Bezug auf den Betrieb von IKT-Systemen gilt für Administratoren zusätzlich:

- Administratoren müssen regelmäßig für die spezifischen Risiken in ihrem Arbeitsbereich sensibilisiert werden. Dazu gehören Anweisungen, Schulungen und Übungen.
- Für personenbezogene administrative Konten mit privilegierten Zugriffsrechten, die für administrative Aufgaben in IKT-Systemen verwendet werden, müssen Passwörter aus mindestens 15 Zeichen bestehen und mindestens 3 von 4 der folgenden Kriterien erfüllen:
    - Kleinbuchstaben (a-z)
    - Großbuchstaben (A-Z)
    - Ziffern/Zahlen (0–9)
    - Sonderzeichen (!,@,#,%,$,+)
- Die Passwörter müssen gemäß den dokumentierten Verfahren verwaltet werden.
- Privilegierte Benutzerkennungen dürfen nicht für die alltägliche Arbeit genutzt werden.
- Identische administrative Passwörter dürfen nicht für verschiedene Anwendungen verwendet werden.
- Server-Panels und Server-Konsolen müssen verschlossen werden, wenn sie nicht benutzt werden.
- Die Sitzungen müssen unmittelbar nach Beendigung der Aufgabe(n) geschlossen werden.
- Der Verantwortungsbereich eines Mitarbeiters mit erweiterten Rechten muss hinsichtlich der zu konfigurierenden IKT-Systeme definiert und dokumentiert werden und die Kompetenzen (Rechte und Pflichten) des Mitarbeiters müssen der Definition „Konfiguration der IKT-Systeme in seinem Verantwortungsbereich“ entsprechen.
- Die Verantwortlichkeiten müssen angemessen getrennt und auf zwei oder mehr Personen verteilt werden, um einen Missbrauch von IKT-Systemen zu verhindern.
- Zur Gewährleistung der Betriebssicherheit ist es erforderlich, dass administrative Ressourcen angemessen geplant und bereitgestellt werden.
- Administrative Ressourcen erfordern eine Vertraulichkeitsvereinbarung (NDA) als Teil von Verträgen

5.7 Sicherheitsvorfälle

Sicherheitsvorfälle sind in erster Linie Vorfälle oder Umstände, die dazu führen können, dass MAN Truck & Bus oder ihre Mitarbeiter, Kunden oder Partner einen unannehmbaren Verlust oder Schaden erleiden. In den meisten Fällen kann nur ein Experte feststellen, ob es sich um einen Sicherheitsvorfall oder nur um einen technischen Defekt oder Fehler handelt. Es ist immer wichtig, einen Sicherheitsvorfall so früh wie möglich zu identifizieren, um den Verlust oder Schaden zu begrenzen. Das Verhalten bei Sicherheitsvorfällen ist in der MTB Markenanweisung MA_13_1_09 – Management von Informationssicherheitsvorfällen detailliert beschrieben.

Alle Systembetreiber und Administratoren der MAN Truck & Bus Gruppe sind für die Erstellung spezifischer Berichte in ihrem Verantwortungsbereich verantwortlich.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Neben den regelmäßigen Überwachungs- und Betriebsberichten müssen sie auch in der Lage sein, regelmäßig und ad hoc spezifische Berichte zur Informationssicherheit bereitzustellen. In Kapitel 6.4 der MTB Markenanweisung MA_13_1_08 – Informationssicherheit für Lieferanten sind einige Beispiele für Berichte von Systembetreibern und Administratoren aufgeführt.

6 Änderungen

Version 3.0

- Änderungsprotokoll hinzugefügt
- Umbenennung
- Änderung von Rollen und Verantwortlichkeiten
- Neues Kapitel „Sicherheitsberichte“ hinzugefügt
- Ansprechpartner für Informationssicherheit in MTB Markenanweisung MA_13_1_09 – Management von Informationssicherheitsvorfällen verschoben
- Neuer Anweisungsname
- Die zugewiesene neue Dokumentennummer "MA_13_1_06" - war "MAN 13.1 Anweisung 7 – Informationssicherheit für Benutzer mit privilegierten IT Rechten".
- Der "MAN 13.1 Anweisung 6 – Management der Informationssicherheit" wurde eine neue Dokumentennummer zugewiesen "MA_13_1_02".

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Informationssicherheitsanforderungen zur Entwicklung sicherer Anwendungen

Ersteller	Steven Rauw erdink Ralf Schlag	**Freigeber**	Andre Wehner	**Version**	3.0
Abt.	FIOS	Abt..	FI	**KSU-Class:**	XX

Gültigkeitsbeginn Datum 01.02.2023	**Geltungsbereich** MAN Truck & Bus SE und deren Tochtergesellschaften	**Genehmigungen (Vorstand)*** **Abgestimmt mit**

* Nur erforderlich, sofern eine Markenanweisung keiner übergeordneten Markenrichtlinie zuzuordnen ist.

Inhalt

Anlagen

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

1 Zweck

Abgeleitet aus der Markenrichtlinie MTB MR_13_1 Informationssicherheit und Markenanweisung MA_13_1_01 Standard für Informationssicherheit definiert diese Markenanweisung MA_13_1_07 – Informationssicherheitsanforderungen zur Entwicklung sicherer Anwendungen die Regeln zur Entwicklung von Software und Anwendungen die bei der MAN Truck & Bus eingesetzt wird.

Zweck dieser Anweisung ist es, den sicheren Softwareentwicklungs-Lebenszyklus (Secure Software Development Life Cycle, SSDLC) von MAN Truck & Bus zu verankern und Sicherheitsanforderungen für sichere Softwareanwendungen zu definieren, die auch vom zertifizierten CSMS (nach UNECE R155 Cybersicherheit) gefordert werden.

Ziel der SSDLC-Aktivitäten ist es, in der MAN Truck & Bus Gruppe einen einheitlichen Prozess zu etablieren, der sicherstellt, dass Informations- und Cybersicherheitsaspekte in der MAN Truck & Bus Gruppe in jeder Phase der Softwareentwicklung ausreichend berücksichtigt werden.

2 Geltungsbereich

Diese Markenanweisung gilt weltweit für die MAN Truck & Bus SE und ihre Tochtergesellschaften sowie deren Mitarbeiter[1]. Sie gilt unmittelbar und bedarf keiner Umsetzungsrichtlinie durch einzelne Tochtergesellschaften. Für Gesellschaften, bei denen die MAN Truck & Bus SE die Geltung der Markenanweisung aus rechtlichen Gründen nicht unmittelbar bewirken kann, ist in Abstimmung mit dem Chief Information Security Officer zu klären, inwieweit diese Markenanweisung Anwendung findet. Dies gilt beispielsweise für Gesellschaften, die sich nicht zu 100 % im Anteilsbesitz der MAN Truck & Bus SE befinden und auch nicht durch einen Beherrschungsvertrag mit der MAN Truck & Bus SE verbunden sind (wie z.B. Gesellschaften, die sich im Anteilsbesitz der MAN Finance and Holding S.A. befinden).

Sofern Gesellschaften eigene Regelungen zu diesem Sachverhalt erlassen haben, sind diese umgehend außer Kraft zu setzen. Bis zur Außerkraftsetzung solcher Regelungen oder Teilen von Regelungen gilt diese Markenanweisung vorrangig.

Sollten Regelungen dieser Markenanweisung aufgrund zwingender lokaler Anforderungen nicht umgesetzt werden können, muss die betroffene Gesellschaft unverzüglich den Chief Information Security Officer der MAN Truck & Bus SE informieren, um notwendige Änderungen oder Ergänzungen zu besprechen.

Das Dokument muss mindestens alle drei Jahre überprüft und gegebenenfalls angepasst werden.

3 Begriffe und Definitionen

Ein Glossar für das gesamte Regelwerk der Informationssicherheit befindet sich in der Zusatzinformation „Begriffe und Definitionen zur Informationssicherheit“.

4 Zielgruppe

Dieses Dokument richtet sich an Mitarbeiter von MAN Truck & Bus, die für die Konzeption und Entwicklung von Softwareanwendungen verantwortlich sind, sowie an deren Führungskräfte.

In einigen Fällen können die Verantwortlichen externe Partner und Lieferanten sein.

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

5 Entwicklung sicherer Anwendungen

5.1 Ziel

Ziel dieses Kapitels ist es, das Auftreten von Schwachstellen in Softwareanwendungen zu verhindern, die durch Design und Implementierung in der Softwareentwicklung im Auftrag oder durch die MAN Truck & Bus Gruppe verursacht werden.

5.2 Softwareentwicklungsprozess

Um sichere Softwareanwendungen zu entwickeln, müssen in allen Phasen des Entwicklungsprozesses
Sicherheitsaspekte berücksichtigt werden. Die Sicherheit muss Bestandteil der funktionalen und technischen Anforderungen eines Anwendungsentwicklungsprozesses sein.

Zunächst müssen funktionale und technische Anforderungen definiert werden. Anschließend sind die Sicherheitsanforderungen im Rahmen der Analyse- und Designphase zu modellieren. Die Secure-Code-Methodik muss befolgt werden, um die Entwicklung sicherer Softwareanwendungen zu gewährleisten.

Jeder Phase des Entwicklungsprozesses muss eine verantwortliche Person oder Einheit zugeordnet werden. Die SSDLC-Phasen sind in der Anlage 1 – Anforderungen zur Entwicklung sicherer Anwendungen dieser Markenanweisung detailliert beschrieben.

Softwareanwendungen, die der Regelung des MAN CSMS unterliegen (wie in der Markenrichtlinie MTB MR_8_103 „Automotive Cyber Security Management System (CSMS) und Software Update Management System (SUMS)“ definiert) und speziell Softwareanwendungen nach AN_MTB_13_508_01 „Einsatz von SSDLC“ müssen die in der Security Knowledge Base spezifizierten MAN-CSMS-SSDLC erfüllen. Die mit diesem Dokument zur Verfügung gestellte MTB Markenanweisung MR_13_1_07 – Informationssicherheitsanforderungen zur Entwicklung sicherer Anwendungen entspricht somit den oben genannten Anweisungen und kann als zusätzliche Informations- und Referenzquelle verwendet werden.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

5.3 Sicherer Softwareentwicklungsprozess

Alle Softwareanwendungen, die in den Anwendungsbereich dieser Anweisung fallen, müssen eine Reihe von Mindestanforderungen für einen sicheren Softwareentwicklungs-Lebenszyklus (SSDLC) erfüllen.

Die folgende Grafik bietet einen umfassenden Überblick über einen sicheren Softwareentwicklungsprozess.

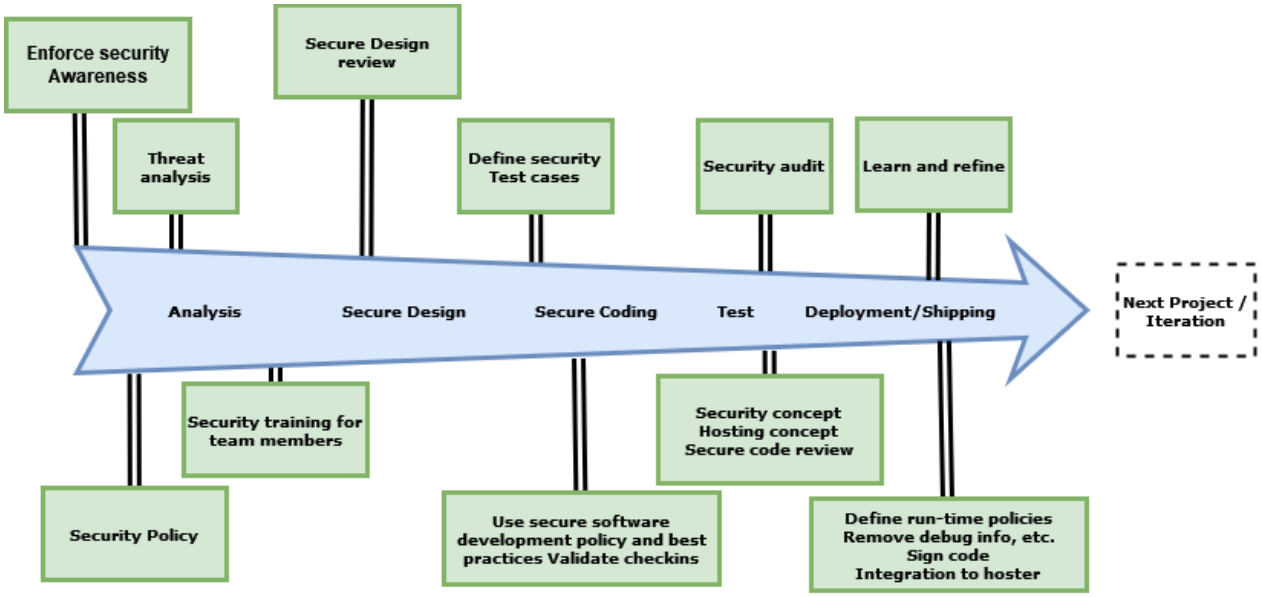


Abbildung 1: Sicherer Softwareentwicklungsprozess

Der Prozess selbst und jede Phase darin sind in Anhang 1 – Anforderungen zur Entwicklung sicherer Anwendungen detailliert beschrieben.

5.4 Ablauf und Organisation

Der MAN Truck & Bus IT-PEP ist eine standardisierte IT-Projektmanagement-Methode. Die Verwendung von IT-PEP ist für Projekte, die bestimmte Kriterien erfüllen, verpflichtend. Alle Softwareentwicklungsprojekte müssen in den Projektphasen wesentliche Meilensteine erreichen (siehe AN_MTB_13_101_03: Verwendung von IT-PEP).

6 SSDLC-Governance

Ziel dieses Prozesses ist es, eine SSDLC-Governance-Funktion bereitzustellen sowie die ISMS-Compliance der entwickelten Softwareanwendungen zu ermöglichen und sicherzustellen. Durch die Schaffung von Verantwortung, Befugnissen und eines angemessenen Kommunikationskanals ermöglicht die SSDLC-Governance den Projekt- und Geschäftsprozessverantwortlichen innerhalb einer Softwareentwicklungsorganisation, Mess- und Kontrollmechanismen für eine sicherere Softwareentwicklung zu etablieren. Ziel der SSDLC-Governance ist es, sicherzustellen, dass die durch den Prozess gelieferten Ergebnisse den strategischen Anforderungen der MAN Truck & Bus Gruppe entsprechen.

SSDLC-Governance hat drei Hauptanliegen:

- Wert verwalten: Das Unternehmen und die Software auf die Organisations-/Projektebene ausrichten, Risiken ausrichten sowie Klarheit und Verantwortlichkeit schaffen.

- Flexibel entwickeln: Globale Ressourcen nutzen, indem agile Entwicklungsentscheidungen ermöglicht und iterative Prozesse zur Risikominderung eingesetzt werden.
- Risiken und Veränderungen steuern: Kontinuierlich Verbesserungen umsetzen, um Risiken zu reduzieren, den Lebenszyklus des Änderungsmanagements zu ermöglichen sowie interne und externe Compliance-Anforderungen zu erfüllen.

6.1 Rollen und Zuständigkeiten der SSDLC-Governance

Im SSDLC-Bereich sind folgende Rollen wichtig, auf denen weitere ISMS-Strukturen und Rollen aufbauen. Weitere Informationen entnehmen Sie bitte der Markenrichtlinie MTB MR_8_103 CSMS & SUMS einschließlich Anlagen.

- **SSDLC-Governance**

  Der SSDLC Governance Lead ist für die allgemeine Einrichtung und Aufrechterhaltung eines angemessenen Sicherheitsniveaus im gesamten SSDLC verantwortlich. Durch Prozesse, Rollen und andere notwendige operative Strukturen stellt der SSDLC Governance Lead sicher, dass die Anforderungen des Regelwerks der Informationssicherheit von MAN sowie des Cyber Security Management Systems im SSDLC-Bereich erfüllt werden. Dazu ist eine enge Zusammenarbeit mit den Geschäftsprozessverantwortlichen erforderlich.

  Details zu der Rolle und den Zuständigkeiten des SSDLC Governance Lead finden Sie in der SSDLC Security Knowledge Base.

- **Geschäftsprozessverantwortlicher**

  Der Geschäftsprozessverantwortliche ist verantwortlich für:

  - Unterstützung der Systemteams bei Fragen rund um die Implementierung
  - Pflege und Aktualisierung der Prozessdokumentation
  - Unterstützung von Maßnahmen zur Erhöhung der Cybersicherheit

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

- Prozessdesign und -überwachung sowie kontinuierliche Verbesserung
- Technischer und funktionaler Support für Systemeigentümer, einschl. Feedbacksammlung von Systemteams und -eigentümern
- Ansprechpartner für die technische Eskalation bei Ausnahmen (einzeln und mit SSDLC-Governance zu bewerten) und Ausführung definierter prozessspezifischer Aktivitäten.

Details zur Rolle und den Zuständigkeiten des Geschäftsprozessverantwortlichen finden Sie in der SSDLC Security Knowledge Base.

- **(Eigentümer eines) System(s)/Produkt(s)**

  Der Eigentümer eins Systems/Produkts ist für die Umsetzung angemessener Sicherheitsanforderungen während des gesamten Lebenszyklus verantwortlich. In diesem Sinne ist die Abstimmung von Sicherheitsanforderungen mit anderen funktionalen Anforderungen sicherzustellen. Der Standard für SSDLC-bezogene Anforderungen ist in der Security Knowledge Base beschrieben. Details zur Rolle und den Zuständigkeiten des SSDLC-System-/-Produkteigentümers finden Sie in der SSDLC Security Knowledge Base.

Details zu den jeweiligen Prozessinhalten und -aktivitäten sind der Anlage 1 – Anforderung zur Entwicklung sicherer Anwendungen sowie der Security Knowledge Base zu entnehmen.

7 Änderungen

Version 3.0

- Neues Dokument erstellt. Die zugewiesene neue Dokumentennummer ist “MA_13_1_07"
- Änderungsprotokoll hinzugefügt
- Umbenennung
- Rollenund Zuständigkeiten hinzugefügt.
- Kapitel „Ablauf und Organisation“ hinzugefügt
- SSDLC-Governance hinzugefügt
- Der "MAN 13.1 Anweisung 7 – Informationssicherheit für Benutzer mit privilegierten IT Rechten" wurde eine neue Dokumentennummer zugewiesen "MA_13_1_06 Informationssicherheit für Systembetrieb und Administration".

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

I. **Anlage 1:** Anforderungen zur Entwicklung sicherer Anwendungen

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Anlage 1 - Anforderungen zur Entwicklung sicherer Anwendungen

Ersteller	Steven Rauw erdink Ralf Schlag	**Freigeber**	Andre Wehner	**Version**	1.0
Abt.	FIOS	Abt..	FI	**KSU-Class:**	xx

Gültigkeitsbeginn Datum 01.02.2023	**Geltungsbereich** MAN Truck & Bus SE und deren Tochtergesellschaften	**Genehmigungen (Vorstand)*** **Abgestimmt mit**

* Nur erf orderlich, sofern eine Markenanweisung keiner übergeordneten Markenrichtlinie zuzuordnen ist.

Inhalt

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

1 Zweck

Zweck dieser Anlage ist es, die SSDLC-Prozessphasen und Reifegrade gemäß der MTB Markenrichtlinie MR_13_1 Informationssicherheit und Markenanweisung MA_13_1_07 – Informationssicherheitsanforderungen zur Entwicklung sicherer Anwendungen zu definieren und zu beschreiben. Des Weiteren werden die Informationssicherheitsanforderungen für die Entwicklung von Software durch externe Dienstleister beschrieben.

2 Security Knowledge Base

Die Security Knowledge Base ist der zentrale Speicherort für Anforderungen und Kenntnisse des CSMS-SSDLC wie in AN_MTB_13_5_508_01 „Einsatz von SSDLC“ spezifiziert. Diese Anforderungen können für jedes Softwareentwicklungsprojekt angewendet werden und die Knowledge Base kann als wertvolle Informationsquelle dem Zweck dienen, die minimalen SSDLC-Anforderungen in der MAN Truck & Bus Gruppe zu erfüllen.

3 Reifegrade in SSDLC

Basierend auf dem Rahmenwerk des OWASP SAMM wurde für die einzelnen Aktivitäten ein Ziel-Reifegrad definiert, den Softwareentwicklungsteams erreichen müssen, um die Anforderungen mit ausreichenden Sicherheitskontrollen zum Schutz von Informationssicherheits- und Cybersicherheits-Aspekten in Bezug auf die Entwicklung und den Betrieb von IT-Systemen zu erfüllen. Jeder Reifegrad innerhalb einer Sicherheitspraxis zeichnet sich durch ein sukzessive anspruchsvolleres Ziel aus, das durch bestimmte Aktivitäten definiert ist, und durch strengere Erfolgskennzahlen als der vorherige Reifegrad. Darüber hinaus kann jede Sicherheitspraxis unabhängig von anderen verbessert werden, auch wenn verbundene Aktivitäten zu den Optimierungen führen können.

	Reifegrade 1	Reifegrade 2	Reifegrade 3
Governance			
Strategie und Kennzahlen	Ziele und Mittel zur Messung der Wirksamkeit des Sicherheitsprogramms ermitteln.	Eine einheitliche strategische Roadmap für die Softwaresicherheit innerhalb des Unternehmens erstellen.	Sicherheitsbemühungen mit den relevanten organisatorischen Indikatoren und Asset-Werten abstimmen.
Richtlinien und Compliance	Governance- und Compliance-Treiber ermitteln und dokumentieren, die für das Unternehmen relevant sind.	Anwendungsspezifische Sicherheits- und Compliance-Grundlagen erstellen.	Einhaltung von Richtlinien, Standards und Anforderungen Dritter messen.
Schulung und Anleitung	Mitarbeitern Zugang zu Ressourcen rund um die Themen sichere Entwicklung und Bereitstellung anbieten.	Alle Mitarbeiter im Software-Lebenszyklus mit technologie- und rollenspezifischen Anleitungen zur sicheren Entwicklung schulen.	Interne Schulungsprogramme entwickeln, die von Entwicklern in verschiedenen Teams unterstützt werden.
Design			
Bedrohungsbeurteilung	Best-Effort-Erkennung schwerer Bedrohungen für das Unternehmen und einzelne Projekte.	Standardisierung und unternehmensweite Analyse von softwarebezogenen Bedrohungen innerhalb des Unternehmens.	Proaktive Verbesserung der Bedrohungsabdeckung im gesamten Unternehmen.

	Reifegrade 1	Reifegrade 2	Reifegrade 3
Design			
Sicherheits-anforderun-gen	Die Sicherheit während des Softwareanforde-rungssprozesses explizit berücksichtigen	Granularität von aus der Geschäftslogik und bekannten Risiken abgeleiteten Sicherheits-anforderungen erhöhen	Sicherheitsanforderungs-prozess für alle Softwareprojekte und Abhängigkeiten Dritter anordnen
Sicherheitsar-chitektur	Berücksichtigung proak-tiver Sicherheitshinweise in den Software-Designprozess integrieren	Den Software-Designprozess auf bekannte sichere Dienste und „Secure-by-Default"-Designs ausrichten	Den Software-Designprozess formell kontrollieren und Nutzung sicherer Komponenten validieren.
Implementierung			
Sicherer Build-Prozess	Der Build-Prozess ist wiederholbar und konsistent	Der Build-Prozess ist optimiert und vollständig in den Arbeitsablauf integriert	Der Build-Prozess verhindert, dass bekannte Fehler in die Produktionsumgebung gelangen
Sichere Bereitstellung	Bereitstellungsprozesse werden vollständig dokumentiert	Bereitstellungsprozesse umfassen Meilensteine bei der Sicherheitsüberprüfung	Der Bereitstellungsprozess ist vollständig automatisiert und umfasst die automatisierte Überprüfung aller kritischen Meilensteine
Fehlerma-nagement	Alle Fehler werden innerhalb jedes Projekts verfolgt	Fehlerverfolgung zur Beeinflussung des Bereitstellungsprozesses	Die Fehlerverfolgung über mehrere Komponenten hinweg wird genutzt, um die Zahl neuer Fehler zu reduzieren
Überprüfen			
Architektur-bewertung	Überprüfung der Architektur, um sicherzustellen, dass für typische Risiken eine Basis-Mitigation vorhanden ist	Überprüfung der vollständigen Bereitstellung von Sicherheitsmechanismen in der Architektur	Überprüfung der Effektivität der Architektur und der Feedback-Ergebnisse zur Verbesserung der Sicherheitsarchitektur
Prüfung nach Anforderun-gen	Opportunistisch grundlegende Schwachstellen und andere Sicherheitsprobleme finden	Implementierungsprüfung durchführen, um anwendungsspezifische Risiken anhand der Sicherheitsanforderungen zu ermitteln	Anwendungssicherheitsniveau nach Fehlerbehebungen und Änderungen oder während der Wartung aufrechterhalten
Sicherheits-tests	Sicherheitstests (manuell und toolbasiert) durchführen, um Sicherheitsmängel zu erkennen	Sicherheitstests während der Entwicklung durch Automatisierung, die durch regelmäßige manuelle Sicherheits-Penetrationstests ergänzt wird, vollständiger und effizienter durchführen	Sicherheitstests als Bestandteil der Entwicklungs- und Bereitstellungsprozesse einbetten

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

	Reifegrade 1	Reifegrade 2	Reifegrade 3
		Betrieb	
Vorfallmanagement	Best-Effort-Vorfallerkennung und -bearbeitung	Formeller Vorfallmanagementprozess vorhanden	Effektives Vorfallmanagement
Umweltmanagement	Best-Effort-Patchen und -Härten	Formeller Prozess mit Grundlagen vorhanden	Konformität mit kontinuierlichen Prozessverbesserungen durchgesetzt
Betriebsmanagement	Grundlegende Praktiken	Gesteuerte, reaktionsschnelle Prozesse	Aktive Überwachung und Reaktion

4 Sicherer Softwareentwicklungsprozess

4.1 Analysephase

- Es muss eine Risikobewertung durchgeführt werden, bei der bestehende Bedrohungen analysiert, das Risiko bewertet und angemessene Sicherheitsanforderungen durch Anwendung des ISi-Bewertungsprozesses definiert werden.
- Alle Sicherheitsanforderungen aus einschlägigen Anweisungen, Richtlinien und Sicherheitskonzepten sowie anwendungsspezifische Anforderungen müssen identifiziert und dokumentiert werden.
- Alle Mitarbeiter, die an einem Softwareentwicklungsprojekt teilnehmen, müssen zu Sicherheitsaspekten in ihrem Bereich geschult werden. Diese Schulung muss den geeigneten Einsatz von Softwareentwicklungswerkzeugen, Technologien, Rahmenwerken und Programmiersprachen sowie einschlägiger Bibliotheken umfassen.

4.2 Sichere Designphase

- Basierend auf den identifizierten Sicherheitsanforderungen muss eine sichere Architektur entworfen werden. Detaillierte Sicherheitsmaßnahmen müssen gemäß der Anforderung aus der ISi-Bewertung festgelegt werden.
- Es ist ein Sicherheitskonzept zu erarbeiten. Dieses muss die zu ergreifenden Sicherheitsmaßnahmen enthalten.
- Überprüfung aller Sicherheitsanforderungen für ausgewählte:
  - Technologien,
  - Softwareentwicklungswerkzeuge,
  - Rahmenwerke,
  - Programmiersprachen und einschlägige Bibliotheken
- Die Sicherheit der Architektur muss in einer Architekturprüfung bewertet werden. Die Architekturprüfung muss von Entwicklern durchgeführt werden, die über das erforderliche

Fachwissen verfügen und das Vier-Augen-Prinzip anwenden, wenn das Design erheblich verändert wird.

- Alle identifizierten Fehler, die sich aus der Architekturprüfung ergeben, sind zu adressieren bzw. die identifizierten Restrisiken sind formell anzunehmen.
- Die Entwicklungs- und Testumgebungen von Softwareanwendungen müssen von der Produktionsumgebung getrennt sein.

4.3 Sichere Kodierphase

- Die Kodierung muss gemäß der definierten Architektur und der entsprechenden Spezifikation der Sicherheitsanforderungen erfolgen.
- Die für die Anwendungsentwicklung verantwortliche Organisation muss Kodierungsrichtlinien definieren.
- Architekturänderungen und Abweichungen von den spezifizierten Sicherheitsanforderungen müssen eine Überprüfung der ISi-Bewertung nach sich ziehen.
- Die Prüfung des Secure Codes muss anhand folgender Tests durchgeführt werden, sofern diese zutreffend sind:
    - Static Application Security Testing (SAST) - Analyse des Quellcodes auf bekannte Schwachstellen.
    - Vor der Bereitstellung muss der Code auf die definierten Sicherheitsanforderungen und -maßnahmen hin überprüft werden.
    - Werden Softwaremodule von Dritten entwickelt, folgen diese den gleichen Informationssicherheitsanforderungen von MAN Truck & Bus.
    - Das Risiko muss mittels einer Risikobewertung (ISi-Bewertung) bewertet werden. Es ist zu prüfen, ob die Implementierung oder Integration einer neuen Anwendung/Software sensible Informationen und die Cybersicherheit der MAN Truck & Bus Gruppe beeinträchtigt.
    - Sofern identifizierte Risiken nicht einzugrenzen sind, müssen sie gemäß dem in MTB 13.1 Anweisung 10 – Handhabung von Ausnahmen beschriebenen Prozess formell angenommen werden.
    - Erkannte Fehler müssen dokumentiert und behoben werden.
    - Bei Designfehlern muss das Sicherheitskonzept vor dem Einsatz in der Produktions-umgebung aktualisiert und freigegeben werden.
- Für Anwendungen, die Informationen mit hohem oder sehr hohem Schutzbedarf verarbeiten, muss die Codeprüfung die folgenden zusätzlichen Aspekte abdecken:
    - Eingabe- und Ausgabedatenvalidierung.
    - korrekte Verarbeitung von Daten innerhalb der Anwendung.
    - Authentizität und Schutz der Nachrichtenintegrität.

4.4 Testphase

Die Testphase wird nach dem Einsatz der Softwareanwendung in der Testumgebung durchgeführt. Die Tests ermöglichen es, zu verifizieren, dass die gesamte Softwareanwendung in Übereinstimmung mit den Sicherheitsspezifikationen funktioniert, und sicherzustellen, dass

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

alle Sicherheitsanforderungen erfüllt werden. Die Tests müssen mindestens folgende Aspekte abdecken:

- Automatisierter Scan der Softwareanwendung auf bekannte Schwachstellen
- Dynamic Application Security Tests (DAST) - Analyse der laufenden Anwendung auf bekannte Schwachstellen
- Abhängigkeitsprüfung – Prüfung von Abhängigkeiten der Anwendung auf bekannte Schwachstellen
- Statische Anwendung
- Bei Designfehlern muss das Sicherheitskonzept vor dem Einsatz in der Produktionsumgebung auf der Grundlage der Ergebnisse der Tests aktualisiert werden.

4.5 Code-Signierung

Die Code-Signierung validiert den Code für die Verwendung in speziellen Umgebungen. Sie bestätigt, dass alle erforderlichen Tests durchgeführt und erfolgreich bestanden wurden. So können Software/Anwendungen während der Laufzeit validiert werden.

Die Code-Signierung sollte als formeller Freigabeprozessschritt erfolgen. Um eine Ablehnung zu verhindern, müssen ausführbare Dateien, Softwaremodule und Skripte digital signiert werden. Hierzu muss ein zentraler Codesignierdienst verwendet werden.

4.6 Bereitstellung

Die Bereitstellung ist der Schritt, bei dem die Software/Anwendung in ihrer endgültigen Zielinfrastruktur bereitgestellt wird. Der zuständige Einsatzleiter validiert die Freigaben und prüft auf einen angemessenen Wartungsplan und den Rollback-Plan. Der Einsatzleiter beobachtet die Rollback-Bedingungen und entscheidet im Fehlerfall über die Durchführung der Rollback-Schritte.

5 Softwareentwicklung durch externe Dienstleister

Softwareentwicklungsleistungen, die von externen Dienstleistern erbracht werden, müssen den gleichen Anforderungen an eine sichere Softwareentwicklung entsprechen wie die interne Entwicklung bei MAN Truck & Bus. Diese Anforderungen und der geforderte Reifegrad werden in der zugehörigen vertraglichen Vereinbarung geregelt und beinhalten auch ein Auditrecht des Dienstleisters durch MAN Truck & Bus gemäß Markenrichtlinie MR_13_1_08, Anlage 1 – Methoden und Anforderungen der Lieferantenverifikation.

Dabei sind insbesondere folgende Themen zu beachten:

- Externe Dienstleister müssen die festgelegten Sicherheitskonzepte befolgen und Risiko-bewertungen durchführen.
- Externe Dienstleister müssen die in Kapitel 4.3 definierten Kodierungsrichtlinien beachten.
- Codeprüfung und -tests müssen erfolgen und die Ergebnisse müssen dokumentiert werden.
- Die extern entwickelte Software muss im Rahmen der ISi-Bewertung für das entsprechende Projekt bewertet werden.
- Je nach Ergebnis der ISi-Bewertung kann ein unabhängiger externer Penetrationstest erforderlich sein
- Erkannte Schwachstellen müssen rechtzeitig und ordnungsgemäß bearbeitet werden.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

6 Änderungen

Version 1.0

- Erstfassung

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Informationssicherheit für Lieferanten

Ersteller	Steven Rauw erdink Ralf Schlag	**Freigeber**	Andre Wehner	**Version**	3.0
Abt.	FIOS	Abt..	FI	**KSU-Class:**	xx

Gültigkeitsbeginn Datum 01.02.2023	**Geltungsbereich** MAN Truck & Bus SE und deren Tochtergesellschaften	**Genehmigungen (Vorstand)*** **Abgestimmt mit**

* Nur erf orderlich, sofern eine Markenanweisung keiner übergeordneten Markenrichtlinie zuzuordnen ist.

Inhalt

Anlagen

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

1 Zweck

Abgeleitet von der Markenrichtlinie MTB MR_13_1 Informationssicherheit und Markenanweisung MTB MA_13_1_01 – Standard für Informationssicherheit definiert und beschreibt diese Markenanweisung die Anforderungen an die Informationssicherheit für das Management von Lieferanten, die für die IT-Services, -Systeme und -Infrastruktur von MAN Truck & Bus verantwortlich sind oder diese im Auftrag von MAN Truck & Bus abwickeln.

Bei der Inbetriebnahme, Zusammenarbeit und Kontrolle von Dienstleistern, die für die Entwicklung, die Installation, den Betrieb und die Konfiguration von MAN Truck & Bus ICT Systeme verantwortlich sind, haben die verantwortlichen Anwendungs-/Systeminhaber sicherzustellen, dass die Anforderungen dieser Markenanweisung angemessen berücksichtigt und erfüllt werden.

Unter Berücksichtigung der Art und des Umfangs der Aufgaben des Lieferanten sind in den vertraglichen Vereinbarungen mit den Lieferanten die im Rahmen der Informationssicherheit der MAN Truck & Bus Gruppe festgelegten Regelungen anzuwenden.

Bestehende Verträge müssen nicht geändert werden. Bei Verträgen, die einer Verlängerung unterliegen, ist die Notwendigkeit von Vertragsänderungen oder -ergänzungen zu bewerten. Ausnahmen, die sich aus der Bewertung und eventuellen Risikoübernahmen ergeben können, sind gemäß den Regelungen der Markenanweisung MTB MA_13_1_10 Ausnahmebehandlung zu behandeln.

2 Geltungsbereich

Diese Markenanweisung gilt weltweit für die MAN Truck & Bus SE und ihre Tochtergesellschaften sowie deren Mitarbeiter[1]. Sie gilt unmittelbar und bedarf keiner Umsetzungsrichtlinie durch einzelne Tochtergesellschaften. Für Gesellschaften, bei denen die MAN Truck & Bus SE die Geltung der Markenanweisung aus rechtlichen Gründen nicht unmittelbar bewirken kann, ist in Abstimmung mit dem Chief Information Security Officer zu klären, inwieweit diese Markenanweisung Anwendung findet. Dies gilt beispielsweise für Gesellschaften, die sich nicht zu 100 % im Anteilsbesitz der MAN Truck & Bus SE befinden und auch nicht durch einen Beherrschungsvertrag mit der MAN Truck & Bus SE verbunden sind (wie z.B. Gesellschaften, die sich im Anteilsbesitz der MAN Finance and Holding S.A. befinden).

Sofern Gesellschaften eigene Regelungen zu diesem Sachverhalt erlassen haben, sind diese umgehend außer Kraft zu setzen. Bis zur Außerkraftsetzung solcher Regelungen oder Teilen von Regelungen gilt diese Markenanweisung vorrangig.

Sollten Regelungen dieser Markenanweisung aufgrund zwingender lokaler Anforderungen nicht umgesetzt werden können, muss die betroffene Gesellschaft unverzüglich den Chief Information Security Officer der MAN Truck & Bus SE informieren, um notwendige Änderungen oder Ergänzungen zu besprechen.

Das Dokument muss mindestens alle drei Jahre überprüft und gegebenenfalls angepasst werden.

3 Begriffe und Definitionen

Ein Glossar für den gesamten Informationssicherheitsrahmen befindet sich in der Zusatzinformation „Begriffe und Definitionen in der Informationssicherheit“.

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

4 Zielgruppe

Die Markenanweisung MA_13_1_08 Informationssicherheit für Lieferanten richtet sich an Mitarbeiter, die für das Management von Lieferanten innerhalb der MAN Truck & Bus Gruppe verantwortlich sind.

5 Informationssicherheit von MAN Truck & Bus IKT-Systemen

Informationen sind eine wichtige Ressource der MAN Truck & Bus Gruppe. Geschäfts- und Produktionsprozesse funktionieren nur, wenn die richtigen Informationen zur richtigen Zeit und am richtigen Ort zur Verfügung stehen. Der wirksame Schutz dieser Informationsressourcen in den IKT-Systemen der MAN Truck & Bus Gruppe ist ein entscheidender Faktor für den Geschäftserfolg des Unternehmens.

Da die Informationsressourcen täglich einer Vielzahl von Bedrohungen ausgesetzt sind, wie beispielsweise:

- Zerstörung oder Verschlüsselung von Informationen durch Computerviren,
- Diebstahl von Informationen durch Ausspähen von Passwörtern,
- Diebstahl von Datenträgern, Smartphones und Computern,
- Ausfall von MAN Truck & Bus IKT-Systemen durch Stromausfall, Sabotage oder Vandalismus,
- Zerstörung von wichtigen Daten durch Feuer oder Wasser,

sind besondere Maßnahmen zu ihrem Schutz erforderlich. Ein wirksamer Schutz ist nur dann möglich, wenn er auf einem breiten Spektrum von miteinander verknüpften Maßnahmen und Schutzvorkehrungen beruht.

Zu den erforderlichen Maßnahmen zur Gewährleistung der Informationssicherheit gehören neben den im MAN Truck & Bus Rahmenwerk zur Informationssicherheit genannten Maßnahmen insbesondere auch:

- Eine Sicherheitskultur bei allen Mitarbeitern eines Dienstleistungsunternehmens.
- Die Einhaltung der festgelegten Prozesse und Verfahren.
- Die Sicherstellung eines angemessenen Umgangs mit Informations- und Kommunikationsgeräten und von Software und deren Schutz.
- Eine risikoorientierte angemessene Berichterstattung über die Umsetzung und Wirksamkeit des Informationssicherheitsmanagements des Dienstleisters an MAN Truck & Bus.
- Das Recht, relevante Aspekte der Informationssicherheit zu prüfen (auch beim Dienstleister).

Der Begriff „risikoorientiert“ bezieht sich auf die Risiken der Geschäftsprozesse der MAN Truck & Bus Gruppe und muss mit MAN Truck & Bus abgestimmt werden.

6 Verantwortlichkeiten des Dienstleisters

Alle Mitarbeiter eines MAN Truck & Bus Servicelieferanten, die für die Konfiguration der MAN Truck & Bus IKT-Systeme verantwortlich sind, müssen sicherstellen, dass die Konfiguration mit den relevanten Informationssicherheitsvorschriften der MAN Truck & Bus Gruppe übereinstimmt. Insbesondere:

- Alle Anwendungsentwickler und Systemarchitekten eines MAN Truck & Bus Dienstleisters sind verantwortlich für ein sicheres Design, adäquate Sicherheitsspezifikationen, angemessene Tests und die Migration der MAN Truck & Bus IKT-Systeme in Übereinstimmung mit den relevanten MAN Truck & Bus Informationssicherheitsvorschriften.
- Alle Mitarbeiter eines MAN Truck & Bus Servicelieferanten mit Betriebsverantwortung haben die Betriebssicherheit der IKT-Systeme gemäß den einschlägigen MAN Truck & Bus Informationssicherheitsvorschriften zu gewährleisten. Dabei muss der Dienstleister auf mögliche

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Bedrohungen achten, die Ansprechpartner der MAN Truck & Bus Gruppe über festgestellte Bedrohungen informieren und verhindern, dass Informationen unnötig gefährdet werden.

Das Informationssicherheitsmanagement von MAN Truck & Bus wird auf der Basis eines risikogerechten Ansatzes umgesetzt. Dabei werden die Risiken für die jeweiligen Geschäftsprozesse berücksichtigt.

Alle Dienstleister der Unternehmen der MAN Truck & Bus Gruppe sind verpflichtet, Risiken im Zusammenhang mit dem erbrachten Dienstleistungsbereich zu identifizieren und in Abstimmung mit der IS-Organisation von MAN Truck & Bus zu managen.

Abhängig von den Anforderungen der MAN Truck & Bus Gruppe und der damit verbundenen Dienstleistung muss der Lieferant Folgendes erfüllen:

- Unterstützung der von der MAN Truck & Bus Gruppe definierten Informationssicherheitsziele in geeigneter Weise.
- Einhaltung des MAN Truck & Bus Rahmenwerks für Informationssicherheit als verbindlicher Rahmen für alle erbrachten Dienstleistungen.
- Bei Bedarf sind auf der Grundlage des MAN Truck & Bus Rahmenwerks für Informationssicherheit zusätzliche Anweisungen für den Verantwortungsbereich des Dienstleisters zu erarbeiten.
- Bereitstellung ausreichender Ressourcen für die Einrichtung, die Umsetzung, den Betrieb, die Überwachung, die Kontrolle, die Wartung und die ständige Verbesserung des Informationssicherheitsmanagements.
- Es sind mindestens die Mindestanforderungen von MAN Truck & Bus an die Informationssicherheit für die Dienstleistung zu erfüllen.
- Zu berücksichtigen ist ferner die Verfügbarkeit, Vertraulichkeit und Integrität von Informationsressourcen/IT-Diensten/IKT-Systemen gemäß den Anforderungen von MAN Truck & Bus an das Risikomanagement des Lieferanten.
- Entwicklung von Risikobehandlungsplänen oder Maßnahmen für alle identifizierten inakzeptablen Risiken im Zusammenhang mit den Dienstleistungen, die der Lieferant für die MAN Truck & Bus Gruppe erbringt.
- Sicherstellung der Durchführung unabhängiger Bewertungen zur Verbesserung der Informationssicherheit.
- Regelmäßige Überprüfung des Informationssicherheitsniveaus durch das eigene Management.
- Gemeinsam mit der MAN Truck & Bus sind das Sicherheitsniveau und entsprechende Indikatoren zu definieren, die den Risiken angemessen sind. Diese sind regelmäßig an MAN Truck & Bus zu berichten.
- Ermittlung und Handhabung rechtlicher und regulatorischer Anforderungen und vertraglicher Verpflichtungen im Zusammenhang mit der Informationssicherheit.
- Sicherstellung, dass die erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen für den Umgang mit personenbezogenen Daten in Übereinstimmung mit den geltenden Vorschriften umgesetzt werden.
- Rechtzeitige Meldung von Informationssicherheitsvorfällen gemäß den festgelegten Anforderungen.
- Förderung des Bewusstseins für die Informationssicherheit und gegebenenfalls Verbesserung dieses Bewusstseins durch Schulungsmaßnahmen.
- Einrichtung und Weitergabe von internen und externen Anlaufstellen und Informationsquellen für die Informationssicherheit.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

- Berücksichtigung von Anforderungen an die Gestaltung und den Betrieb von IKT-Systemen.

Die Umsetzung dieser Anforderungen muss in nachprüfbarer Form dokumentiert werden, um den Anforderungen von Audits und der Handhabung von eventuellen Haftungsansprüchen zu genügen.

6.1 Ansprechpartner für Informationssicherheit

Falls vertraglich vorgeschrieben, müssen die Dienstleister einen Verantwortlichen für Informationssicherheit benennen, der sich mit allen Fragen der Informationssicherheit befasst. Dieser Mitarbeiter fungiert als Ansprechpartner für den CISO oder die Informationssicherheitsorganisation von MAN Truck & Bus.

Der CISO der MAN Truck & Bus Gruppe ist der verantwortliche Ansprechpartner des Dienstleisters für alle unternehmens- und konzernweiten Themen der Informationssicherheit. Dies gilt insbesondere für den Umgang mit Vorfällen im Bereich der Informationssicherheit.

Fragen im Zusammenhang mit dem Schutz personenbezogener Daten in den Unternehmen der MAN Truck & Bus Gruppe sind dem zuständigen Datenschutzbeauftragten oder der Datenschutzabteilung der MAN Truck & Bus Gruppe zu melden (siehe hierzu die Markenrichtlinie MTB MR_04_6 Umgang mit personenbezogenen Daten und Datenschutzorganisation).

6.2 Standard für Informationssicherheit

Sofern vertraglich festgelegt, sind die Dienstleister der MAN Truck & Bus Gruppe verpflichtet, ein funktionsfähiges Informationssicherheitsmanagementsystem (ISMS) auf Basis der Norm ISO 27001 zu implementieren, aufrechtzuerhalten und kontinuierlich zu verbessern.

6.3 Verifizierung und Anforderungen an Lieferanten

Die Informationssicherheitsorganisation von MAN Truck & Bus legt die Anforderungen an die Lieferanten zur Erbringung sicherer Dienstleistungen fest. Diese stehen im Zusammenhang mit der Klassifizierung von Informationen und dem Schutzniveau, das die entsprechende Dienstleistung erfordert (siehe Markenanweisung MTB MA_13_1_03 Klassifizierung von Informationsressourcen).

Der verantwortliche Diensteigentümer stellt sicher, dass die Anforderungen an die Informationssicherheit überprüft und erfüllt werden, bevor der Vertrag über die Erbringung der Dienstleistung unterzeichnet wird.

Um den Risiken der Informationssicherheit angemessen begegnen zu können, müssen die Lieferanten bei hohem oder sehr hohem Schutzbedarf über eine gültige Zertifizierung der Informationssicherheit verfügen (z. B. ISO 27001 oder TISAX).

Legt ein potenzieller Lieferant keine gültige Zertifizierung vor, kann ein Vertrag nur dann geschlossen werden, wenn er sich verpflichtet, sich innerhalb einer bestimmten Frist zertifizieren zu lassen (der Vertrag muss eine besondere Klausel enthalten, in der diese Abweichung und die Forderung nach einer Zertifizierung beispielsweise innerhalb von 9 Monaten beschrieben wird).

Dieses Prüfverfahren bestätigt die Konformität und Eignung des Lieferanten für die Erbringung der jeweiligen Dienstleistung und den Umgang mit Informationen im Auftrag von MAN Truck & Bus.

Ausführliche Informationen über die Verifizierung und die Anforderungen an Lieferanten befinden sich im Anhang: Markenanweisung MTB MA_13_1_08 Informationssicherheit für Lieferanten, Anlage 1 - Verfahren und Anforderungen zur Überprüfung von Lieferanten.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

6.4 Berichterstattung

Die Lieferanten sind verpflichtet, auf Anforderung der MAN Truck & Bus regelmäßig Berichte über das Sicherheitsniveau vorzulegen. Einige Beispiele für Berichte sind im Folgenden aufgeführt:

- **Einhaltung von Richtlinien** – Die Systembetreiber und Systemadministratoren müssen die Einhaltung der Informationssicherheitsrichtlinien, der Anweisungen und Vorschriften der MAN Truck & Bus Gruppe bestätigen. Sie müssen die Richtlinien, die Anweisungen und Vorschriften kennen und einhalten. Dieser Bericht wird jährlich vorgelegt.
- **Systemzugriff** – Es ist eine aktuelle Liste aller Mitarbeiter zu führen, die Zugang zu den Systemen haben. Dieser Bericht wird vierteljährlich vorgelegt.
- **Änderungen im Systemzugang** – Es ist eine Liste mit allen Änderungen im Systemzugang zu Diensten einschließlich der Lieferanten zu führen. Dieser Bericht wird vierteljährlich vorgelegt.
- **Systemzugriffsrechte** – Es ist eine Liste der Rollen und Zugriffsrechte des einzelnen Mitarbeiters zu führen. Dieser Bericht wird vierteljährlich vorgelegt.
- **Management von Änderungen der Systemsicherheit** – Es ist eine Liste von Systemänderungen in Bezug auf die Informationssicherheit zu führen. Dieser Bericht wird vierteljährlich vorgelegt.
- **Management von Sicherheitsereignissen und Sicherheitsvorfällen** – Es ist eine Liste aller aufgetretenen/entdeckten sicherheitsrelevanten Ereignisse und Vorfälle zu führen. Dieser Bericht wird vierteljährlich vorgelegt.
- **Management von Sicherheitsvorfällen - Reaktionszeit** – Es ist eine Liste aller Reaktionszeiten auf Sicherheitsvorfälle und über Überprüfungen der Einhaltung des Prozesses für das Management von Sicherheitsvorfällen in der MAN Truck & Bus Gruppe zu führen. Dieser Bericht wird vierteljährlich vorgelegt.
- **Systemanalyse-Tools** – Darstellung und Beschreibung des Einsatzes von Sicherheits-Tools im Rahmen der Systembereitstellung (Firewalls, Antivirus, Patch-Management, inkl. deren Versionen). Dieser Bericht wird vierteljährlich vorgelegt.
- **Patch-Management (do)** – Es ist ein Bericht über die Anwendung aller aufgeführten kritischen Patches zu erstellen. Dieser Bericht wird vierteljährlich vorgelegt.
- **Patch-Management (check)** – Es ist ein Bericht über die regelmäßige Überprüfung der Patch-Levels aller Systeme zu erstellen. Dieser Bericht wird vierteljährlich vorgelegt.
- **Antivirus-Management (do)** – Es ist zu dokumentieren, dass alle zentral verwalteten Systeme über einen installierten Viren- und Malware-Schutz verfügen. Dieser Bericht wird vierteljährlich vorgelegt.
- **Antivirus-Management (check)** – Es ist zu dokumentieren, dass alle Systeme regelmäßig gescannt werden und die neuesten empfohlenen Versionen verwendet werden. Dieser Bericht wird vierteljährlich vorgelegt.
- **Systemrisikobericht** – Darstellung von Risiken im Zusammenhang mit der Informationssicherheit, die identifiziert, dokumentiert und verwaltet werden. Dieser Bericht wird vierteljährlich vorgelegt.
- **Berichte über Systemaudits** – Darstellung des Status aller Prüfungsfeststellungen und von Lücken und Prüfungsergebnissen sowie eine Dokumentation, ob sie regelmäßig überprüft/aktualisiert werden. Dieser Bericht wird jährlich vorgelegt.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

- **Standardbericht zum Systemdatenschutz** – Darstellung des Stands der durchgeführten Maßnahmen zur Einhaltung der Datenschutzbestimmungen. Dieser Bericht wird jährlich vorgelegt.
- **Bericht über Vorfälle beim Systemdatenschutz** – Darstellung aller Vorfälle, die aus Sicht des Datenschutzes aufgetreten sind, einschließlich einer Beschreibung der Maßnahmen zur Vermeidung derartiger Vorfälle. Dieser Bericht ist regelmäßig pro Vorfall zu erstellen und unmittelbar nach Abschluss der Analyse des Vorfalls vorzulegen.

7 Allgemeine Anforderungen an IKT-Systeme und IT-Dienstleister

- Für jeden einzelnen Mitarbeiter des Lieferanten, der für die Konfiguration der IKT-Systeme der MAN Truck & Bus Gruppe verantwortlich ist, müssen die Kompetenzen (Rechte und Pflichten) des Mitarbeiters definiert und dokumentiert werden.
- Die Fähigkeiten der Mitarbeiter müssen der Aufgabe entsprechen.
- Der Dienstleister muss die Aufgaben angemessen trennen, um den Missbrauch von IKT-Systemen zu verhindern.
- Die erforderlichen Ressourcen für die Gewährleistung der Betriebssicherheit müssen geplant und bereitgestellt werden.
- Die Mitarbeiter müssen hinsichtlich der Bedeutung der Informationssicherheit für den Erfolg von MAN Truck & Bus sensibilisiert werden.
- Es muss regelmäßig eine bedrohungsbasierte Bewertung der Informationssicherheitsrisiken im Zusammenhang mit dem angebotenen Dienst und eine Anpassung an die Anforderungen durchgeführt werden.

7.1 Erfordernis der Integration in das Risikomanagement

Das Risiko- und Chancenmanagement (ROM) ist in der MAN Truck & Bus Gruppe geregelt und zielt darauf ab, Risiken und Chancen frühzeitig zu erkennen, Chancen mit Erfolgspotenzial zu managen und Risiken, die das Unternehmen gefährden könnten, zu vermeiden.

Ein Dienstleister, der Dienstleistungen für IKT-Systeme zur Unterstützung der Geschäftsprozesse von MAN Truck & Bus anbietet, muss eine Risikoanalyse erstellen. Die Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen müssen anhand realistischer Bedrohungsszenarien ermittelt werden. Für die Bewertung der Brutto- und Nettorisiken sind die Eintrittswahrscheinlichkeit und die Auswirkung auf die Informationen einmal ohne Berücksichtigung von Risikobehandlungsmaßnahmen und einmal mit Berücksichtigung der Maßnahmen zu bewerten.

Die Entscheidung über die Auswahl geeigneter Informationssicherheitsmaßnahmen zur Beherrschung der Risiken muss gemeinsam zwischen dem Dienstleistungserbringer und dem Verantwortlichen für die Dienstleistung bei MAN Truck & Bus getroffen werden.

Dabei müssen die Mindestanforderungen aus dem Informationssicherheitsrahmen von MAN Truck & Bus oder eine gleichwertige Reihe von Sicherheitsanforderungen angewendet werden.

7.2 Anforderungen an die Gestaltung von IKT-Systemen

Die Anforderungen werden in Kapitel 6.1 der Markenanweisung MTB MA_13_1_06 Informationssicherheit für Systembetrieb und Systemverwaltung ausführlich beschrieben.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

7.3 Anforderungen an die Gestaltung von Netzwerken

Die Anforderungen werden in Kapitel 6.2 der Markenanweisung MTB MA_13_1_06 Informationssicherheit für Systembetrieb und Systemverwaltung ausführlich beschrieben.

7.4 Anforderungen an den Betrieb von IKT-Systemen

Die Anforderungen werden in Kapitel 6.3 der Markenanweisung MTB MA_13_1_06 Informationssicherheit für Systembetrieb und Systemverwaltung ausführlich beschrieben.

7.5 Anforderungen an den Betrieb der Netzwerkinfrastruktur

Die Anforderungen werden in Kapitel 6.4. der Markenanweisung MTB MA_13_1_06 Informationssicherheit für Systembetrieb und Systemverwaltung ausführlich beschrieben.

7.6 Anforderungen an Administratoren bei IT-Dienstleistern

Da die Administratoren des Dienstleisters eine besondere betriebliche Verantwortung für die IKT-Systeme haben, müssen sie folgende Anforderungen gemäß der Markenanweisung MTB 13_1_01 Standard für Informationssicherheit, Artikel 16, erfüllen:

- Sie müssen höhere Schutzanforderungen für die Verwendung und Handhabung von Verwaltungspasswörtern prüfen.
- Administratoren müssen regelmäßig für die spezifischen Risiken in ihrem Arbeitsbereich sensibilisiert werden. Dazu gehören Anweisungen, Schulungen und Übungen.
- Die Passwörter müssen gemäß den dokumentierten Verfahren verwaltet werden.
- Privilegierte Benutzerkennungen dürfen nicht für die alltägliche Arbeit genutzt werden.
- Umfassende Zugriffsrechte müssen in regelmäßigen Abständen überprüft werden. Die Intervalle richten sich nach dem Umfang und der Kritikalität des Zugriffsrechts.
- Identische administrative Passwörter dürfen nicht für verschiedene Anwendungen verwendet werden.
- Server-Panels und Server-Konsolen müssen verschlossen werden, wenn sie nicht benutzt werden.
- Die Sitzungen müssen unmittelbar nach Beendigung der Aufgabe(n) geschlossen werden.

8 Änderungen

Version 3.0

- Änderungsprotokoll hinzugefügt
- Der Name der Anweisung wurde geändert
- Umbenennung
- Änderungen der Rollen und Zuständigkeiten
- Abschnitt 6.3 – Verifizierung und Anforderungen an Lieferanten hinzugefügt
- Abschnitt 6.4 – Berichterstattung hinzugefügt
- Doppelter Abschnitt gelöscht
- Umbenennung der Anweisung – lautete "MAN 13.1 Anweisung 8 – Informationssicherheit bei der Zusammenarbeit mit IT-Service Providern“.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

I. **Anlage 1:** Verfahren und Anforderungen im Rahmen der Lieferantenüberprüfung

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Anlage 1 - Verfahren und Anforderungen im Rahmen der Lieferantenüberprüfung

Ersteller	Steven Rauw erdink Ralf Schlag	**Freigeber**	Andre Wehner	**Version**	1.0
Abt.	FIOS	Abt..	FI	**KSU-Class:**	XX

Gültigkeitsbeginn 01.02.2023	**Geltungsbereich** MAN Truck & Bus SE und deren Tochtergesellschaften	**Genehmigungen (Vorstand)*** **Abgestimmt mit**

* Nur erforderlich, sofern eine Markenanweisung keiner übergeordneten Markenrichtlinie zuzuordnen ist.

Inhalt

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

1 Zweck

Der Zweck dieses Anhangs ist die Definition und Beschreibung der detaillierten Informationssicherheitsanforderungen bei Lieferanten, die im Auftrag von MAN Truck & Bus SE mit Informationen umgehen.

Die Anlage ergänzt die Markenanweisung MTB MA_13_1_08 Informationssicherheit bei Lieferanten.

2 Prüfverfahren und Anforderungen

2.1 Informationen zur Handhabung bei Lieferanten

Ausgangspunkt der Überprüfung ist die korrekte Identifizierung und Klassifizierung der wichtigsten Informationsressourcen im Zusammenhang mit der vom Anbieter zu erbringenden Dienstleistung. Der Verantwortliche des Dienstes klassifiziert die Informationen, die vom Partner bearbeitet werden sollen. Die Bearbeitung umfasst die Übermittlung, Speicherung und Nutzung der Informationen. Die Klassifizierung unterstützt bei der Ermittlung des Schutzbedarfs sowie der Anforderungen, die der Lieferant in Bezug auf die erbrachte Dienstleistung einhalten muss. Zu diesem Zweck wird das ISi-Bewertungsverfahren in Zusammenarbeit mit der Abteilung für Informationssicherheit durchgeführt.

Um die Eignung eines potenziellen Lieferanten festzustellen, müssen möglicherweise weitere Aspekte überprüft werden. Diese könnten rechtlicher Natur sein, wie beispielsweise der Umgang mit personenbezogenen Daten, mit Dienstleistungen rund um Finanzsysteme im Zusammenhang mit der Berichterstattung, mit Informationen, die möglicherweise der Exportkontrolle unterliegen, mit Unternehmen, bei denen Probleme mit Anti-Korruptions- oder Lieferkettenvorschriften entstehen könnten.

2.1.1 Anforderungen an die Zertifizierung

Um Informationssicherheitsrisiken adäquat zu begegnen, benötigen Lieferanten, die im Auftrag der MAN Truck & Bus mit Informationen umgehen, die als vertraulich, streng vertraulich und damit mit hohem oder sehr hohem Schutzbedarf eingestuft sind, eine gültige Informationssicherheitszertifizierung.

- ISO 27001-Zertifikat

  Eine geeignete ISO 27001-Zertifizierung setzt Folgendes voraus:

  - Das Zertifikat muss auf dem neuesten Stand sein.
  - Der Geltungsbereich des zertifizierten Informationssicherheits-managementsystems umfasst den gesamten Bereich, der mit der Informationsverarbeitung bei MAN Truck & Bus befasst ist.

- TISAX-Zertifikat

  Eine TISAX-Zertifizierung setzt Folgendes voraus:

  - Die TISAX-Zertifizierung ist auf dem neuesten Stand.
  - Für jeden Standort, der an der Informationsverarbeitung von MAN Truck & Bus beteiligt ist, liegt eine TISAX-Zertifizierung vor.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

- Die Informationen der Zertifizierung werden mit der VW-ENX-ID "PVPT9Z" in der ENX-Datenbank[1] veröffentlicht.
- Das TISAX-Label ist auf die Klassifizierung der verarbeiteten Informationen abgestimmt:
  - (Info, hoch) für Informationen mit hohem Schutzbedarf (z. B. vertraulich)
  - (Info, sehr hoch) für Informationen mit sehr hohem Schutzbedarf (streng vertrauliche oder besondere personenbezogene Informationen)
  - (Daten) für personenbezogene Informationen

2.1.2 Abweichungen

Wenn ein potenzieller Lieferant keine gültige Zertifizierung nachweisen kann, kann ein Vertrag nur abgeschlossen werden, wenn er sich verpflichtet, sich innerhalb einer bestimmten Frist zertifizieren zu lassen.

- Der Vertrag enthält eine Klausel mit folgendem Wortlaut:
  - TISAX: Der Lieferant verpflichtet sich, für seinen Hauptstandort und jeden anderen Standort, der Informationen im Auftrag von MAN Truck & Bus verarbeitet, eine Zertifizierung nach dem TISAX-Verfahren auf der Bewertungsstufe 2 bis spätestens zum XX.XX.202X durchzuführen.

    Die Zertifizierung muss mindestens die folgenden Module umfassen:
    - Basismodul Informationssicherheit (Info, hoch)
    - Zusatzmodul Datenschutz (Daten)
  - ISO 27001: Der Lieferant verpflichtet sich, bis zum XX.XX.202X eine Zertifizierung nach ISO 27001 durchzuführen. In diesem Fall ist die Leistungserbringung für die MAN Truck & Bus vollständig in den Geltungsbereich des zertifizierten Informationssicherheits-managementsystems des Lieferanten einzubeziehen.
- Der Lieferant legt eine GAP-Analyse vor, die einen Aktionsplan für die Erreichung der Zertifizierungsstufe innerhalb des vorgesehenen Zeitrahmens enthält.
- Die Abteilung für Informationssicherheit von MAN Truck & Bus wird die Analyse überprüfen und den Lieferanten bestätigen.

2.1.3 Lieferantenvertrag

Nach der Klassifizierung der Informationsressourcen und der Validierung der Anforderungen an die Zertifizierung der Informationssicherheit, muss die Zusammenarbeit mit dem Lieferanten auf einem gültigen Vertrag zwischen der MAN Truck & Bus SE und dem Lieferanten basieren. Vor dem Vertragsabschluss muss eine

[1] TISAX-Liste - in Abschnitt 3 wird auf alle Lieferanten verwiesen, die ihre TISAX-Ergebnisse dem VW Konzern mitgeteilt haben (Aktualisierung alle zwei Wochen).

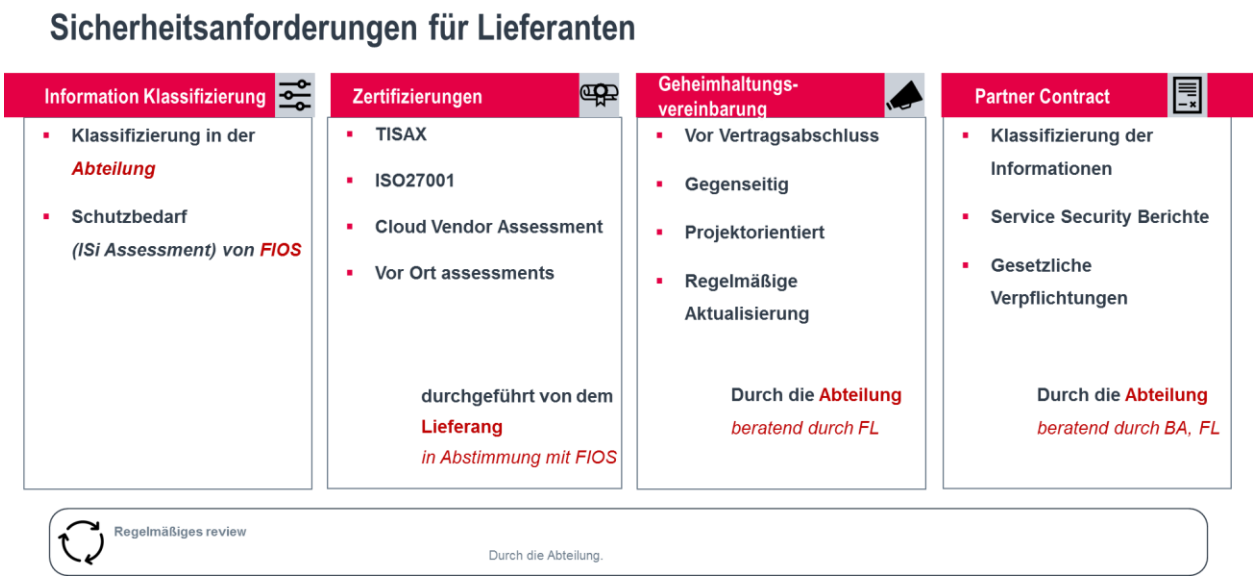
Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Geheimhaltungsvereinbarung unterzeichnet und regelmäßig auf dem neuesten Stand gehalten werden. Der Vertrag enthält Folgendes:

- Klassifizierung der Informationen, die mit dem Lieferanten geteilt wird.
- Der Vertrag muss die Verpflichtung enthalten, dass der Lieferant regelmäßig Berichte über die Informationssicherheit vorlegt.
- Zusätzliche Klauseln und Anhänge müssen rechtliche und regulatorische Anforderungen enthalten, beispielsweise hinsichtlich Datenschutz, Kartellrecht oder Exportkontrolle.

2.1.4 Prüfung

Es müssen regelmäßige Überprüfungen von Änderungen im Zusammenhang mit der Klassifizierung von Informationsressourcen und der Einhaltung der vereinbarten Anforderungen an die Informationssicherheit durch die Lieferanten durchgeführt werden.



2.2 Bewertung von Cloud-Anbietern (CVA)

Cloud-Dienste erfordern eine zusätzliche Überprüfung, um festzustellen, ob die Informationssicherheitsstandards erfüllt sind. Der Grund dafür ist, dass der Dienst in der Regel direkt über das Internet zugänglich ist. Auch der genaue Standort der Informationen und die Personen, die Zugang zu den Informationen haben, sind oft nicht klar definiert.

Mit einer Cloud-Anbieterbewertung wird das Sicherheitsniveau der Anbieter von Cloud-Diensten bewertet. Ziel ist es, die internen Kontrollsysteme von Cloud-Anbietern im Hinblick auf die Informationssicherheit zu bewerten.

Eine solche Bewertung basiert auf einem branchenübergreifenden Kriterienkatalog, der einen fundierten Hinweis auf den Stand der Informationssicherheit speziell bei Cloud-Anbietern gibt. Sie besteht aus Kontrollen in verschiedenen Bereichen (Domänen) der Informationssicherheit.

Ein CVA (z. B. DCSO CVA, CSA STAR und BSI C5) ist obligatorisch für Projekte und Lösungen mit einem hohen oder sehr hohen Schutzbedarf, bei denen Cloud-Dienste von Drittanbietern wie Software as a Service und Platform as a Service genutzt werden.

3 Referenzdokumente

- Beschaffungsbedingungen IT des VW Konzerns (MAN (wgroupsupply.com))
- ISi-Assessment - (MAN Intranet > Corporate > Information Security > ISi Assessment)
- Lieferantenberichte (MAN Intranet > Corporate > Information Security > Supplier Assessments > Supplier Reports)
- VW KRL13 Anhang 1
- TISAX List (TISAX Liste - Konzernsicherheit - Konzern-Wiki (volkswagen-net.de))
- Richtlinie 03.01.017 Cloud-Sicherheit (Richtlinie Cloud-Sicherheit Konzern-Wiki (volkswagen-net.de))
- Richtlinie 03.01.016 Management von Lieferungen durch Dritte (Richtlinie Management von Lieferungen durch Dritte Konzern-Wiki (volkswagen-net.de))

4 Änderungen

Version 1.0

- Erstellung

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Umgang mit personenbezogenen Daten und Organisation des Datenschutzes

Ersteller Heike Bösl Abt.	**Freigeber** Dr. Karl-Heinz Müller Abt.	**Version** **3.0** **KSU-Klasse:** X.X
Gültigkeitsbeginn Datum 01.07.2020	**Geltungsbereich** MAN Gruppe	**Genehmigungen (Vorstand)** Drees Dr. Intra Schenk Cortes **Abgestimmt mit**

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

Inhalt

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Zweck

Der respektvolle Umgang untereinander sowie mit Kunden, Mitarbeitern, Lieferanten und sonstigen Businesspartnern und Beteiligten stellt ein prägendes Element der Unternehmen der MAN Gruppe dar. Im Bereich des Datenschutzes findet dieser Respekt seinen Ausdruck in den Aktivitäten, die darauf abzielen, die Persönlichkeitsrechte natürliche Personen bei der Verarbeitung ihrer personenbezogenen Daten auf einem hohen Niveau zu schützen. Dabei soll zugleich eine angemessene Nutzung personenbezogener Daten ermöglicht und damit die Geschäftstätigkeit der MAN Gruppe im Allgemeinen und deren digitale Transformation im Besonderen unterstützt werden. Nicht zuletzt sollen datenschutzrelevante Rechtsverstöße und daraus ggf. resultierende rechtliche und wirtschaftliche Nachteile bestmöglich vermieden werden.

Zweck dieser Richtlinie ist es, die Erreichung der angestrebten Ziele dadurch sicherzustellen, dass für alle relevanten Unternehmen der MAN Gruppe

- grundsätzliche Regeln und Rahmenbedingungen für den Umgang mit personenbezogenen Daten fest-gelegt werden,
- eine praxistaugliche Organisationsstruktur für den Datenschutz etabliert wird und zudem
- ein angemessenes Daten(schutz)management eingerichtet wird.

Mit dieser Richtlinie werden die Anforderungen der Volkswagen Konzernrichtlinie „Datenschutz im Volks-wagen Konzern“ und der TRATON Konzernrichtlinie 4.2 „Schutz personenbezogener Daten und Organisation des Datenschutzes“ umgesetzt. Diese Richtlinie regelt nicht das Thema Datensicherheit. Letzteres wird durch separate Regelungen erfasst.

2 Geltungsbereich

Der sachliche Geltungsbereich dieser Richtlinie umfasst sämtliche Vorgänge, bei denen personenbezogene Daten von natürlichen Personen ganz oder teilweise automatisiert erhoben, gespeichert, geordnet, verknüpft, übermittelt, genutzt, verändert, ausgelesen, vernichtet oder sonst verarbeitet werden. Dies gilt ins-besondere für personenbezogene Daten von Beschäftigten, Kunden, Lieferanten oder sonstigen Geschäftspartnern. Diese Richtlinie gilt auch für die nicht automatisierte Verarbeitung von personenbezogenen Daten in strukturieren Datensammlungen.

Diese Richtlinie gilt unmittelbar für die MAN SE und ihre Mitarbeiter. Die Inhalte dieser Richtlinie sind dar-über hinaus in allen Unternehmen umzusetzen, an denen die MAN SE direkt oder indirekt zu mehr als 50 % beteiligt ist und in denen Datenverarbeitungsvorgänge der in Absatz 1 genannten Art stattfinden (Konzern-gesellschaften).

In einigen Ländern schützt das nationale Datenschutzrecht Informationen über juristische Personen in gleicher Weise wie Informationen über natürliche Personen. In diesen Fällen hat die Geschäftsleitung des Unternehmens durch eine ergänzende Regelung auf Unternehmensebene festzulegen, inwieweit die Inhalte dieser Richtlinie auch für Informationen über juristische Personen gelten.

Soweit Inhalte dieser Richtlinie in einem Land nicht mit Vorschriften des nationalen oder supranationalen Rechts vereinbar sind, gelten diese Vorschriften des nationalen oder supranationalen Rechts vorrangig. Dies gilt insbesondere, wenn das nationale Recht ein höheres Datenschutzniveau vorsieht als diese Richt-linie.

Der Umsetzung dieser Richtlinie dienende, ergänzende Regelungen sind dem jeweils zuständigen Daten-schutzbeauftragten rechtzeitig vor ihrer Veröffentlichung zur Freigabe vorzulegen. Ausnahmen von den in dieser Richtlinie enthaltenen Regelungen sind nur zulässig, wenn diese zuvor mit MAN SE, Group Data Protection abgestimmt worden sind.

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

3 Begriffe und Definitionen

Die in dieser Richtlinie benannten Rollen und Verantwortlichkeiten werden der Einfachheit halber auch stell-vertretend für die feminine und diverse Form ausschließlich in der maskulinen Form verwendet.

Anonymisierung personenbezogener Daten bedeutet, dass sämtliche Identifikationsmerkmale (z. B. Name, E-Mail-Adresse, Nutzerkennung) soweit gelöscht oder verändert werden, dass die Identität der betroffenen Person nicht mehr bzw. nur mit unverhältnismäßig hohem Aufwand festgestellt werden kann.

Auftragsverarbeiter ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag eines Datenverantwortlichen verarbeitet.

Betroffene Person ist die bestimmte oder bestimmbare natürliche Person, auf die sich personenbezogene Daten beziehen, z. B. Beschäftigte eines Konzernunternehmens oder Kontaktpersonen bei einem Kunden.

Datenempfänger ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, an die personenbezogene Daten übermittelt oder der gegenüber sie in sonstiger Weise offengelegt werden.

Datenschutzbeauftragter ist die Person, die auf Basis dieser Richtlinie oder nationalen Rechts durch die Unternehmensleitung formell als für Datenschutzfragen in diesem Unternehmen benannt worden und fachlich in dieser Funktion nicht weisungsgebunden ist.

Datenschutzmanager ist die von einem Fachbereich, Bereich, Standort, Unternehmen oder einer Unternehmensgruppe formell benannte Person, die dem Datenschutzbeauftragten des Unternehmens und den jeweils übergeordneten Datenschutzmanagern als Ansprechpartner in datenschutzrelevanten Themen dient und die in ihrem jeweiligen Verantwortungsbereich fachlich weisungsgebunden für die operative Um-setzung der datenschutzrechtlichen Vorgaben sorgt. Je nach Zuständigkeitsbereich werden die benannten Personen als Konzern-, Unternehmens-, Ressort-, Fachbereichsdatenschutzmanager oder in vergleichbarer Weise bezeichnet.

Datenverantwortlicher ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen, über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

Dritter ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Datenverantwortlichen und dem Auftragsverarbeiter.

Einschränkung der Verarbeitung ist das Markieren von gespeicherten personenbezogenen Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken. Beispiel: nur aus steuerlichen Gründen gespeicherte Daten werden markiert, damit sie nicht mehr für Marketingzwecke genutzt werden können.

Einwilligung ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Personenbezogene Daten sind Informationen über eine bestimmte oder bestimmbare natürliche Person. Bestimmbar ist die Person, wenn sie direkt oder indirekt über eine oder mehrere Informationen (z. B. Name, Personalnummer, Nutzerkennung oder Anschrift) identifiziert werden kann.

Pseudonymisierung: Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Voraussetzung ist, dass diese

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

zusätzlichen Informationen gesondert aufbewahrt werden und technischen bzw. organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zu-gewiesen werden.

Sensible personenbezogene Daten (besondere Kategorien personenbezogener Daten) sind Daten, aus denen die rassische oder ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung oder Gewerkschaftszugehörigkeit hervorgehen, genetische und biometrische Daten, personenbezogene Daten über die Gesundheit, das Sexualleben oder die genetischen Eigenschaften einer natürlichen Person sowie personenbezogene Daten, die mit Ordnungswidrigkeiten, Straftaten oder strafrechtlichen Verurteilungen zusammenhängen

Übermittlung ist jede Bekanntgabe personenbezogener Daten an eine andere natürliche oder juristische Person, Behörde, Einrichtung oder Stelle. Eine Übermittlung liegt auch vor, wenn eine andere Stelle die Möglichkeit des Zugriffs auf personenbezogene Daten erhält.

Verarbeitung ist jeder manuell oder automatisiert ausgeführte Vorgang im Zusammenhang mit personen-bezogenen Daten, insbesondere das Erheben, Speichern, Ordnen, Verändern, Übermitteln, Auslesen, Offenlegen, Verknüpfen, Einschränken, Löschen oder Vernichten.

Verfahren zur Verarbeitung personenbezogener Daten ist ein Bündel von zusammengehörigen Verarbeitungen, das einem einheitlichen Zweck dient. Beispiele: Entgeltabrechnung, Kundenbeziehungsmanagement, Videoüberwachung.

4 Grundsätze für die Verarbeitung personenbezogener Daten

Bei der Verarbeitung personenbezogener Daten sind nachstehende Grundsätze zwingend zu beachten. Bestehen Zweifel an der Zulässigkeit einer Verarbeitung, ist diese bis auf Weiteres zu unterlassen und der Datenschutzbeauftragte zu kontaktieren.

4.1 Verarbeitung nach Treu und Glauben

Personenbezogene Daten werden fair und unter Einhaltung der Grundsätze von Treu und Glauben verarbeitet.

4.2 Keine Datenverarbeitung ohne Rechtsgrundlage

Personenbezogene Daten dürfen nur verarbeitet werden, wenn für die jeweilige Verarbeitung eine entsprechende Rechtsgrundlage existiert und diese ausreichend dokumentiert ist. Eine Verarbeitung ohne ausreichende Rechtsgrundlage ist unzulässig und darf daher nicht stattfinden.

Für die Verarbeitung personenbezogener Daten durch eine Gesellschaft und ihre Mitarbeiter kommen folgende Rechtsgrundlagen in Betracht:

Vertrag | Personenbezogene Daten, die für den Abschluss, die Durchführung oder die Beendigung eines Vertrages mit der betroffenen Person erforderlich sind, dürfen verarbeitet werden. Dies gilt auch für personenbezogene Daten, die zur von der betroffenen Person erwünschten Anbahnung von Vertragsverhältnissen oder die Erfüllung nachvertraglicher Pflichten erforderlich sind.

Gesetz | Personenbezogene Daten dürfen verarbeitet werden, wenn ein Gesetz oder eine verbindliche gerichtliche oder behördliche Entscheidung dies erforderlich macht.

Interessenabwägung | Personenbezogene Daten dürfen verarbeitet werden, wenn und soweit dies zur Wahrung der berechtigten Interessen des Datenverantwortlichen oder eines Dritten erforderlich ist und dem-gegenüber die Interessen der betroffenen Person am Unterlassen der Verarbeitung nicht überwiegen.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

Einwilligung | Wenn die betroffene Person in die Verarbeitung ihrer Daten freiwillig, konkret, zweifelsfrei und auf der Basis ausreichender Informationen eingewilligt hat, dürfen die von der Einwilligung umfassten personenbezogenen Daten verarbeitet werden. Beruht die Verarbeitung auf einer Einwilligung, muss der Datenverantwortliche jederzeit durch eine geeignete Dokumentation nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

Lebenswichtige Interessen | Die Verarbeitung personenbezogener Daten ist zulässig, wenn diese erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

Öffentliche Interessen | Die Verarbeitung personenbezogener Daten ist zulässig, wenn diese im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Datenverantwortlichen übertragen worden ist.

4.3 Zweckbindung

Personenbezogene Daten dürfen nur erhoben werden, wenn sie zur Erreichung eines konkret festgelegten, legitimen Zwecks erforderlich sind. Der Fachbereich, der die Datenverarbeitung anfordert, hat die Zwecke vor der Verarbeitung zu dokumentieren, sofern diese nicht offensichtlich sind.

Die Verwendung personenbezogener Daten zu einem anderen als dem ursprünglichen Zweck ist zulässig, wenn dieser neue Zweck mit dem ursprünglichen vereinbar ist. Die Änderung des Verwendungszwecks ist zu dokumentieren. Ist der neue Zweck mit dem ursprünglichen nicht vereinbar, ist die Verwendung der personenbezogenen Daten nur zulässig, wenn für die Verwendung der personenbezogenen Daten zu dem neuen Zweck eine eigene Rechtsgrundlage gegeben ist.

4.4 Verhältnismäßigkeit, Datensparsamkeit

Bei der Verarbeitung personenbezogener Daten ist der Grundsatz der Verhältnismäßigkeit zu beachten. Eine Verarbeitung ist nur verhältnismäßig, wenn

- sie dazu geeignet ist, einen legitimen Zweck zu erreichen.
- kein milderes, gleichermaßen geeignetes Mittel zur Erreichung dieses Zweckes zur Verfügung steht. Als milderes Mittel kommt insbesondere die Erhebung von Daten ohne Personenbezug oder eine Verarbeitung von anonymisierten oder pseudonymisierten Daten in Betracht.
- die Zahl der betroffenen Personen und der Umfang der verarbeiteten Daten auf das notwendige Maß reduziert worden sind (Datensparsamkeit).
- der Kreis der Personen, die Zugriff auf personenbezogene Daten erhalten, auf diejenigen begrenzt ist, die diesen Zugriff zur Erfüllung ihrer bestimmungsgemäßen Tätigkeit benötigen (Need-to-know-Prinzip).
- und der Verarbeitung keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen.

4.5 Grundsatz der Direkterhebung

Personenbezogene Daten sind grundsätzlich direkt bei den betroffenen Personen zu erheben. Eine Erhebung bei Dritten ist zulässig, wenn eine Rechtsvorschrift dies vorsieht oder verlangt, dies im Interesse der betroffenen Person ist oder eine Direkterhebung nur mit unverhältnismäßigem Aufwand möglich wäre. Unabhängig davon, ob personenbezogene Daten direkt oder nicht direkt bei der betroffenen Person erhoben werden, ist diese gemäß Ziffer 4.6 zu informieren.

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

4.6 Transparenz und Information der betroffenen Person

Personenbezogene Daten sind in einer für den Datenverantwortlichen und die betroffenen Personen nach-vollziehbaren Art und Weise zu verarbeiten.

Die betroffenen Personen sollen daher von dem Fachbereich, der die Datenverarbeitung anfordert, spätestens zum Zeitpunkt der Datenerhebung über die Verarbeitung ihrer personenbezogenen Daten in einer transparenten, leicht verständlichen Form und unter Berücksichtigung nationaler Anforderungen informiert werden. Die Information soll insbesondere folgende Elemente enthalten:

- die Identität des Datenverantwortlichen,
- die Zwecke der Verarbeitung,
- die Rechtsgrundlage für die Verarbeitung,
- die berechtigten Interessen, falls die Datenverarbeitung auf eine Interessenabwägung gestützt wird,
- die Kategorien der verarbeiteten personenbezogenen Daten,
- die Speicherdauer,
- den Datenempfänger oder die Kategorien von Datenempfängern
- die Quelle, aus der die Daten stammen, sofern sie nicht direkt beim Betroffenen erhoben werden, sowie
- Hinweise darauf, wie den Betroffenen eventuell zustehende Datenschutzrechte ausgeübt werden können.

Die Information kann unterbleiben, wenn sie unter Berücksichtigung der Umstände der Erhebung, des Zwecks der Verarbeitung oder überwiegender Interessen des Datenverantwortlichen nicht geboten erscheint. Dies ist beispielsweise der Fall, wenn die betroffene Person bereits Kenntnis von der Verarbeitung hat oder die Verarbeitung gesetzlich vorgeschrieben ist. Bei der Erhebung personenbezogener Daten ist kenntlich zu machen, welche Angaben freiwillig und welche verpflichtend sind.

4.7 Datenqualität

Personenbezogene Daten sind sachlich richtig zu erheben und zu verarbeiten. Es sind angemessene Maß-nahmen zu treffen, damit unrichtige oder unvollständige Daten rechtzeitig berichtigt, ergänzt oder gelöscht werden.

4.8 Datensicherheit

Der Datenverantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, um personenbezogene Daten vor unbefugter oder unzulässiger Verarbeitung, Zerstörung, Verlust oder Veränderung zu schützen. Die Maßnahmen müssen unter Berücksichtigung des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten und dem sonstigen Aufwand ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. In diesem Zusammenhang sind insbesondere die für das jeweilige Unternehmen auf dem Gebiet der Datensicherheit geltenden Richtlinien und Anweisungen einzuhalten.

4.9 Löschung von Daten

Nicht mehr benötigte personenbezogene Daten sind zu löschen. Das entsprechende Löschkonzept ist grundsätzlich bereits vor der Datenerhebung zu erstellen. Nicht mehr benötigt werden personenbezogene Daten insbesondere, wenn der Zweck, für den sie ursprünglich erhoben worden

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

sind, nicht mehr existiert, die Daten zur Erreichung dieses Zwecks nicht mehr erforderlich sind oder eine Zulässigkeitsvoraussetzung für die Datenverarbeitung nachträglich weggefallen ist. Ist eine Löschung der Daten nur mit unverhältnismäßig hohem Aufwand möglich oder werden die personenbezogenen Daten nur noch zur Erfüllung von Aufbewahrungspflichten oder vergleichbaren Zwecken benötigt, sind sie zu markieren mit dem Ziel, ihre künftige Verarbeitung entsprechend einzuschränken.

Bei der Erstellung des Löschkonzepts und bei der Löschung von Daten sind die Vorschriften für die Aufbewahrungsfristen und die Klassifizierung von Daten der konzernweiten Klassifizierungssystematik für Unter-lagen (KSU) in ihrer jeweils gültigen Fassung zu beachten, sofern nicht zwingende gesetzliche Vorschriften etwas anderes vorschreiben

5 Spezielle Formen der Datenverarbeitung

5.1 Auftragsverarbeitung

Bei einer Auftragsverarbeitung werden personenbezogene Daten von einem Auftragsverarbeiter (Auftrag-nehmer) im Auftrag des Datenverantwortlichen (Auftraggeber) verarbeitet. Verantwortlich für die ordnungs-gemäße Verarbeitung der personenbezogenen Daten bleibt der Auftraggeber.

Unternehmen, die dem Geltungsbereich dieser Richtlinie unterfallen, dürfen eine Auftragsverarbeitung als Auftraggeber nur durchführen, wenn folgende Voraussetzungen erfüllt sind:

- Der Auftraggeber hat mit dem Auftragnehmer einen Auftragsverarbeitungsvertrag abgeschlossen, in dem zumindest folgende Themen geregelt sind: Gegenstand, Dauer, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien der betroffenen Personen, Löschfristen, Schicksal der personenbezogenen Daten nach Beendigung des Auftrags sowie Kontrollrechte und Weisungen des Auftraggebers.
- Der Auftragnehmer hat ausreichende technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten ergriffen. Die diesbezügliche Prüfung obliegt der zuständigen Fachabteilung.
- Der Auftragnehmer schaltet ohne die vorherige allgemeine oder spezielle Genehmigung des Auftrag-gebers keinen weiteren Auftragnehmer (Unterauftragnehmer) zur Erfüllung seiner Aufgaben ein. Der Auftraggeber hat seine Auftragnehmer sorgfältig auszuwählen und mit ihnen Verträge zu schließen, die ebenfalls die vorstehend genannten Mindestinhalte aufweisen. Der Auftraggeber hat sich regelmäßig von der ordnungsgemäßen Durchführung des Auftrags zu überzeugen.

Da der Auftragnehmer kein Dritter im Sinne dieser Richtlinie ist, bedarf der Datentransfer vom Auftraggeber an den Auftragnehmer keiner gesonderten Rechtsgrundlage gemäß Ziffer 4.2.

5.2 Übermittlung von personenbezogenen Daten an Dritte

Die Übermittlung personenbezogener Daten an Dritte ist nur zulässig, wenn sie auf einer gesonderten Rechtsgrundlage gemäß Ziffer 4.2 beruht. Dies gilt auch, wenn der Dritte eine andere Konzerngesellschaft oder eine andere Gesellschaft des Volkswagen Konzerns ist.

Die Verarbeitung der übermittelten Daten durch den Datenempfänger bedarf einer eigenen Rechtsgrundlage, deren Vorhandensein durch den Datenempfänger vor der Verarbeitung sicherzustellen ist.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

5.3 Gemeinsam Datenverantwortliche

Legen zwei oder mehr Datenverantwortliche die Zwecke und Mittel der Verarbeitung gemeinsam fest, sind sie gemeinsam Datenverantwortliche. Gemeinsam Datenverantwortliche haben in einer Vereinbarung transparent festzulegen, wer von ihnen welche datenschutzrechtliche Verpflichtung zu erfüllen hat.

5.4 Übermittlung von personenbezogenen Daten an Drittstaaten

Bei der Übermittlung personenbezogener Daten aus einem Mitgliedstaat der Europäischen Union in ein Land außerhalb des Europäischen Wirtschaftsraums sind die hierfür maßgeblichen besonderen Vorschriften einzuhalten.

6 Konzernweit verbindliche Maßnahmen zum Datenschutz

Die dem Geltungsbereich dieser Richtlinie unterfallenden Konzerngesellschaften ergreifen in ihrem Verantwortungsbereich die nachstehend genannten verbindlichen Maßnahmen, um dadurch vergleichbare Standards im Datenschutz sicherzustellen, Synergien innerhalb der TRATON und MAN Gruppe zu erzielen und ein einheitliches, konzernweites Berichtswesen zu ermöglichen.

6.1 Verzeichnis von Verarbeitungstätigkeiten

Die Konzerngesellschaften werden ein vollständiges und aussagefähiges Verzeichnis ihrer datenschutzrelevanten Verarbeitungstätigkeiten erstellen und fortlaufend aktualisieren. Hierzu erlassene verbindliche Vor-gaben der MAN Gruppe werden eingehalten, es sei denn, diese verstoßen gegen zwingende Rechtsvorschriften des betreffenden Landes.

6.2 Meldeprozess für Datenschutzverletzungen

Die Konzerngesellschaften werden in ihrem Zuständigkeitsbereich Meldeprozesse implementieren, die sicherstellen, dass Datenschutzverletzungen in ihrem Verantwortungsbereich schnellstmöglich erkannt und ihre negativen Auswirkungen durch geeignete Maßnahmen so weit wie möglich begrenzt werden. Eventuell erforderliche Meldungen an Aufsichtsbehörden haben fristgerecht zu erfolgen.

6.3 Risikomanagement, Monitoring

Die Konzerngesellschaften werden ein angemessenes Datenschutzrisikomanagement installieren und da-bei auch die entsprechenden zentralen Vorgaben beachten.

Zum Zwecke eines strukturierten und systematischen Monitoring werden die Konzerngesellschaften insbesondere entsprechende Kontrollen in ihrem internen Kontrollsystem verankern bzw. entsprechende zentral vorgegebene Kontrollen wirksam implementieren und durchführen. In Absprache mit dem Markensprecher Datenschutz kann ein geeignetes Monitoring auch in anderer Weise sichergestellt werden.

6.4 Lösch- und Zugriffsberechtigungskonzepte

Die Konzerngesellschaften werden in ihrem jeweiligen Verantwortungsbereich Lösch- und Zugriffsberechtigungskonzepte erstellen und implementieren, um sicherzustellen, dass personenbezogene Daten daten-schutzkonform verarbeitet und gelöscht werden.

Bei der Erstellung des Löschkonzepts und bei der Löschung von Daten sind die Vorschriften für die Aufbewahrungsfristen und die Klassifizierung von Daten der konzernweiten KSU in ihrer jeweils gültigen Fassung zu beachten, sofern nicht zwingende gesetzliche Vorschriften etwas anderes vorschreiben.

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

6.5 Etablierung eines Datenschutzberichtswesens

Die Konzerngesellschaften werden in ihrem Zuständigkeitsbereich Datensammlungen und Prozesse etablieren, die ein angemessenes Datenschutzberichtswesen innerhalb des MAN, TRATON und Volkswagen Konzerns ermöglichen.

7 Rollen und Verantwortlichkeiten

7.1 Leitungsorgane

Rechtlich verantwortlich für die Einhaltung der datenschutzrelevanten gesetzlichen und betrieblichen Rege-lungen ist das Leitungsorgan der jeweiligen Gesellschaft. Das Leitungsorgan unterstützt die Fachbereiche und die Mitglieder der Datenschutzorganisation bei der Erfüllung ihrer Aufgaben insbesondere durch die Zurverfügungstellung ausreichender personeller und sachlicher Ressourcen.

Die Leitungsorgane benennen dem für sie zuständigen Markensprecher Datenschutz (vgl. Ziffer 8.3.1) das Mitglied dieses Leitungsorgans, das für die Einhaltung der zum Schutz personenbezogener Daten erlassenen gesetzlichen und betrieblichen Regelungen fachlich und organisatorisch verantwortlich ist.

Berichten mehrere Datenschutzfunktionen an dasselbe Mitglied des Leitungsorgans, so kann dieses einen Berichtspflichtigen mit der Koordinierung der Berichte beauftragen.

7.2 Beschäftigte

Jeder Beschäftigte hat die individuelle Pflicht, seine Tätigkeit im Einklang auch mit den datenschutzrelevanten Vorschriften auszuüben. Führungskräften obliegt darüber hinaus insoweit eine Vorbildfunktion.

7.3 Fachbereiche

Es ist Aufgabe der Fachbereiche, in ihrem Verantwortungsbereich für die Einhaltung der gesetzlichen und betrieblichen Regelungen zum Datenschutz zu sorgen und die insoweit erforderlichen Maßnahmen zu treffen. Zu diesen Maßnahmen gehören insbesondere die ordnungsgemäße Dokumentation der für ihren Bereich maßgeblichen inhaltlichen und organisatorischen Datenschutzaktivitäten.

Über Sachverhalte aus seinem Fachbereich, die auch den Aufgabenbereich des Datenschutzbeauftragten (vgl. 8.3.3) oder den des Unternehmensdatenschutzmanagers (vgl. 8.4.2) betreffen, informiert der Leiter des Fachbereichs diese unaufgefordert, rechtzeitig und in geeigneter Form. Den Leiter des Fachbereichs trifft insoweit eine Bringschuld. Er wird zudem Maßnahmen ergreifen und Prozesse etablieren, um die Um-setzung der Datenschutzprinzipien „Privacy by Design“ und „Privacy by Default“ in seinem Zuständigkeits-bereich sicherzustellen.

Zur Unterstützung bei der Erfüllung seiner datenschutzrelevanten Aufgaben bestellt der Leiter des Fachbereichs erforderlichenfalls einen Fachbereichsdatenschutzmanager (vgl. 8.4.3).

7.4 Datenschutzorganisation

Die MAN Datenschutzorganisation wirkt darauf hin, dass der Datenschutz in den Gesellschaften der MAN Gruppe gesetzeskonform, praxisnah und die MAN Geschäftstätigkeit unterstützend realisiert wird. Sie ist dabei sowohl beratend und überprüfend als auch in der operativen Umsetzung der datenschutzrechtlichen Vorgaben tätig. Die Gestaltung und Umsetzung des Datenschutzes soll dabei möglichst effizient und effektiv erfolgen. Einzelheiten hierzu vgl. unten Ziffer 8.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

7.5 Informationssicherheitsorganisation

Datenschutz- und Informationssicherheitsaufgaben überlappen sich im Bereich des technischen und organisatorischen Schutzes personenbezogener Daten. Die Informationssicherheit unterstützt die Datenschutz-aktivitäten des Unternehmens insbesondere durch die Definition, Bereitstellung und Prüfung der erforderlichen technischen und organisatorischen Maßnahmen. Darüber hinaus informieren sich die Daten-schutz- und Informationssicherheitsorganisationen regelmäßig gegenseitig über Vorgänge, die für den je-weils anderen Bereich von Bedeutung sein können.

7.6 Interne Revision

Die interne Revision unterstützt im Rahmen ihrer allgemeinen Aufgaben die Datenschutzaktivitäten der Unternehmen, indem sie bei der Planung ihres jährlichen Prüfungsprogramms auch geeignete Prüfvorschläge des Datenschutzes berücksichtigt.

7.7 Rechtsabteilung

Datenschutz und Rechtsabteilung informieren sich regelmäßig gegenseitig über Vorgänge aus dem eigenen Verantwortungsbereich, die auch für den jeweils anderen Bereich von Bedeutung sein können.

7.8 Arbeitnehmervertretungen

Die Aufgaben der Arbeitnehmervertretungen und die des Datenschutzes überlappen sich im Bereich der Wahrung der datenschutzrelevanten Persönlichkeitsrechte der Beschäftigten. Arbeitnehmervertretungen und Datenschutz arbeiten insoweit vertrauensvoll zusammen. Die Rechte der Arbeitnehmervertretungen bleiben durch diese Richtlinie unberührt.

8 Datenschutzorganisation

8.1 Aufgabe der Datenschutzorganisation

Die MAN Datenschutzorganisation wirkt darauf hin, dass der Datenschutz in den Gesellschaften der MAN Gruppe gesetzeskonform, praxisnah und die MAN Geschäftstätigkeit unterstützend realisiert wird. Die Gestaltung und Umsetzung des Datenschutzes soll möglichst effizient und effektiv erfolgen.

Personen, die entsprechende Rollen innerhalb der Datenschutzorganisation wahrnehmen, müssen hierzu hinreichend fachlich qualifiziert sein und die Möglichkeit eingeräumt bekommen, ihre jeweilige Rolle effektiv und entsprechend der Maßgaben dieser Konzernrichtlinie zu erfüllen.

8.2 Einheit aus weisungsfreien und weisungsgebundenen Teilen

Die Datenschutzorganisation der MAN Gruppe besteht grundsätzlich aus zwei organisatorisch getrennten Bereichen mit verschiedenen Aufgaben, die in ihrer Gesamtheit die ordnungsgemäße Erfüllung der das Unternehmen treffenden datenschutzrechtlichen Anforderungen sicherstellen sollen. Den einen Teilbereich stellt die weisungsfreie Datenschutzorganisation dar. Sie besteht aus den in 8.3 dargestellten Funktionen. Den anderen Teil bildet die weisungsgebundene Datenschutzorganisation. Sie besteht aus den in 8.4 dar-gestellten Funktionen.

Die Aufteilung der das Unternehmen treffenden datenschutzrelevanten Aufgaben auf zwei organisatorisch getrennte Bereiche ist zum einen erforderlich, um der Aufgabenbeschreibung für Datenschutzbeauftragte in der EU Datenschutz-Grundverordnung (DS-GVO) und vergleichbaren Gesetzen gerecht zu werden. Zum anderen dient sie der Vermeidung von Interessenskonflikten

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

zwischen beratenden und prüfenden Funktionen einerseits und den operativen umsetzenden Funktionen andererseits.

8.3 Weisungsfreie Datenschutzorganisation

8.3.1 Markengruppensprecher Datenschutz

Der Markengruppensprecher Datenschutz koordiniert die Datenschutzaktivitäten der unter TRA-TON zusammengefassten Marken in Angelegenheiten, die markenübergreifend oder von grundsätzlicher Bedeutung sind. Seine Ansprechpartner sind dabei insbesondere die Geschäftsleitung der TRATON SE, die jeweiligen Markensprecher Datenschutz, die Markendatenschutzmanager so-wie Group Legal und der Konzerndatenschutzbeauftragte bei Volkswagen AG.

Der Markengruppensprecher Datenschutz wird vom Vorstand der TRATON SE bestellt. Die Bestellung erfolgt schriftlich durch arbeitsvertragliche oder innerbetriebliche Regelung. Der Markengruppensprecher Datenschutz muss nicht Mitarbeiter der TRATON SE, jedoch Mitarbeiter eines Unternehmens der TRATON Gruppe sein.

8.3.2 Markensprecher Datenschutz

Der Markensprecher Datenschutz koordiniert die Datenschutzaktivitäten der Datenschutzbeauftragten der unter einer Marke zusammengefassten Unternehmen in Angelegenheiten, die unternehmensübergreifend oder für die Marke von grundsätzlicher Bedeutung sind. Seine Ansprechpartner sind dabei insbesondere die Geschäftsleitung der Führungsgesellschaft der jeweiligen Marke, die Datenschutzbeauftragten der Unternehmen oder vergleichbare Funktionen, die in der jeweiligen Marke zusammengefasst sind, der Markendatenschutzmanager sowie der Markengruppensprecher Datenschutz. Der Markensprecher Datenschutz berichtet in dieser Eigenschaft direkt an das Leitungsorgan der Führungsgesellschaft der Marke.

Der Markensprecher Datenschutz wird von der Führungsgesellschaft der Marke bestimmt. Die Bestimmung erfolgt schriftlich durch arbeitsvertragliche oder innerbetriebliche Regelung. Der Markensprecher Datenschutz muss nicht Mitarbeiter des Unternehmens selbst, jedoch Mitarbeiter eines Unternehmens der TRATON Gruppe sein. Die Vertretung mehrerer Marken durch denselben Markensprecher Daten-schutz ist zulässig. Soweit die Führungsgesellschaft einer Marke keinen Markensprecher Daten-schutz bestimmt hat, nimmt diese Funktion der Markengruppensprecher Datenschutz wahr.

8.3.3 Datenschutzbeauftragte

Die Geschäftsleitung jedes Unternehmens der MAN Gruppe ist verpflichtet, eine Person mit deren Einverständnis schriftlich zum Datenschutzbeauftragten oder in eine vergleichbare Funktion zu bestellen. Diese Pflicht entfällt nur, wenn und soweit das Unternehmen im Mittel des vergangenen Kalenderjahres weniger als 20 Mitarbeiter beschäftigt oder der Markensprecher Datenschutz eine schriftliche Befreiung erteilt hat.

Um Interessenkonflikte zu vermeiden, soll der Datenschutzbeauftragte grundsätzlich nicht Mitglied der Geschäftsleitung oder Leiter des lokalen IT- oder HR-Bereiches sein. Abweichungen von diesem Grundsatz sind nur mit Zustimmung des Markensprechers Datenschutz zulässig. Der Daten-schutzbeauftragte muss nicht Mitarbeiter des bestellenden Unternehmens, aber Mitarbeiter eines Unternehmens der TRATON Gruppe sein.

Sofern das Unternehmen nach lokalem Datenschutzrecht einen Datenschutzverantwortlichen bestellen muss oder bereits bestellt hat, übt dieser gleichzeitig die Funktion des Datenschutzbeauftragten aus. Dabei ist es unerheblich, ob der Datenschutzverantwortliche nach

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

lokalem Recht als Datenschutzverantwortlicher, Datenschutzbeauftragter, Data Protection Officer oder mit vergleich-baren Begriffen bezeichnet wird und ob die Rechte und Pflichten des Datenschutzverantwortlichen nach lokalem Recht abweichend von denen dieser Richtlinie geregelt sind.

Die Datenschutzbeauftragten erfüllen die ihnen durch Gesetz oder diese Richtlinie oder übertragenen Aufgaben. In ihrer Eigenschaft als Datenschutzbeauftragte berichten sie direkt an das Leitungs-organ ihres Unternehmens. Ausnahmen sind mit dem Markensprecher Datenschutz abzustimmen.

Zu den Aufgaben der Datenschutzbeauftragten zählen insbesondere

- die Unterrichtung und Beratung von Management und Mitarbeitern in Datenschutzfragen,
- die Überwachung der Einhaltung der gesetzlichen und unternehmensinternen Datenschutz-vorschriften,
- die Unterstützung bei der Erfüllung eventueller Meldepflichten nach lokalem Datenschutzrecht,
- die eigene fachspezifische Fortbildung im Datenschutz,
- die Vorgabe von Leitlinien für die operative Umsetzung des Datenschutzes im Unternehmen,
- die Zurverfügungstellung geeigneter Muster für Datenschutzverträge, Datenschutzklauseln, Datenschutzerklärungen, Datenschutzhinweise und andere Dokumente,
- die Berichterstattung über die Datenschutzaktivitäten des Unternehmens an die Geschäfts-leitung und den Markensprecher Datenschutz sowie
- als fachlicher Ansprechpartner für die Datenschutzbehörden zu fungieren.

Die Aufgaben des Datenschutzbeauftragten und seines Hilfspersonals in den Konzerngesellschaften umfassen keine fachliche Verantwortung für die operative Umsetzung der gesetzlichen, regulatorischen und betrieblichen datenschutzrechtlichen Anforderungen oder die Freigabe von Datenschutzanliegen oder konkreten Verarbeitungsprozessen.

Die Datenschutzbeauftragten sind verpflichtet, alle Angelegenheiten, die ihnen in ihrer Funktion als Datenschutzbeauftragter bekannt werden, vertraulich zu behandeln und insoweit Verschwiegenheit zu wahren.

8.4 Weisungsgebundene Datenschutzorganisation

8.4.1 Markendatenschutzmanager

Der Markendatenschutzmanager koordiniert die Datenschutzaktivitäten der Datenschutzmanager der unter einer Marke zusammengefassten Unternehmen in Angelegenheiten, die unternehmens-übergreifend oder für die Marke von grundsätzlicher Bedeutung sind. Seine Ansprechpartner sind dabei insbesondere die Geschäftsleitung der Führungsgesellschaft der jeweiligen Marke, die Datenschutzmanager der Unternehmen, die in der jeweiligen Marke zusammengefasst sind, der Markensprecher Datenschutz sowie der Markengruppensprecher Datenschutz. Der Markendatenschutzmanager berichtet in dieser Eigenschaft direkt an das Leitungsorgan der Führungsgesellschaft der Marke.

Der Markendatenschutzmanager wird von der Führungsgesellschaft der Marke bestimmt. Die Bestimmung erfolgt schriftlich durch arbeitsvertragliche oder innerbetriebliche Regelung. Der

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

Markendatenschutzmanager muss nicht Mitarbeiter des Unternehmens selbst, jedoch Mitarbeiter eines Unternehmens der TRATON Gruppe sein.

8.4.2 Unternehmensdatenschutzmanager

Die Geschäftsleitung jedes Unternehmens der MAN Gruppe ist verpflichtet, eine unternehmensangehörige Person mit deren Einverständnis schriftlich zum Unternehmensdatenschutzmanager zu bestellen. Diese Pflicht entfällt nur, wenn und soweit das Unternehmen im Mittel des vergangenen Kalenderjahres weniger als 20 Mitarbeiter beschäftigt oder der Markensprecher Datenschutz eine schriftliche Befreiung erteilt hat.

Zentrale Aufgabe des Unternehmensdatenschutzmanagers und der ihm in dieser Funktion direkt oder indirekt fachlich zugeordneten Mitarbeiter ist die operative Umsetzung des Datenschutzes im Unternehmen. Er koordiniert und unterstützt die Leiter der Fachbereiche bei der Erfüllung ihrer Datenschutzaufgaben. Er ist erster Ansprechpartner für alle datenschutzrelevanten Fragen und Angelegenheiten im Unternehmen, sofern diese Aufgabe nicht von den ihm fachlich zugeordneten Fachbereichsdatenschutzmanagern wahrgenommen wird.

Solange das Unternehmen keinen Unternehmensdatenschutzmanager bestellt hat, obwohl dies gemäß Absatz 1 erforderlich ist, wird diese Funktion von dem für Datenschutz zuständigen Mitglied des Leitungsorgans der Gesellschaft wahrgenommen.

8.4.3 Fachbereichsdatenschutzmanager

Erforderlichenfalls bestellen die Leiter von Fachbereichen zur fachbereichsinternen Unterstützung der sie nach dem Gesetz und dieser Richtlinie treffenden datenschutzrechtlichen Aufgaben schriftlich einen oder mehrere Fachbereichsdatenschutzmanager. Zentrale Aufgabe der Fachbereichs-manager ist es, die operative Umsetzung des Datenschutzes im jeweiligen Fachbereich sicherzustellen. In ihrer Eigenschaft als Fachbereichsdatenschutzmanager sind diese dem Unternehmensdatenschutzmanager fachlich zugeordnet.

Absatz 1 gilt analog für andere organisatorische Einheiten innerhalb des Unternehmens wie z.B. Standorte, Ressorts, Abteilungen.

8.4.4 Übersicht

Wie in Ziffern 8.3 und 8.4.1-8.4.3 beschrieben, sind die mit Datenschutzaufgaben beauftragten Mitarbeiter grundsätzlich auf folgenden Ebenen tätig:

Ebene	Beispiele	weisungsfreier Datenschutz	weisungsgebundener Datenschutz
Markengruppe	TRATON	Markengruppensprecher Daten-schutz	./.
Marke	MAN	Markensprecher Datenschutz	Markendatenschutzmanager
Gesellschaft	MAN Truck & Bus SE	Datenschutzbeauftragter	Unternehmensdatenschutzmanager
Abteilung, Bereich	IT, HR, Vertrieb	./.	Fachbereichsdatenschutzmanager

Abweichungen von dieser Nomenklatur sind nur in Abstimmung mit dem Markengruppensprecher Datenschutz zulässig.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

9 Rechte der betroffenen Personen

Die Rechte der betroffenen Personen auf Auskunft, Löschung, Berichtigung, Einschränkung der Verarbeitung, Widerspruch und Widerruf von Einwilligungserklärungen bestimmen sich nach dem für das jeweilige Unternehmen maßgeblichen Datenschutzrecht, nach den insoweit auf Markenebene abgestimmten Vorgehensweisen sowie nach den in Bezug auf diese Rechte maßgeblichen innerbetrieblichen Regelungen.

10 Meldung von Datenschutzverletzungen

10.1 Datenschutzverletzung

Eine Datenschutzverletzung liegt vor, wenn die Sicherheit der personenbezogenen Daten verletzt worden ist und dies zur Vernichtung, Veränderung, unbefugten Offenlegung oder zum Verlust oder unbefugtem Zugang zu personenbezogenen Daten geführt hat. Datenschutzverletzungen sind schnellstmöglich zu identifizieren und zu beenden.

10.2 Einbeziehung des Datenschutzbeauftragten

Der Datenschutzbeauftragte ist unverzüglich zu unterrichten, wenn

a) personenbezogene Daten Unbefugten zur Kenntnis gelangt sind, in sonstiger Weise rechtswidrig oder nicht richtlinienkonform verarbeitet worden sind oder konkrete Anhaltspunkte einen entsprechenden Verdacht begründen und hierdurch erhebliche Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen einer nicht nur geringen Zahl von betroffenen Personen drohen,

b) aufgrund der Verletzung von Vorschriften zum Schutz personenbezogener Daten eine gesetzliche Meldepflicht gegenüber einer Behörde besteht oder

c) von Gerichten oder Behörden auf Grund von datenschutzrechtlichen Verstößen Sanktionen gegen das Unternehmen verhängt werden sollen oder bereits verhängt worden sind.

10.3 Einbeziehung des Marken(gruppen)sprechers Datenschutz

Der zuständige Markensprecher und der Markengruppensprecher werden in die Unterrichtung einbezogen, sofern der Datenschutzverstoß bzw. dessen Sanktionierung für mehr als eine Markengesellschaft von Relevanz ist oder grundsätzliche Bedeutung hat.

10.4 Einbeziehung von Group Legal und Group Data Protection bei VW AG

Bei Datenschutzverstößen oder Anfragen von Aufsichtsbehörden, die für mehr als eine Marke relevant oder von grundsätzlicher Bedeutung sind, bezieht der Markengruppensprecher bzw. der zuständige Markensprecher Group Legal bei VW bzw. den Konzerndatenschutzbeauftragten von VW unverzüglich mit ein.

10.5 Meldung von Datenschutzverletzungen an Aufsichtsbehörden

Meldepflichtige Datenschutzverletzungen sind den Behörden form- und fristgerecht zu melden. Die Meldung von Datenschutzverletzungen an Aufsichtsbehörden erfolgt nach den für die betroffenen Gesellschaften geltenden gesetzlichen Bestimmungen. Gesetzlich oder behördlich vorgegebene Formen und Fristen der Meldung sind einzuhalten.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

11 Ausnahmen

Ausnahmen zu den in dieser Richtlinie enthaltenen Regelungen sind nur zulässig, wenn sie zuvor in Textform vom Markensprecher Datenschutz genehmigt worden sind.

Hinweis: Gedruckte Versionen und lokale Dateien unterliegen nicht dem Änderungsdienst!

1 Der einfacheren Lesbarkeit dienend wird im Folgenden auf die Ausformulierung Mitarbeiterinnen und Mitarbeiter verzichtet und der Begriff „Mitarbeiter“ synonym verwendet.

VOLKSWAGEN

AKTIENGESELLSCHAFT

Informationssicherheit

Handlungsleitlinien
– Handlungsleitlinie für Systembetreiber und Administratoren –

Herausgeber

Group Information Security

Regelung Nr.

02.03

Status

Veröffentlicht

Version

4.1

Klassifizierung

Intern

Datum

03.11.2022

Geltungsbereich

Diese Leitlinie gilt für die Volkswagen AG (Organisationseinheiten (OE) auf Konzernebene und auf Markenebene der Marke Volkswagen Pkw, der Marke Volkswagen Nutzfahrzeuge und der Marke Volkswagen Group Components). Alle Systembetreiber und Administratoren müssen diese Leitlinie erfüllen und einhalten.

Bezüglich der Umsetzung der Regelung in anderen Volkswagen-Konzerngesellschaften gilt ORL 1 „Organisatorische Regelungen der Volkswagen AG“.

©Volkswagen AG, Intern, KSU: 2.1

Inhalt

INTERNAL

INTERNAL

I Zweck

In dieser Informationssicherheits-Handlungsleitlinie werden die Regeln für die Informationssicherheit definiert, die von Systembetreibern und Administratoren beim Umgang mit Informationen und IT-Geräten (z. B. PCs, Laptops oder andere mobile Endgeräte) zu befolgen sind. Für den Schutz von speicherprogrammierbaren Steuerungen (SPS) und Robotersteuerungen gelten die speziellen Vorschriften aus dem Anhang (siehe Anhang B).

Darüber hinaus gilt für die Zielgruppe der Systembetreiber und Administratoren die Informationssicherheits-Handlungsleitlinie für Beschäftigte bzw. für Dritte, sofern der Systembetreiber oder Administrator Beschäftigter einer Partnerfirma ist.

Zweck dieser Informationssicherheits-Handlungsleitlinie ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Schutz der Rechte und Interessen der Gesellschaft und aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit einer Konzerngesellschaft eingehen und/oder Tätigkeiten für diese ausführen.

Die Inhalte dieses Dokuments basieren auf der internationalen Norm ISO/IEC 27002:2013.

Dieses Dokument und alle zugehörigen Änderungs- und Aktualisierungsmitteilungen werden über die üblichen Verteilwege kommuniziert (siehe Anhang 0).

INTERNAL

1 Kontext

Die folgende Übersicht zeigt die Einordnung der Informationssicherheits-Handlungsleitlinien in das Regelwerk der Informationssicherheit:

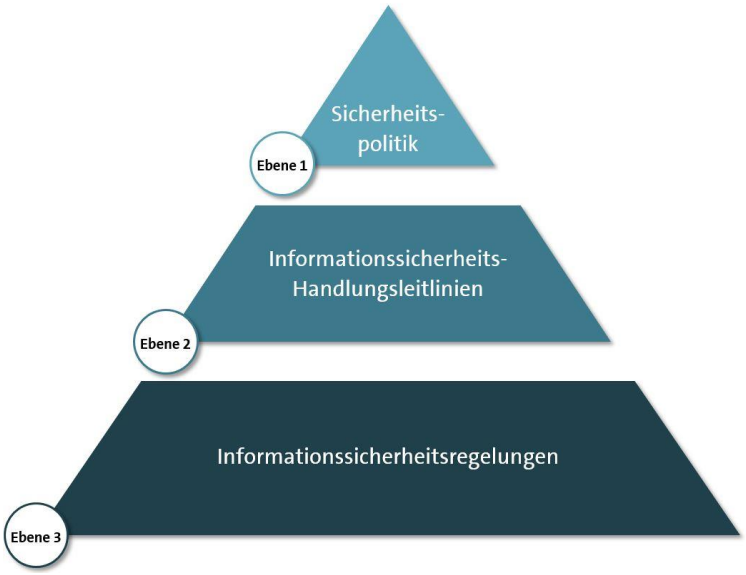


Abbildung 1: Informationssicherheitsregelwerk

Ebene 1 Informationssicherheitspolitik:
Definiert die grundlegenden Ziele, Strategien und Verantwortlichkeiten zur Gewährleistung eines Mindestniveaus der Informationssicherheit und ist in der KRL 18 und den abgeleiteten Markenausprägungen (siehe Anhang B.2.3) dokumentiert.

Ebene 2 Informationssicherheitshandlungsleitlinien:
Ausgestaltung der Informationssicherheitspolitik in organisatorische Anweisungen für einzelne Benutzergruppen

Ebene 3 Informationssicherheitsregelungen:
Spezifikation von regulativen Anforderungen im technischen Umfeld und Beschreibung von technischen Funktionen und Prozessen der Informationssicherheit

2 Asset-Management

Alle unternehmenseigenen IT-Systeme (siehe Anhang B.2.5) sind in einem Register zu erfassen. Die betriebliche Verantwortung für ein IT-System ist einer Person oder Organisationseinheit zu übertragen, die das System aktiv verwaltet.

Die Verantwortung für Informationen hat der jeweilige Informationseigentümer. Dies gilt auch für über IT-Systeme bereitgestellte Informationen. Zuständigkeiten dürfen delegiert werden.

Dieses Register der IT-Systeme muss mindestens folgende Informationen umfassen:

- Beschreibung der IT-Systeme, einschließlich Schnittstellen zu anderen IT-Systemen

INTERNAL

- die verantwortliche Organisationseinheit bzw. Person
- die Geschäftsprozesse, denen die IT-Systeme zugeordnet sind
- der Hosting Standort (z. B. Rechenzentrum)
- Geschäftsprozess-Zugehörigkeit
- Klassifizierung von Daten sowie, falls erforderlich, Hinweise zu spezifischen Schutzanforderungen und Schutzmaßnahmen
- Existenz personenbezogener Daten
- Informationseigentümer

3 Physische Sicherheit und Umgebungssicherheit

- Geschäftskritische IT-Systeme müssen gegen Stromausfälle geschützt werden (z. B. mithilfe einer unterbrechungsfreien Stromversorgung).
- Der Systembetreiber sorgt im Rahmen seiner Kompetenzen u. a. für die Verfügbarkeit von Daten, indem sichergestellt wird, dass sämtliches Equipment zu jeder Zeit ordnungsgemäß gewartet ist. Dazu zählt u. a. die Wartung von IT-Geräten entsprechend den Herstellervorgaben
- Betrieb von IT-Geräten entsprechend den Spezifikationen der Hersteller (z. B. Temperatur, Luftfeuchtigkeit)
- Schutz von IT-Geräten vor unbefugtem Zugriff, Manipulation, Beschädigung oder schädlichen Umgebungsbedingungen (z. B. Feuer, Wasser, Schmutzbelastung)

4 Kommunikations- und Betriebsmanagement

4.1 Betriebliche Verfahren und Zuständigkeiten

4.1.1 Dokumentierte Betriebsverfahren

Der Systembetreiber ist dafür verantwortlich, dass alle für den Betrieb von IT-Systemen erforderlichen Dokumentationen (z. B. betriebliche Service-Handbücher), verfügbar und auf dem aktuellen Stand sind. Für Veröffentlichungen ist zu beachten, dass Unberechtigte keine Kenntnis von vertraulichen oder geheimen Daten, einschließlich sicherheitsrelevanter Informationen (z. B. Firewall-Konfigurationseinstellungen), erhalten.

Dokumentationen sind entsprechend den unternehmensspezifischen Regelungen zu archivieren (siehe Anhang, 06). Der Systembetreiber ist verpflichtet, die festgelegten betrieblichen Verfahren zu befolgen (z. B. zum Change Prozess).

4.1.2 Change Management

Änderungen an laufenden IT-Systemen sind vor ihrer Implementierung in diesen IT-Systemen im Rahmen eines festgelegten Prozesses zu planen, zu testen, freizugeben und zu dokumentieren. Die Vorgaben aus der Regelung (siehe Anhang A.1.5) sind zu befolgen.

INTERNAL

4.1.3 Aufgabentrennung

Der Einsatz unterschiedlicher Beschäftigter für ausführende (z. B. Programmierung, Entwicklung) und kontrollierende (z. B. Audit, Akzeptanz) Tätigkeiten ist organisatorisch festzulegen.

Darüber hinaus sind Aufgaben aufzuteilen, da andernfalls ein erhöhtes Risiko für absichtlichen oder versehentlichen Missbrauch auf Kosten des Konzerns besteht (Vier-Augen-Prinzip).

Es ist das Prinzip der Aufgabentrennung gemäß der Regelung (Siehe Anhang A.1.2) zu beachten.

4.1.4 Trennung von Entwicklungs-, Test- und Produktivumgebungen

Entwicklungsumgebungen, Testumgebungen und Produktivumgebungen (laufende IT-Systeme) sind logisch bzw. physisch voneinander zu trennen. Eine Ausnahme sind große Produktionsanlagen, bei denen dies nicht ohne vertretbaren Aufwand möglich wäre.

Sofern möglich, sind Tests mit generierten Testdaten auszuführen (z. B. mithilfe eines Testdatengenerators).

IT-Systeme dürfen nur in Testumgebungen getestet werden, die speziell hierfür vorgesehen sind. Es ist sicherzustellen, dass der Betrieb von produktiven IT-Systemen nicht beeinträchtigt wird.

Wenn zu Testzwecken Einzelpersonen Zugriff auf personenbezogene, vertrauliche oder geheime Daten erhalten würden, die sie nicht zur Ausführung ihrer vertraglichen Tätigkeiten benötigen, müssen die Daten vor Durchführung der Tests so unkenntlich gemacht werden, dass die Originaldaten nicht identifizierbar sind, bevor sie vom produktiven IT-System in die Test- oder Entwicklungsumgebung übertragen werden. Die Kopie bzw. Verwendung von Informationen aus produktiven IT-Systemen ist nur nach vorheriger Genehmigung durch den Informationseigentümer gestattet. Kopierte Daten unterliegen den gleichen Vorgaben zur Informationssicherheit wie die ursprünglichen Daten.

Wenn ausschließlich personenbezogene Daten der Tester aus den Datenschutzkategorien IT-Nutzungsdaten und/oder berufliche Kontakt- und Identifikationsdaten im Entwicklungs- oder Testsystem enthalten sind, ist dies grundsätzlich zulässig. Sämtliche Anforderungen der DSGVO sind in diesem Zusammenhang einzuhalten. Bei Fragen ist die zuständige DSMO (siehe Anhang B.2.18) des Fachbereichs zu kontaktieren.

Nach der Durchführung von Tests sind dafür verwendete Informationen aus produktiven IT-Systemen wieder vollständig zu löschen.

Die in einem produktiven IT-System geltenden Zugriffsrechte und Rollen sind auch in den Test- und Entwicklungssystemen zu implementieren und den vorgesehenen testenden Personen zuzuweisen, wenn Kopien der produktiven Daten genutzt werden.

4.2 Serviceerbringung durch Dritte

Sicherheitsrelevante Tätigkeiten (wie z. B. die Verwaltung kryptographischer Schlüssel, der Sicherheitsinfrastruktur oder von Sicherheitssystemen) dürfen erst durch Dritte ausgeführt werden, nachdem die zuständige Stelle dies genehmigt hat (siehe Anhang B.2.7). Dabei sind die Vorgaben aus Regelung (siehe Anhang A.1.6) zu befolgen.

4.3 Systemplanung und Abnahme

Die Kapazitätsanforderungen an ein IT-System sind während der Planungsphase zu spezifizieren.

Die Sicherheitsanforderungen an ein IT-System sind ebenfalls in der Planungsphase in Zusammenarbeit mit den Informationseigentümern zu spezifizieren. Zur Inbetriebnahme neuer IT-Systeme ist eine dokumentierte und durchgeführte Übergabe an den Systembetreiber durchzuführen.

INTERNAL

Die Systemplanung (funktionale Spezifikation, Systementwurf, Systemimplementierung) und die Systemabnahme (Systemeinführung) sind entsprechend den konzernweit geltenden Standards zur Systementwicklung (z. B. IT PEP) auszuführen.

4.4 Schutz vor Schadcode und Mobile Code

IT-Geräte und IT-Systeme sind durch Schutzmaßnahmen (z. B. Virenscanner), die durch die zuständige Stelle (siehe Anhang B.2.7) genehmigt wurden, vor Schadsoftware zu schützen. Die jeweiligen Schutzmaßnahmen sind zu dokumentieren und auf dem aktuellen Stand zu halten.

Werden IT-Geräte mit Schadsoftware (z. B. Malware) infiziert, sind sie unter Abschätzung möglicher Auswirkungen (z. B. Produktionsausfälle) vom Netzwerk zu trennen. Es gelten die Vorgaben der Regelung (siehe Anhang A.1.1).

4.5 Datensicherung

Alle Personen, die für IT-Systeme zuständig sind, müssen für ausreichende Datensicherungen sorgen, damit eine gegebenenfalls erforderliche Wiederherstellung von Informationen in einem angemessenen Zeitrahmen möglich ist. Die Vorgaben aus der Regelung (siehe Anhang A.1.7) sind zu befolgen.

4.6 Netzwerksicherheitsmanagement

Nach der Installation von Netzwerkkomponenten (z. B. Router) sind umgehend deren systemspezifische Schutzfunktionen (z. B. Passwortschutz) zu aktivieren und Standardpasswörter entsprechend den Vorgaben für Passwörter zu ändern. Alle aktiven Netzwerkkomponenten sind mithilfe eines Managementsystems zentral zu verwalten und zu überwachen, um Fehler oder kritische Ereignisse rechtzeitig erkennen zu können.

4.7 Elektronische Kommunikation

Es gelten folgende Vorgaben:

- Systemgenerierte E-Mails müssen einer verantwortlichen Person zugeordnet werden können.
- E-Mail-Postfächer sind vor unbefugtem Zugriff zu schützen.

4.8 Öffentlich verfügbare Informationen

Für den Zugriff aus öffentlich erreichbaren IT-Systemen auf interne Netzwerke dürfen ausschließlich sichere Gateway-Komponenten verwendet werden.

Informationen der jeweiligen Marken und Gesellschaften des Volkswagen Konzerns, die über öffentlich erreichbare IT-Systeme bereitgestellt werden, sind durch geeignete Sicherheitsmaßnahmen (z. B. verschlüsselte Übertragung von Authentifizierungsinformationen) vor unbefugten Zugriffen und Änderungen zu schützen.

4.9 Monitoring

4.9.1 Audit-Protokolle

Der Zugriff von Nutzern auf IT-Systeme, die als "geheim" klassifizierte Informationen verarbeiten, muss protokolliert werden. Die Protokolle (Logs) sind entsprechend den betrieblichen Regelungen der Gesellschaft aufzubewahren (siehe Anhang A.1.2).

Folgende Inhalte müssen Protokolle mindestens enthalten:

INTERNAL

- eindeutige Identifizierung der protokollierten Person (z. B. Name oder ID)
- Protokoll der Zugriffsversuche auf das IT-System
- Protokoll der Zugriffe auf Daten und andere Ressourcen

4.9.2 Verwendung des Monitoring-Systems

Alle Protokolle sind regelmäßig im Rahmen von Audits oder bei vermuteten Informationssicherheitsvorfällen zu prüfen.

Bei der Prüfung von Protokollen sind die erforderlichen Genehmigungsverfahren zu befolgen (siehe Anhang 08).

4.9.3 Schutz von Protokollinformationen

Alle Protokolle sind so aufzubewahren, dass die protokollierten Personen keine Berechtigung zum Modifizieren oder Ändern der Protokollinformationen haben. Protokolle dürfen nicht manipuliert oder deaktiviert werden. Systemadministratoren dürfen die Protokollierung nicht unbemerkt deaktivieren können.

Falls in Protokollen als "geheim" klassifizierte Informationen enthalten sind (z. B. die Daten selbst vor und nach einer Änderung, übertragene Daten o. ä.), muss sichergestellt werden, dass nur solche Personen Zugriff darauf haben, für die der Informationseigentümer die Genehmigung erteilt hat.

4.9.4 Administrator- und Betreiberprotokolle

Alle Tätigkeiten von Administratoren und Systembetreibern in IT-Systemen, die als „vertraulich“ oder „geheim“ klassifizierte Informationen enthalten, müssen protokolliert werden. Mindestens für IT-Systeme, in denen als „geheim“ klassifizierte Informationen verarbeitet werden, müssen Aktivitätsprotokolle der Systembetreiber so gespeichert werden, dass auch Personen mit erweiterten Zugriffsrechten die Protokollinformationen nicht ändern oder löschen können.

Die Inhalte, die Protokolle mindestens enthalten müssen, sind in der Regelung (siehe Anhang A.1.2) dokumentiert.

4.9.5 Fehlerprotokollierung

Alle durch Nutzer gemeldete Fehler und Funktionsstörungen sind zu protokollieren. Alle Maßnahmen, die Betreiber zum Zwecke der Fehlerbehebung unternehmen, sind zu dokumentieren.

4.9.6 Zeitsynchronisierung

Informationssysteme, in denen Protokollinformationen gespeichert werden, müssen auf eine genau vereinbarte gemeinsame Referenzzeit synchronisiert werden.

INTERNAL

5 Zugriffskontrolle

5.1 Geschäftsanforderungen für die Zugriffskontrolle

Für den Zugriff auf Informationen sind auf Grundlage einer durch den Informationseigentümer durchgeführten Risikobewertung Mechanismen zur Authentifizierung und Autorisierung einzurichten. Die durch den Informationseigentümer spezifizierten Rollen und Berechtigungen müssen implementiert werden. Weiterführende Vorgaben zum Thema Zugriffskontrolle sind in der Regelung (siehe Anhang A.1.2) dokumentiert und zu beachten.

Ein Antrag auf Zugriffsrechte für IT-Systeme muss schriftlich unter Verwendung eines entsprechenden Formulars (z.B. Benutzerantrag) bzw. über ein festgelegtes und genehmigtes IT-System erfolgen (siehe Anhang A.1.2). Es muss dokumentiert werden, welche Personen Zugriffsrechte auf ein bestimmtes IT-System haben.

Die Vergabe von Zugriffsrechten muss durch die Leitung der Organisationseinheit des Nutzers sowie durch den Informationseigentümer (Vier-Augen-Prinzip) bewilligt werden. Ausnahmen sind zentrale Dienste (z. B. das Intranet). Die Übertragung zur Genehmigung ist zulässig.

Benutzerkennungen sind stets Einzelpersonen zuzuweisen. Die Verteilung von Identifikationsmitteln (z. B. SmartCards oder SecurID-Karten) zum Zweck des Wartungszugriffs ist unter den folgenden Voraussetzungen gestattet:

- Die Verteilung wird durch eine verantwortliche Person dokumentiert. Die verantwortliche Person stellt sicher, dass schriftlich protokolliert wird, durch wen Identifikationsmittel aus welchem Grund und zu welchem Zeitpunkt an wen verteilt wurden.
- Für diese Dokumentation gelten dieselben Aufbewahrungsfristen wie für die Aufbewahrung von Benutzeranträgen. Es sind Vorgehensweisen für die Generierung und das Zurücksetzen von Passwörtern zu definieren und zu veröffentlichen.

5.2 Benutzerverwaltung

Weiterführende Vorgaben zum Thema Benutzerverwaltung sind in der Regelung (siehe Anhang A.1.2) dokumentiert und zu beachten.

Nach der Installation eines IT-Systems bzw. einer Software sind umgehend die Standardpasswörter des Herstellers entsprechend den Vorgaben für Passwörter zu ändern.

Alle zur regelmäßigen Prüfung der Benutzerberechtigungen erforderlichen Informationen müssen der Leitung jeder OE zur Verfügung gestellt werden.

Soweit technisch machbar, sind die Zugriffsberechtigungen von Beschäftigten externer Lieferanten/Partnerunternehmen für IT-Systeme auf die Dauer eines Projekts zu beschränken (maximal ein Jahr).

Benutzerkennungen, die mehr als 400 Tage nicht verwendet wurden, sind zu sperren.

Für Passwörter sind die folgenden Mindestanforderungen zu erfüllen (diese gelten nicht für PINs):

- Es müssen geeignete Maßnahmen getroffen werden, die das Erraten von Benutzerkennungen und Passwörtern verhindern (z. B. verlängerte Wartezeit zwischen fehlgeschlagenen Anmeldeversuchen oder Zugriffssperren nach einer bestimmten Anzahl an fehlgeschlagenen Anmeldeversuchen).

INTERNAL

- Die Anmeldung an IT-Systemen muss sicher verschlüsselt erfolgen. Ist dies nicht möglich, sind Einmalpasswörter zu verwenden.

Für den Umgang mit Passwörtern sind die folgenden Mindestanforderungen zu erfüllen:

- Vordefinierte bzw. Standard-Passwörter in IT-Systemen müssen in individuelle Passwörter geändert werden.
- Passwörter dürfen niemals als Klartext gespeichert werden.
- Jeder Nutzer muss jederzeit die Möglichkeit haben, sein Passwort zu ändern.
- Passwörter dürfen bei der Eingabe an Bildschirmen nicht als Klartext angezeigt werden.

5.3 Pflichten von Nutzern mit privilegierten Rechten

5.3.1 Allgemeine Vorgaben

Folgende Vorgaben sind durch alle Systembetreiber und Administratoren zu befolgen:

- Die Vorgaben aus der Informationssicherheits-Handlungsleitlinie für Beschäftigte (Umgang mit Passwörtern) bzw. für Dritte, sofern der Systembetreiber oder Administrator Beschäftigter einer Partnerfirma ist, sind zu befolgen.
- Die Vorgaben aus der Regelung (siehe Anhang A.1.2) sind zu befolgen und in IT-Systemen und Anwendungen umzusetzen. In allen IT-Systemen/Anwendungen müssen die Anforderungen an Passwörter aus der Regelung durchgesetzt werden.
- Routinetätigkeiten, für die keine administrativen Rechte erforderlich sind, dürfen nicht mit privilegierten/administrativen Benutzerkennungen durchgeführt werden. Hierfür ist eine Benutzerkennung mit eingeschränkten Rechten zu verwenden. Das Passwort einer administrativen Benutzerkennung darf nicht für weitere Benutzerkennungen verwendet werden. Zusätzliche Konten können beispielsweise dann erforderlich sein, wenn Anwendungen oder IT-Systeme nicht an den zentralen Authentifizierungsdienst angeschlossen sind, oder für unterschiedliche Rollen (Nutzer/Administrator).

5.3.2 Generierung von Passwörtern (persönliche Administrator-Konten und IT-Systembezogene Konten)

Bei der Generierung eines Passworts müssen folgende Mindestanforderungen erfüllt werden:

- Es sind keine trivialen Passwörter zulässig (z. B. „Test1234“) oder Passwörter aus dem persönlichen Umfeld (z. B. Name, Geburtsdatum).
- Es dürfen keine identischen Passwörter für berufliche und private Zwecke generiert werden.
- Es dürfen keine identischen Passwörter für IT-Systeme, die vom Volkswagen Konzern bereitgestellt werden, und IT-Systeme, die von Dritten bereitgestellt werden (z. B. Anwendungen, Registrierungsdienste im Internet), generiert werden.
- Passwörter müssen mindestens einmal jährlich geändert werden.

5.3.2.1 Persönliche administrative Benutzerkennungen

Administrator-Konten dürfen ausschließlich Nutzern zugewiesen werden, die die obligatorische Schulung zur Informationssicherheitssensibilisierung für Administratoren (siehe Anhang A.1.8) abgelegt haben.

INTERNAL

Weiterführende Vorgaben zum Thema persönliche administrative Benutzerkennungen sind in der Regelung (siehe Anhang A.1.2) dokumentiert und zu beachten.

5.3.2.2 Systembezogene Benutzerkennungen

Die Verfügbarkeit von systembezogenen Passwörtern ist durch die für das IT-System verantwortliche Person zu gewährleisten (z. B. durch das Hinterlegen von Passwörtern).

Weiterführende Vorgaben zum Thema systembezogene Benutzerkennungen sind in der Regelung (siehe Anhang A.1.2)dokumentiert und zu beachten.

5.3.3 Verwendung von administrativen Benutzerkennungen

Administrative Funktionen (wie z. B. die Benutzerverwaltung) dürfen nur für die jeweilige Aufgabe und unter Verantwortung des individuellen Administrators verwendet werden. Administrative Berechtigungen sind entsprechend den Grundsätzen „geringste Berechtigung“ und „Need to know“ mithilfe von funktions-/rollenspezifischen Profilen zu beschränken.

Es dürfen nur persönliche Administrator-Konten verwendet werden.

Die unternehmensspezifischen Regelungen (siehe Anhang 05) sind zu befolgen.

Folgende administrative Tätigkeiten sind unter Verwendung der zur Verfügung stehenden administrativen Funktionen zulässig:

- Wartung und Fehlerbehebung
- Verwaltung von Zugriffsrechten für Nutzer in der eigenen Organisationseinheit für den Zugriff auf Daten der eigenen Organisationseinheit. Für die Vergabe von Zugriffsrechten für Daten der eigenen Organisationseinheit an Nutzer, die nicht zur eigenen Organisationseinheit gehören, ist die dokumentierte Genehmigung der zuständigen Leitung der Organisationseinheit erforderlich.
- Installation geprüfter und genehmigter Software entsprechend den Lizenzbedingungen
- Für das Ausführen von administrativen Tätigkeiten für Kunden (z. B. zur Fehlerbehebung) ist die vorherige Genehmigung durch den zuständigen Nutzer erforderlich. Für die Installation von Standardsoftware oder Sicherheits-Updates, die über die zentrale Softwareverteilung bereitgestellt werden, ist keine Genehmigung erforderlich.

Folgende administrative Tätigkeiten sind nicht zulässig:

- Entfernen von Nutzergruppen oder Systemkonten zentraler Stellen aus der Gruppe der lokalen Administratoren ohne Genehmigung durch den Vorgesetzten
- Erstellen von zusätzlichen Administrator-Konten (unter Umgehung des Prozesses zum Erstellen von Administrator-Konten)
- Administration von fremden Gruppen oder fremden Arbeitsplatzrechnern (nicht zuständige OEs)
- Erstellen von Konten mit Passwörtern ohne Ablaufdatum
- Zugriff auf Speicherbereiche von Nutzern sofern nicht für administrative Tätigkeiten erforderlich. Für den Zugriff auf Inhalte (z. B. Öffnen von Dateien) ist eine Genehmigung entsprechend den unternehmensspezifischen Regelungen erforderlich (siehe Anhang 06).
- Erstellen von lokalen Konten

5.4 Netzwerkzugriffskontrolle

Nur angemeldete und berechtigte Nutzer dürfen Zugriff auf das konzerninterne Netzwerk erhalten. Die Vorgaben aus der Regelung (siehe Anhang A.1.9) sind zu befolgen.

INTERNAL

Externe Zugriffe auf das konzerninterne Netzwerk sind durch Zwei-Faktor-Authentifizierung (z. B. mittels PKI-Ausweis) zu schützen. Datenübertragungen sind durch sichere Verschlüsselung zu schützen. Die Vorgaben aus der Regelung (siehe Anhang A.1.9) sind zu befolgen.

Alle nicht benötigten Dienste und Ports sind zu deaktivieren.

Sämtliche erforderliche Netzwerkkommunikation ist zu dokumentieren.

Jedes IT-System ist in ein Netzwerksegment einzugliedern, welches das erforderliche Sicherheitsniveau bietet. Details hierzu finden sich in der entsprechenden Regelung (siehe Anhang A.1.10).

5.5 Betriebssystem-Zugriffskontrolle

5.5.1 Sichere Anmeldeverfahren

Der Zugriff auf IT-Systeme, die nicht-öffentliche Daten enthalten, muss durch geeignete Mittel (z. B. Authentifizierung) abgesichert und auf berechtigte Nutzer beschränkt werden.

Der IT-Systemverantwortlicher ist verantwortlich für die Implementierung sicherer Anmeldeverfahren (z. B. starke Authentifizierung mittels PKI-Karte) entsprechend der jeweiligen Datenklassifizierung.

Weiterführende Vorgaben zum Thema sichere Anmeldeverfahren sind in der Regelung (siehe Anhang A.1.2) dokumentiert und zu beachten.

5.5.2 Benutzeridentifikation und -authentifizierung

Soweit technisch machbar, muss für administrative Aufgaben eine starke Authentifizierung eingerichtet werden (Zwei-Faktor-Authentifizierung über „Kenntnis und Eigentum“). Falls dies nicht möglich ist, sind nach Vereinbarung mit den zuständigen Stellen (siehe Anhang 07) alternative Sicherungsmethoden (z. B. stärkere Passwörter) zu verwenden.

Bei der Generierung oder dem Zurücksetzen eines Passworts müssen die für Passwörter geltenden Mindestanforderungen erfüllt werden.

5.5.3 Passwortmanagement

Die für die jeweiligen IT-Systeme zuständigen Personen müssen die in der Regelung (siehe Anhang A.1.2) festgelegten Mindestanforderungen an Passwörter umsetzen.

5.5.4 Verwendung von IT-Systemwerkzeugen

Es müssen geeignete Maßnahmen (z. B. Entzug entsprechender Berechtigungen) getroffen werden, um zu verhindern, dass unbefugte Nutzer sicherheitsrelevante IT-System- und Anwendungseinstellungen (beispielsweise über IT-Systemwerkzeuge) ändern können.

5.5.5 Session-Timeouts

Dialogsitzungen, die nach einem längeren Zeitraum nicht mehr aktiv verwendet werden, müssen deaktiviert oder durch geeignete Mittel geschützt werden.

INTERNAL

5.5.6 Sicheres Löschen von Datenträgern

Bei der Entsorgung oder dem Recycling von Datenträgern ist ein sicheres Löschen bzw. Zerstören zu gewährleisten.

Es muss sichergestellt werden, dass Daten mit hoher Wahrscheinlichkeit nicht mehr wiederhergestellt werden können.

Folgende Vorgaben sind für das sichere Löschen zu befolgen:

Allgemeine Vorgaben:

- Wenn ein sicheres Löschen nicht möglich ist (oder fehlschlägt), muss der Datenträger physisch zerstört werden.
- Das sichere Löschen ist durch die zuständige Stelle (siehe Anhang B.2.17) durchzuführen.
- Es muss ein Nachweis über das sichere Löschen verwahrt werden.
- Zum sicheren Löschen dürfen nur genehmigte Werkzeuge verwendet werden (siehe Anhang 04).

Magnetische Datenträger (HDDs):

- Zum Überschreiben muss ein Pseudozufallszahlengenerator-Stream verwendet werden.
    - Interne Daten: einfaches Überschreiben ist ausreichend
    - Vertrauliche und geheime Daten: Diese müssen mindestens zweifach überschrieben werden. Das erfolgreiche Überschreiben muss durch die löschende Stelle überprüft werden.

Nichtmagnetische Datenträger (USB-Laufwerke, Flash-Speicherkarten usw.):

- Die Verwendung eines Pseudozufallszahlengenerator-Streams wird empfohlen.
- Einfaches Überschreiben ist ausreichend.

Solid State Disks (SSD-Festplatten):

- Das Verfahren „Enhanced Secure Erase“, das vom Hersteller der SSD unterstützt sein muss, ist zu verwenden.
- Der Hersteller muss bestätigen, dass die verwendete Methode zum Löschen als sichere Methode für seine Produkte gilt.
- Wenn dies nicht erfüllt werden kann, muss die SSD physisch zerstört werden.

6 Beschaffung, Entwicklung und Wartung von IT-Systemen

6.1 Sicherheitsanforderungen für IT-Systeme

Bevor ein IT-System entwickelt und eingesetzt wird, sind alle erforderlichen Informationssicherheitsmaßnahmen zu identifizieren und zu implementieren (z. B. IT-Systemhärtung oder Patch Management).

Für die Umsetzung der auferlegten Informationssicherheitsmaßnahmen ist der jeweilige IT-System-verantwortliche verantwortlich. Dies gilt auch beim Einsatz von zentral bereitgestellten Sicherheits-technologien.

INTERNAL

6.1.1 Vertraulichkeit

Informationen sind entsprechend ihrer Klassifizierung vor unbefugtem Zugriff zu schützen. Je nach Klassifizierung in Bezug auf die Vertraulichkeit sind folgende Sicherheitsmaßnahmen erforderlich:

Klassifizierung	Definition
Öffentlich	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches)
Intern	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Need to know“ • Ein-Faktor-Authentifizierung (z. B. Benutzerkennung und Passwort)
Vertraulich	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Need to know“ • Zwei-Faktor-Authentifizierung (z. B. Smartcard und PIN) – insbesondere für den Zugriff auf Anwendungen – oder zusätzliche Schutzmechanismen wie verschlüsseltes Speichern (z. B. verschlüsselte Daten auf Dateifreigaben oder verschlüsselte USB-Laufwerke) • Transportverschlüsselung
Geheim	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Need to know“ • Zwei-Faktor-Authentifizierung (z. B. Smartcard und PIN), insbesondere für den Zugriff auf Anwendungen • Transportverschlüsselung • Datenspeicherverschlüsselung

6.1.2 Integrität

Informationen sind entsprechend ihrer Klassifizierung vor unerwünschten Änderungen und unbefugten Manipulationen zu schützen. Je nach Klassifizierung in Bezug auf die Integrität sind folgende Sicherheitsmaßnahmen erforderlich:

Klassifizierung	Definition
Niedrig	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches)
Mittel	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Need to know“ • Ein-Faktor-Authentifizierung (z. B. Benutzerkennung und Passwort) • Datenbanken: Der Schutz der referentiellen Integrität muss aktiviert sein.

INTERNAL

Hoch	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Need to know“ • Validierung von Eingangs- und Ausgangsdaten sowie Kontrolle der internen Verarbeitung auf Fehlerreduzierung und Vermeidung von Standardangriffen wie „Buffer Overflows“ oder Einschleusung von ausführbarem Code (z. B. Steuerung der Beschränkung für Felder, Feldbeschränkung für spezielle Bereiche) • Erstellen sicherer Hash-Werte für Daten • Verifizierung von Hash-Werten vor der Verarbeitung von Daten
Sehr hoch	Zusätzlich zu den Anforderungen für „Hoch“: • Zwei-Faktor-Authentifizierung (z. B. Smartcard und PIN) für Schreibzugriffe • Generierung und Verifizierung von digitalen Signaturen für gespeicherte Daten bzw. vergleichbare Sicherheitsmaßnahmen • Erstellen sicherer Hash-Werte für Daten • Verifizierung von Hash-Werten vor der Verarbeitung von Daten • Signieren von Hash-Werten (sichere Speicherung von Schlüsseln)

6.1.3 Verfügbarkeit

Die Verfügbarkeit von IT-Systemen muss entsprechend der jeweiligen Klassifizierung gewährleistet werden. Je nach Klassifizierung in Bezug auf die Verfügbarkeit sind folgende Sicherheitsmaßnahmen erforderlich:

Klassifizierung	Definition
Niedrig	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Wiederherstellungsmaßnahmen in 72 Stunden oder später. Dazu sind geeignete Maßnahmen zu implementieren.
Mittel	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Wiederherstellungsmaßnahmen in 24 Stunden bzw. höchstens 72 Stunden (BIA-IT: Stufe 3 und 4). Dazu sind geeignete Maßnahmen zu implementieren.
Hoch	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Wiederherstellungsmaßnahmen in 1 Stunde bzw. höchstens 24 Stunden (BIA-IT: Stufe 2). Dazu sind geeignete Maßnahmen zu implementieren.
Sehr hoch	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Wiederherstellungsmaßnahmen innerhalb 1 Stunde (BIA-IT: Stufe 1). Dazu sind geeignete Maßnahmen zu implementieren.

6.2 Kryptographische Maßnahmen

Die Vorgaben aus der Regelung (siehe Anhang A.1.11) sind einzuhalten.

INTERNAL

6.3 Sicherheit von Systemdateien

6.3.1 Kontrolle von betrieblicher Software

Software darf ausschließlich durch berechtigte Beschäftigte installiert werden (siehe Anhang 09).

Neue oder geänderte Programme dürfen erst in laufenden Systemen eingesetzt werden, wenn sie entsprechend den gültigen Changemanagement-Prozessen (siehe Anhang A.1.5) erfolgreich getestet und freigegeben wurden. Die Version bzw. der Status der Korrektur der verwendeten Software ist entsprechend den unternehmensspezifischen Regelungen (siehe Anhang 010) zu dokumentieren und zu archivieren.

6.3.2 Zugriffskontrolle auf Quellcode

Programmquellcode ist entsprechend der jeweiligen Datenklassifikation (hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit) zu klassifizieren und zu schützen.

6.4 Sicherheit in Entwicklungs- und Supportprozessen

Der Einsatz von Administrationswerkzeugen und Protokollen darf die Sicherheit von Anwendungen nicht beeinträchtigen.

Bevor neue Versionen oder Patches für eine Software installiert werden, sind Tests durchzuführen, um sicherzustellen, dass die Modifikationen weder den laufenden Betrieb noch die Sicherheit beeinträchtigen.

Geltende Verfahrensbeschreibungen und betriebliche Dokumentationen sind nach Änderungen bei Bedarf anzupassen.

Werden Änderungen an Softwarepaketen vorgenommen, sind deren Auswirkungen auf vorhandene Regelungen, Verträge und Sicherheitsmaßnahmen zu ermitteln. Eine Änderung darf nur durchgeführt werden, wenn sie laut Lizenzen und Wartungsverträgen zulässig ist.

6.5 Management von Patches und technischen Schwachstellen

Um mögliche Risiken zu minimieren, sind alle verfügbaren Sicherheitsupdates und -patches unverzüglich zu testen und zu installieren.

Geltende Verfahrensbeschreibungen und betriebliche Dokumentationen sind bei Bedarf anzupassen.

Die Vorgaben aus der Regelung (siehe Anhang A.1.5) sind zu befolgen.

Regelmäßige Überprüfungen auf Verwundbarkeiten müssen durchgeführt werden.

7 IT Service Continuity Management

Unvorhersehbare oder unerwartete Ereignisse, die zu unzumutbar langen IT-Systemausfällen führen und Geschäftsprozesse bedrohen können, werden nachstehend gemeinsam als IT-Notfälle bezeichnet.

Es müssen Methoden zur Identifizierung und Bewertung kritischer IT-Geschäftsprozesse entwickelt werden, mit denen die Geschäftskontinuität, wie in der Regelung (siehe Anhang A.1.12) beschrieben, sichergestellt werden kann.

INTERNAL

8 Compliance und Einhaltung von Verpflichtungen

Für den Einsatz von IT-Systemen auf IT-Infrastrukturen ist der durch die IT-Infrastruktur gewährleistete Schutz bezüglich Vertraulichkeit, Integrität und Verfügbarkeit nicht zu überschreiten. Sollte dies in Ausnahmefällen nicht sichergestellt werden können, sind die IT-Systemverantwortlichen verpflichtet gemeinsam mit dem Verantwortlichen der IT-Infrastruktur entsprechende Lösungen zu finden, sodass eine angemessene Wirtschaftlichkeit erreicht wird.

Bei der Nutzung von Verschlüsselung und/oder elektronischen Signaturen (siehe Anhang 01) müssen alle länderspezifischen Bestimmungen zum Import und Export von bzw. dem Zugriff auf Hardware, Software und Informationen befolgt werden. Dies gilt insbesondere bei der Nutzung im Ausland.

Bei Fragen zu länderspezifischen Bestimmungen sind die entsprechenden Stellen zu kontaktieren (siehe Anhang 02).

Alle Systembetreiber müssen zufällige Stichprobenprüfungen für ihre IT-Systeme durchführen, um die Einhaltung der sicherheitsbezogenen Bestimmungen und Leitlinien zu verifizieren. Die Ergebnisse sind zu dokumentieren.

Methoden und Werkzeuge zur Systemüberwachung (z. B. Auditfunktionen des Betriebssystems) sind entsprechend dem hierfür geltenden Genehmigungsverfahren einzurichten und zu verwenden (siehe Anhang 03).

Alle Systembetreiber sind verpflichtet, in IT-Systemen entdeckte Sicherheitslücken zu schließen.

Die Anforderungen und Tätigkeiten im Rahmen von Audits sind sorgfältig zu planen (insbesondere für laufende Systeme), um das Risiko der Beeinträchtigung von Geschäftsprozessen zu minimieren.

Die folgenden Vorgaben sind zu befolgen:

- Der Testumfang ist festzulegen und zu prüfen.
- Zu Testzwecken dürfen Software und Daten ausschließlich mit Lesezugriff verwendet werden.
- IT-Ressourcen sind zu identifizieren und für die Tests zur Verfügung zu stellen.
- Alle Verfahren, Anforderungen und Zuständigkeiten sind zu dokumentieren.

Um den Missbrauch oder die Kompromittierung von Auditwerkzeugen zu verhindern, dürfen ausschließlich berechtigte Beschäftigte die Werkzeuge für IT-Systemaudits verwenden.

Die unbegrenzte Auditberechtigung der Revisionsabteilung ist hiervon nicht betroffen.

INTERNAL

II Zuständigkeiten

Bei mitbestimmungspflichtigen Sachverhalten ist die Einbindung der betriebsverfassungsrechtlichen Gremien sicherzustellen.

Verstöße gegen die Handlungsleitlinien werden individuell nach gültigen gesetzlichen, vertraglichen und gesellschaftsrechtlichen Bestimmungen geprüft und entsprechend geahndet.

Abweichungen von dieser Handlungsleitlinie, die das Sicherheitsniveau senken, sind nur temporär und nach Rücksprache mit den zuständigen Stellen (siehe Anhang 01.1) gestattet.

INTERNAL

Anhang

INTERNAL

A Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheitsregelung Nr. 03.01.01 Anti-Malware und Systemschutz

A.1.2 Informationssicherheitsregelung Nr. 03.01.05 IAM

A.1.3 Informationssicherheitsregelung Nr. 03.01.09 Ausnahmegenehmigungen

A.1.4 Glossar Information Security

A.1.5 Informationssicherheitsregelung Nr. 03.01.08 Change und Patch Management

A.1.6 Informationssicherheitsregelung Nr. 03.01.16 Dienstleistung durch Dritte

A.1.7 Informationssicherheitsregelung Nr. 03.01.06 Backup und Archivierung

A.1.8 Informationssicherheitsregelung 03.01.10 Awareness und Schulung

A.1.9 Informationssicherheitsregelung Nr. 03.02.04 Netzwerkzugänge

A.1.10 Informationssicherheitsregelung Nr. 03.02.02 Trennung und Zonierung

A.1.11 Informationssicherheitsregelung Nr. 03.01.02 Kryptographie

A.1.12 Informationssicherheitsregelung: 03.01.14 IT Service Continuity Management

Die mitgeltenden Unterlagen sind auf der Konzern Informationssicherheit Website zu finden:
https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk

A.2 Anhänge

A.2.1 Feedbackformular

Das Feedbackformular für Verbesserungsvorschläge zu den Regelungen kann im Downloadbereich der Konzern Informationssicherheit Website https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk heruntergeladen werden.

Bitte senden Sie das ausgefüllte Formular an: VWAG R: WOB, IT Security Regulations <itsr@volkswagen.de>

INTERNAL

A.3 Gültigkeit

Diese Informations-Sicherheitsregelung tritt zum Zeitpunkt der Veröffentlichung in Kraft. Aktualisierte Inhalte dieser Regelung sind innerhalb eines Übergangszeitraums von sechs Monaten umzusetzen.

Nächstes Überprüfungsdatum: September 2023

A.4 Dokumenthistorie

Version	Name	Org.-Einheit	Datum	Kommentar
1.0	K-SIS/G1	K-SIS/G1	25 Mai 2004	Initiale Version
2.0	K-SIS/G1	K-SIS/G1	30. 01.2013	Überarbeitung durch GISSC Prozess
3.0	K-SIS/G1	K-SIS/G1	11.11 2015	Überarbeitung durch GISSC Prozess
3.0a	K-FIS/G	K-FIS/G	14. März 2019	C2.15: Spezifisches Produkt entfernt
4.0	K-DS/G	K-DS/G	22. September 2022	Überarbeitung durch Regelungsteam und Freigabe in K-DS Leitungsrunde
4.1	K-DS/G	K-DS/G	03.11.2022	Ergänzungen in Kapitel 4.1.4 und 6.1

INTERNAL

B Gesellschaftsspezifische Ausprägungen

B.1 Konzernweit geltend

In diesem Kapitel werden Ausprägungen aufgeführt, die für den gesamten Konzern gelten. Diese spezifischen Ausprägungen dürfen nicht verändert werden.

B.1.1 Die zuständige Stelle bei Abweichungen von diesen Handlungsleitlinien, die das Sicherheitsniveau senken, ist die jeweilige Informationssicherheitsorganisation der Marke oder Gesellschaft. Generell sind die Vorgaben der Regelung zu Ausnahmegenehmigungen (Siehe Anhang A.1.3) zu beachten.

B.1.2 Kontakt für die Volkswagen AG über My.Serve: https://iserve.vw.vwg/vw/catalog_item_detail.do?sysparm_document_key=sc_cat_item,7f89128a50e61600ac0ade4eccc3502f

B.2 Gesellschaftsspezifische Ausprägungen

In diesem Kapitel werden spezifische Eigenschaften aufgeführt, die für eine Gesellschaft gelten. Diese Eigenschaften können je nach Gesellschaft angepasst werden. Zur Information werden Ausprägungen, die für die Marke Volkswagen gelten, kursiv angegeben.

B.2.1 *Speicherprogrammierbare Steuerungen (SPS) und Robotersteuerungen müssen in Netzwerken betrieben werden, in denen ausschließlich die für den Betrieb erforderliche Kommunikation zulässig ist.*

B.2.2 Veröffentlicht im Intranet:
https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk+-+Politik

B.2.3 Für Marke Volkswagen dokumentiert in der ORL 18

B.2.4 *Weiterführende Informationen sind dem Self Service Portal der Konzernsicherheit K-SK-3 zu entnehmen: https://volkswagen-net.de/wikis/display/Konzernsicherheit/Selfservice-Portal*

B.2.5 Bei IT-Systemen handelt es sich um vollständige IT-Systeme mit Hardware- und Softwarekomponenten einschließlich deren wechselseitiger Kommunikationsbeziehungen.

B.2.6 Dokumentation ist unter Einhaltung der gesetzlichen Bestimmungen und der Vorgaben der Abteilung zu archivieren. Beispielsweise sind Dokumente, die sich indirekt auch auf die Buchhaltung beziehen, gemäß den „Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)“ für die gesamte Lebensdauer des IT-Systems und 10 Jahre darüber hinaus zu archivieren. In der ORL 24 „Aufbewahrung von Unterlagen“, Regelungsportal (vw.vwg) *, finden sich weitere Details.*

B.2.7 Zuständigkeit: Informationssicherheitsorganisation des Konzerns, E-Mail: ITSG@volkswagen.de

B.2.8 Das Anlegen personenbezogener Protokolle ist durch die zuständige Personalabteilung, die Datenschutzstelle sowie die jeweiligen Komitees zu genehmigen. Die Prüfung von Leistung und Verhalten ist nicht gestattet.

B.2.9 Zuständigkeit: IT-Systemadministratoren und lokale Administratoren

INTERNAL

B.2.10 Die Version bzw. der Status der Korrektur ist unter Einhaltung der gesetzlichen Bestimmungen und der Vorgaben der Abteilung zu archivieren. Beispielsweise sind Dokumente, die sich indirekt auch auf die Buchhaltung beziehen, gemäß den „Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)" für die gesamte Lebensdauer des IT-Systems und 10 Jahre darüber hinaus zu archivieren. In der Organisationsrichtlinie Nr. 24/0 „Aufbewahrung von geschäftlichen und digitalen Dokumenten", http://regelungsportal.wob.vw.vwg/Seiten/Start.aspx , finden sich weitere Details.

B.2.11 Nationales Gesetz zur Anerkennung elektronischer Signaturen: In Deutschland hat das Signaturgesetz (SigG) Gültigkeit. In diesem Gesetz werden die allgemeinen Bedingungen für die Verwendung elektronischer Signaturen beschrieben. Es wurde an die EU-Richtlinie „Gemeinschaftliche Rahmenbedingungen für elektronische Signaturen" vom 13.12.1999 [ECRL99] angepasst und hat mit seinem Inkrafttreten als „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften" am 22.05.2001 das Signaturgesetz von 1997 abgelöst. Durch dieses Gesetz werden die Rahmenbedingungen für die Gleichstellung von qualifizierten elektronischen Signaturen mit handschriftlichen Signaturen geschaffen. Es legt fest, in welchen Fällen qualifizierte elektronische Signaturen gemäß Signaturgesetz gleichwertig mit handschriftlichen Signaturen sind. Als Ergebnis gelten digitale Signaturen gemäß Signaturgesetz als sehr sicher, auch vor Gericht.

B.2.12 Zuständigkeit: Rechtsabteilung

B.2.13 Audit-Anforderungen müssen genehmigt werden. Die Audit-Anforderungen sind schriftlich durch die zuständige Personalabteilung, die Datenschutzstelle sowie die jeweiligen Komitees zu genehmigen.

B.2.14 z. B. das Programm „Blancco"

B.2.15 Passwörter für Administrator-Konten müssen sicher verwaltet werden (z.B. Password Vault, Rotation, CyberArc).

B.2.16 Nur in Notfällen zulässig und in Zusammenarbeit mit dem Betriebsrat und der „Kommission Datenschutz".

*B.2.17 Die Inhalte nicht mehr benötigter Speichermedien müssen zuverlässig durch Überschreiben oder physische Zerstörung des Mediums gelöscht werden. Zur ordnungsgemäßen Entsorgung werden Datenträger-Entsorgungsbeutel für Volkswagen-Speichermedien verwendet, die vom Sekretariat (über den normalen Beschaffungsprozess für Büro-Verbrauchsmaterialien) erhältlich sind. Das sichere Löschen bzw. Verschrotten von Speichermedien erfolgt durch IT Client Support (*https://volkswagen-net.de/wikis/display/SFWIKI/IT+Client+Support*).*

B.2.18 Datenschutzmanager-Organisation (DSMO): Ansprechpartner für Ihren Fachbereich finden Sie im Datenschutz-Wiki. Für weitere Informationen siehe auch: ORL 50 „Datenschutz und Datenschutz-Governance"

INTERNAL

VOLKSWAGEN

AKTIENGESELLSCHAFT

Informationssicherheit

Handlungsleitlinien
– Handlungsleitlinie für IT-Systementwickler –

Herausgeber

Group Information Security Organisation

Regelung Nr.

02.04

Status

Veröffentlicht

Version

4.1

Klassifizierung

Intern

Datum

03.11.2022

Geltungsbereich

Diese Leitlinie gilt für die Volkswagen AG (Organisationseinheiten (OE) auf Konzernebene und auf Markenebene der Marke Volkswagen Pkw, der Marke Volkswagen Nutzfahrzeuge und der Marke Volkswagen Group Components). Alle IT-Systementwickler (gemäß Definition in A.4) müssen diese Leitlinie erfüllen und einhalten.

Bezüglich der Umsetzung der Regelung in anderen Volkswagen-Konzerngesellschaften gilt ORL 1 „Organisatorische Regelungen der Volkswagen AG“.

©Volkswagen AG, Intern, KSU: 2.1

INTERNAL

Inhalt

INTERNAL

I Zweck

In dieser Informationssicherheits-Handlungsleitlinie werden die organisatorischen Vorgaben und Regeln für die Informationssicherheit definiert, die von IT-Systementwicklern in ihrem Zuständigkeitsbereich für IT-Systeme und die IT-Infrastruktur zu befolgen sind.

Darüber hinaus gilt für die Zielgruppe der IT-Systementwickler die Informationssicherheits-Handlungsleitlinie für Beschäftigte bzw. für Dritte, sofern der IT-Systementwickler Beschäftigter einer Partnerfirma ist. IT-Systementwickler (siehe Anhang A.4) müssen sich über alle (rollenspezifischen) Vorgaben informieren und diese einhalten, wenn sie in zusätzlichen Rollen arbeiten.

Zweck dieser Informationssicherheits-Handlungsleitlinie ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Schutz der Rechte und Interessen der Gesellschaft und aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit einer Konzerngesellschaft eingehen und/oder Tätigkeiten für diese ausführen.

Die Inhalte dieses Dokuments basieren auf der internationalen Norm ISO/IEC 27002:2013.

Dieses Dokument und alle zugehörigen Änderungs- und Aktualisierungsmitteilungen werden über die üblichen Verteilwege kommuniziert (siehe Anhang B.2).

INTERNAL

1 Kontext

Die folgende Übersicht zeigt die Einordnung der Informationssicherheits-Handlungsleitlinien in das Regelwerk der Informationssicherheit:

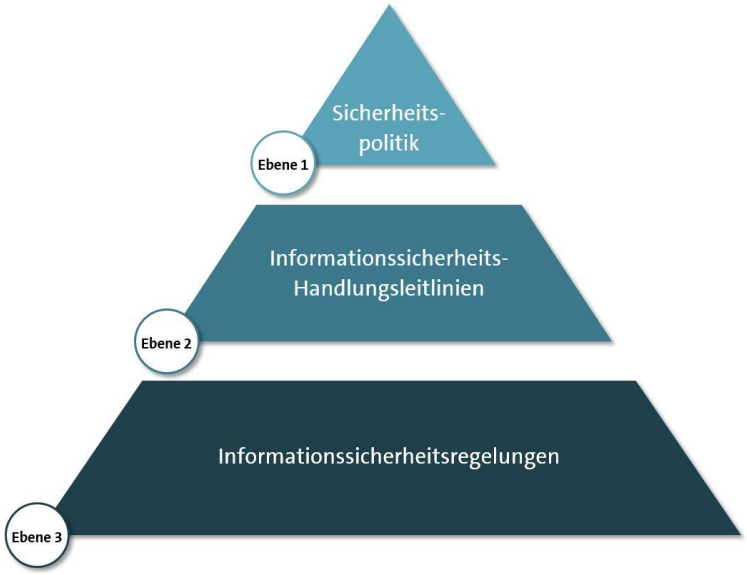


Abbildung 1: Informationssicherheitsregelwerk

Ebene 1: Informationssicherheitspolitik
Definiert die grundlegenden Ziele, Strategien und Verantwortlichkeiten zur Gewährleistung eines Mindestniveaus der Informationssicherheit und ist in der KRL 18 und den abgeleiteten Markenausprägungen (siehe Anhang B.2.2) dokumentiert.

Ebene 2: Informationssicherheitshandlungsleitlinien:
Ausgestaltung der Informationssicherheitspolitik in organisatorische Anweisungen für einzelne Benutzergruppen

Ebene 3: Informationssicherheitsregelungen:
Spezifikation von regulativen Anforderungen im technischen Umfeld und Beschreibung von technischen Funktionen und Prozessen der Informationssicherheit

2 Asset-Management

Die Verantwortung für Informationen hat der jeweilige Informationseigentümer. Dies gilt auch für über IT-Systeme bereitgestellte Informationen. Zuständigkeiten dürfen delegiert werden.

3 Kommunikations- und Betriebsmanagement

Sicherheitsrelevante Tätigkeiten (wie z. B. die Verwaltung kryptographischer Schlüssel, der Sicherheitsinfrastruktur oder von Sicherheitssystemen) dürfen erst durch Dritte ausgeführt werden, nachdem die zuständige Stelle dies genehmigt hat (siehe Anhang 05). Dabei sind die Vorgaben aus der Regelung Nr. 03.01.16 Dienstleistung durch Dritte zu befolgen.

INTERNAL

Die Kapazitätsanforderungen an ein IT-System sind während der Planungsphase zu spezifizieren.

Die Schutzbedarfe an ein IT-System sind ebenfalls in der Planungsphase gemeinsam mit den Informationseigentümern zu spezifizieren.

Die IT-Systemplanung (funktionale Spezifikation, IT-Systementwurf, IT-Systemimplementierung) und die IT-Systemabnahme (IT-Systemeinführung) sind entsprechend den konzernweit geltenden Standards zur IT-Systementwicklung (z. B. IT-PEP) auszuführen.

Informationen, die über öffentlich erreichbare IT-Systeme (z. B. über Internet) bereitgestellt werden, sind durch geeignete Sicherheitsmaßnahmen (z. B. verschlüsselte Übertragung von Authentifizierungs-informationen, Integritätsprüfungen) vor unbefugten Zugriffen und Änderungen zu schützen.

4 Zugangskontrolle

Für den Zugriff auf Informationen sind auf Grundlage einer durch den Informationseigentümer durchgeführten Risikobewertung Mechanismen zur Authentifizierung und Autorisierung einzurichten.

Es müssen geeignete Maßnahmen getroffen werden, die das Erraten von Benutzerkennungen und Passwörtern verhindern (z. B. verlängerte Wartezeit zwischen fehlgeschlagenen Anmeldeversuchen oder Zugriffssperren nach einer bestimmten Anzahl an fehlgeschlagenen Anmeldeversuchen).

Anforderungen zur Authentisierung sind gemäß der Regelung (siehe Anhang A.1.2) umzusetzen. Alle Anmeldeinformationen (z. B. Passwörter oder Schlüssel) sind mindestens als „vertraulich“ zu klassifizieren und entsprechend zu behandeln.

Anmeldeinformationen sind vor unbefugtem Zugriff zu schützen. Passwörter dürfen niemals als Klartext gespeichert werden.

Dialogsitzungen, die nach einem längeren Zeitraum nicht mehr aktiv verwendet werden, müssen deaktiviert oder durch geeignete Mittel geschützt werden.

Bei der Kommunikation mit bzw. zwischen vertraulich oder geheim eingestuften IT-Systemen muss eine gegenseitige (bidirektionale) Authentifizierung (z. B. TLS) verwendet werden.

Die Verarbeitung von Informationen ist gemeinsam mit dem Informationseigentümer festzulegen. Dies schließt ausdrücklich jegliche Verwendung in IT-Systemen oder Übertragungen zwischen IT-Systemen ein. Die Genehmigung durch den Informationseigentümer ist zu dokumentieren.

INTERNAL

5 Beschaffung, Entwicklung und Wartung von IT-Systemen

5.1 Sicherheitsanforderungen für IT-Systeme

Bevor ein IT-System entwickelt und eingesetzt wird, sind alle erforderlichen Informationssicherheitsmaßnahmen zu identifizieren und zu implementieren (z. B. Systemhärtung oder Patch Management).

Für IT-Systeme (z. B. Datenbanken und Sicherungsmedien) gelten ebenfalls die Vorgaben zum Umgang mit Informationen (siehe Informationssicherheits-Handlungsleitlinie für Beschäftigte, Abschnitt „Umgang mit klassifizierten Informationen“).

5.1.1 Vertraulichkeit

Informationen sind entsprechend ihrer Klassifizierung vor unbefugtem Zugriff zu schützen. Je nach Klassifizierung in Bezug auf die Vertraulichkeit sind folgende Sicherheitsmaßnahmen erforderlich:

Klassifizierung	Definition
Öffentlich	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches)
Intern	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Need to know“ • Ein-Faktor-Authentifizierung (z. B. Benutzerkennung und Passwort)
Vertraulich	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Need to know“ • Zwei-Faktor-Authentifizierung (z. B. Smartcard und PIN) – insbesondere für den Zugriff auf Anwendungen – oder zusätzliche Schutzmechanismen wie verschlüsseltes Speichern (z. B. verschlüsselte Daten auf Dateifreigaben oder verschlüsselte USB-Laufwerke) • Transportverschlüsselung
Geheim	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Need to know“ • Zwei-Faktor-Authentifizierung (z. B. Smartcard und PIN), insbesondere für den Zugriff auf Anwendungen • Transportverschlüsselung • Ablageverschlüsselung

5.1.2 Integrität

Informationen sind entsprechend ihrer Klassifizierung vor unerwünschten Änderungen und unbefugten Manipulationen zu schützen. Je nach Klassifizierung in Bezug auf die Integrität sind folgende Sicherheitsmaßnahmen erforderlich:

INTERNAL

Klassifizierung	Definition
Gering	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches)
Mittel	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Need to know“ • Ein-Faktor-Authentifizierung (z. B. Benutzerkennung und Passwort) • Datenbanken: Der Schutz der referentiellen Integrität muss aktiviert sein.
Hoch	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Need to know“ • Validierung von Eingangs- und Ausgangsdaten sowie Kontrolle der internen Verarbeitung auf Fehlerreduzierung und Vermeidung von Standardangriffen wie „Buffer Overflows“ oder Einschleusung von ausführbarem Code (z. B. Steuerung der Beschränkung für Felder, Feldbeschränkung für spezielle Bereiche) • Erstellen sicherer Hash-Werte für Daten • Verifizierung von Hash-Werten vor der Verarbeitung von Daten
Sehr hoch	Zusätzlich zu den Anforderungen für „Hoch“: • Zwei-Faktor-Authentifizierung (z. B. Smartcard und PIN) für Schreibzugriffe • Generierung und Verifizierung von digitalen Signaturen für gespeicherte Daten bzw. vergleichbare Sicherheitsmaßnahmen • Erstellen sicherer Hash-Werte für Daten • Verifizierung von Hash-Werten vor der Verarbeitung von Daten • Signieren von Hash-Werten (sichere Speicherung von Schlüsseln)

5.1.3 Verfügbarkeit

Die Verfügbarkeit von IT-Systemen muss entsprechend der jeweiligen Klassifizierung gewährleistet werden. Je nach Klassifizierung in Bezug auf die Verfügbarkeit sind folgende Sicherheitsmaßnahmen erforderlich:

Klassifizierung	Definition
Gering	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Wiederherstellungsmaßnahmen in 72 Stunden oder später. Dazu sind geeignete Maßnahmen zu implementieren.
Mittel	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Wiederherstellungsmaßnahmen in 24 Stunden bzw. höchstens 72 Stunden (BIA-IT: Stufe 3 und 4). Dazu sind geeignete Maßnahmen zu implementieren.
Hoch	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Wiederherstellungsmaßnahmen in 1 Stunde bzw. höchstens 24 Stunden (BIA-IT: Stufe 2). Dazu sind geeignete Maßnahmen zu implementieren.
Sehr hoch	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches)

INTERNAL

	• Wiederherstellungsmaßnahmen innerhalb 1 Stunde (BIA-IT: Stufe 1). Dazu sind geeignete Maßnahmen zu implementieren.

5.2 Verarbeitung in Anwendungen

Die Sicherheit von IT-Systemen ist durch die Implementierung der Maßnahmen aus den konzernweit geltenden Standards zur IT-Systementwicklung (z. B. IT-PEP) sicherzustellen.

Für alle Beratungstätigkeiten zur Einführung von IT-Systemen gelten die Regelungen und betriebsinternen Vereinbarungen der jeweiligen Konzerngesellschaft (siehe Anhang 03).

5.3 Kryptographische Maßnahmen

Grundlegende Entscheidungen zur Strategie, Verwendung und zum Umgang mit kryptographischen Methoden sind durch die zuständigen Stellen festzulegen (siehe Anhang 04).

Die Vorgaben der Regelung zu Kryptographie (siehe Anhang A.1.3) sind zu befolgen. Es dürfen ausschließlich die darin festgelegten Methoden/Verfahren verwendet werden.

5.4 Sicherheit von IT-Systemdateien

5.4.1 Schutz von IT-Systemtestdaten

Entwicklungsumgebungen, Testumgebungen und Produktivumgebungen (laufende IT-Systeme) sind logisch bzw. physisch voneinander zu trennen.

Sofern möglich, sind Tests mit generierten Testdaten auszuführen (z. B. mithilfe eines Testdatengenerators).

IT-Systeme dürfen nur in Testumgebungen getestet werden, die speziell hierfür vorgesehen sind. Es ist sicherzustellen, dass der Betrieb von produktiven IT-Systemen nicht beeinträchtigt wird.

Wenn zu Testzwecken Einzelpersonen Zugriff auf personenbezogene, vertrauliche oder geheime Daten erhalten, die sie nicht zur Ausführung ihrer vertraglichen Tätigkeiten benötigen, müssen die Daten vor Durchführung der Tests so unkenntlich gemacht werden, dass die Originaldaten nicht identifizierbar sind bevor sie vom produktiven IT-System in die Test- oder Entwicklungsumgebung übertragen werden. Die Kopie bzw. Verwendung von Informationen aus produktiven IT-Systemen ist nur nach vorheriger Genehmigung durch den Informationseigentümer gestattet. Kopierte Daten unterliegen den gleichen Vorgaben zur Informationssicherheit wie die ursprünglichen Daten.

Wenn ausschließlich personenbezogene Daten der Tester aus den Datenschutzkategorien IT-Nutzungsdaten und/oder berufliche Kontakt- und Identifikationsdaten im Entwicklungs- oder Testsystem enthalten sind, ist dies grundsätzlich zulässig. Sämtliche Anforderungen der DSGVO sind in diesem Zusammenhang einzuhalten. Bei Fragen ist die zuständige DSMO (siehe Anhang B.2.6) des Fachbereichs zu kontaktieren.

Nach der Durchführung von Tests sind dafür verwendete Informationen aus produktiven IT-Systemen wieder vollständig zu löschen.

INTERNAL

Die in einem produktiven IT-System geltenden Zugriffsrechte und Rollen sind auch in den Test- und Entwicklungssystemen zu implementieren und den vorgesehenen testenden Personen zuzuweisen, wenn Kopien der produktiven Daten genutzt werden.

5.4.2 Zugriffskontrolle auf Quellcode

Quellcode ist entsprechend der jeweiligen Datenklassifikation (siehe Kapitel 5.1) zu klassifizieren und zu schützen.

5.5 Sicherheit in Entwicklungs- und Unterstützungsprozessen

Alle Vorgehensweisen und Prozesse, die Auswirkungen auf IT-Systeme haben, müssen so gestaltet werden, dass das erwünschte Informationssicherheitsniveau erreicht wird.

Es sind formale Änderungsmanagement-Verfahren zu implementieren. Dabei ist sicherzustellen, dass die Sicherheits- und Überwachungsfunktionen des IT-Systems nicht durch Änderungen kompromittiert werden können.

Werden Änderungen an Softwarepaketen oder deren Quellcode vorgenommen, sind deren Auswirkungen auf vorhandene Regelungen und Sicherheitsmaßnahmen zu ermitteln.

6 Compliance und Einhaltung gesetzlicher Verpflichtungen

Bei der Nutzung von Verschlüsselung und/oder elektronischen Signaturen müssen alle länderspezifischen Bestimmungen zum Import und Export von bzw. dem Zugriff auf Hardware, Software und Informationen befolgt werden.

Die Lizenz- und Nutzungsrechte Dritter gemäß den geltenden Bestimmungen (einschließlich Vertragsrecht) sind bei der Systementwicklung zu beachten und einzuhalten.

INTERNAL

II Zuständigkeiten

Bei mitbestimmungspflichtigen Sachverhalten ist die Einbindung der betriebsverfassungsrechtlichen Gremien sicherzustellen.

Verstöße gegen die Handlungsleitlinien werden individuell nach gültigen gesetzlichen, vertraglichen und gesellschaftsrechtlichen Bestimmungen geprüft und entsprechend geahndet.

Abweichungen von dieser Handlungsleitlinie, die das Sicherheitsniveau senken, sind nur temporär und nach Rücksprache mit den zuständigen Stellen (siehe Anhang **Fehler! Verweisquelle konnte nicht gefunden werden.**1) gestattet.

INTERNAL

Anhang

INTERNAL

A Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheitsregelung Nr. 03.01.09 Ausnahmegenehmigungen

A.1.2 Informationssicherheitsregelung Nr. 03.01.05 IAM

A.1.3 Informationssicherheitsregelung Nr. 03.01.02 Kryptographie

Die mitgeltenden Unterlagen sind auf der Konzern Informationssicherheit Website zu finden:

https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk

A.2 Anhänge

A.2.1 Feedbackformular

Das Feedbackformular für Verbesserungsvorschläge zu den Regelungen kann im Downloadbereich der Konzern Informationssicherheit Website https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk heruntergeladen werden.

Bitte senden Sie das ausgefüllte Formular an: VWAG R: WOB, IT Security Regulations <itsr@volkswagen.de>

A.3 Gültigkeit

Diese Informationssicherheitsregelung tritt zum Zeitpunkt der Veröffentlichung in Kraft. Aktualisierte Inhalte dieser Regelung sind innerhalb eines Übergangszeitraums von sechs Monaten umzusetzen.

Nächstes Überprüfungsdatum: September 2023

A.4 Abkürzungen und Definitionen

Abkürzung/Begriff	Erklärung
IT-Systementwickler	alle Personen, die an der Definition, dem Entwurf, der Entwicklung und der Implementierung eines IT-Systems beteiligt sind Dabei handelt es sich typischerweise um folgende Rollen: • IT-Systemplaner

INTERNAL

	• IT-Systemarchitekt • Softwarearchitekt • Systementwickler • Softwareentwickler • Anwendungsentwickler • Programmierer • Tester

A.5 Dokumenthistorie

Version	Name	Org.-Einheit	Datum	Kommentar
1.0	K-SIS/G1	K-SIS/G1	24. Mai 2004	Initiale Version
2.0	K-SIS/G1	K-SIS/G1	30. Januar 2013	Überarbeitung durch GISSC Prozess
3.0	K-SIS/G1	K-SIS/G1	11. November 2015	Überarbeitung durch GISSC Prozess Review: 2.4.2019
4.0	K-DS/G	K-DS/G	22. September 2022	Überarbeitung durch Regelungsteam und Freigabe in K-DS Leitungsrunde
4.1	K-DS/G	K-DS/G	03. November 2022	Ergänzung in Kapitel 5.4.1

INTERNAL

B Gesellschaftsspezifische Ausprägungen

B.1 Konzernweit geltend

In diesem Kapitel werden Ausprägungen aufgeführt, die für den gesamten Konzern gelten. Diese spezifischen Ausprägungen dürfen nicht verändert werden.

B.1.1 Die zuständige Stelle bei Abweichungen von diesen Handlungsleitlinien, die das Sicherheitsniveau senken, ist die jeweilige Informationssicherheitsorganisation der Marke oder Gesellschaft. Generell sind die Vorgaben der Regelung zu Ausnahmegenehmigungen (Siehe Anhang A.1.1) zu beachten.

Kontakt für die Volkswagen AG über My.Serve:
https://iserve.vw.vwg/vw/catalog_item_detail.do?sysparm_document_key=sc_cat_item,7f89128a50e61600ac0ade4eccc3502f

B.2 Gesellschaftsspezifische Ausprägungen

In diesem Kapitel werden spezifische Eigenschaften aufgeführt, die für eine Gesellschaft gelten. Diese Eigenschaften können je nach Gesellschaft angepasst werden. Zur Information werden Ausprägungen, die für die Marke Volkswagen gelten, kursiv angegeben.

B.2.1 Veröffentlicht im Group Wiki:
https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk+-+Politik

B.2.2 Für Marke Volkswagen dokumentiert in der ORL 18

B.2.3 Die verwendete Anwendungssoftware muss gemäß BV 2/80 „Unterrichtung und Beratung über Systemvorhaben der Informationsverarbeitung“ mit dem Betriebsrat beraten werden.

B.2.4 Zuständigkeiten: Informationssicherheitsorganisation des Konzerns, IT Projects, Architectures & Standards

B.2.5 Zuständigkeiten: Informationssicherheitsorganisation des Konzerns

B.2.6 Datenschutzmanager-Organisation (DSMO): Ansprechpartner für Ihren Fachbereich finden Sie im Datenschutz-Wiki. *Für weitere Informationen siehe auch: ORL 50 „Datenschutz und Datenschutz-Governance“*

INTERNAL

VOLKSWAGEN

AKTIENGESELLSCHAFT

Informationssicherheit

Handlungsleitlinien
- Handlungsleitlinie für Dritte -

Herausgeber

Group Information Security

Regelung Nr.

02.06

Status

veröffentlicht

Version

5.0

Klassifikation

Intern

Datum

22.09.2022

Geltungsbereich

Diese Anweisungen gelten für alle Dritte, die schutzbedürftige Informationen für den Volkswagen Konzern entsprechend vertraglicher Vereinbarungen verarbeiten.

©Volkswagen AG, Intern, KSU: 2.1

Inhaltsverzeichnis

INTERNAL

I Zweck und Definitionen

In dieser Informationssicherheits-Handlungsleitlinie werden die organisatorischen Vorgaben und die Regeln für die Informationssicherheit definiert, die von Dritten beim Umgang mit Informationen des Volkswagen Konzerns zu befolgen sind. Die Begriffe Informationen und Daten in diesem Dokument beziehen sich ausschließlich auf Informationen und Daten des Volkswagen Konzerns.

Dritte sind definiert als Vertragspartner, die Dienstleistungen für den Volkswagen Konzern auf Basis vertraglicher Beziehungen erbringen. Tochtergesellschaften und Marken des Volkswagen Konzerns, sowie Gesellschaften, an denen der Volkswagen Konzern Mehrheitsbeteiligungen hält, sind von dieser Definition ausgeschlossen.

I.I Dokumentenstruktur und Zielgruppe

Diese Handlungsleitlinie richtet sich an die Geschäftsleitung der Dritten. Die Geschäftsleitung der Dritten hat sicherzustellen, dass deren Beschäftige sowie deren Erfüllungs-/Verrichtungsgehilfen auf diese Informationssicherheits-Handlungsleitlinie verpflichtet werden.

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

Kapitel	**Zielgruppe**
1	Alle Dritte
2	Dritte, die in der Volkswagen Konzern Infrastruktur arbeiten.
3	Dritte, die Volkswagen Informationen außerhalb der Volkswagen Konzern Infrastruktur im Zugriff haben.
4	Dritte, die Volkswagen Informationen außerhalb der Volkswagen Infrastruktur bereitstellen.

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

INTERNAL

1 Allgemeine Anforderungen an alle Dritte

1.1 Klassifikation von Informationen

Die Klassifikation hat den Zweck, Informationen abhängig von deren Schutzbedarf in Stufen einzuordnen. Abhängig von der Einordnung sind unterschiedliche Schutzmaßnahmen erforderlich.

Alle Volkswagen Konzern Informationen sind nach der Vertraulichkeit zu klassifizieren. Vertraulichkeitseinstufungen können mit einem Ablaufdatum versehen werden.

Werden vom Dritten Dokumente oder Informationen für den Volkswagen Konzern erstellt, ist die Klasssifikation nach Vertraulichkeit beim Ansprechpartner des Volkswagen Konzerns zu erfragen und entsprechend zu kennzeichnen.

1.2 Umgang mit klassifizierten Informationen

Informationen dürfen nur einer berechtigten Gruppe von Personen zum Zwecke der vereinbarten Tätigkeiten und unter Einhaltung der entsprechenden Regelungen zugänglich gemacht werden. Dabei ist das Need-to-know-Prinzip zu befolgen.

Um vertrauliche oder geheime Informationen zu schützen, sind die entsprechenden IT-Geräte so einzurichten, dass der Zugriff durch Unberechtigte verhindert und das Risiko einer Einsichtnahme durch unbefugte Dritte minimiert wird.

Informationen müssen während des gesamten Lebenszyklus entsprechend ihrer aktuellen Vertraulichkeitseinstufung vor einem Zugriff durch Unberechtigte geschützt werden. Es gelten folgende Regelungen:

Klassifikation	Anforderungen
Öffentlich	• Kennzeichnung: keine/optional (z.B. Vermerk im Impressum) • Vervielfältigung und Verteilung: keine Einschränkungen • Speicherung: keine Einschränkungen • Entsorgung: keine Einschränkungen
Intern	• Kennzeichnung: Angabe der Vertraulichkeitsstufe „Intern“ oder „Internal“ auf der ersten Seite des Dokuments • Vervielfältigung und Verteilung: nur an berechtigte Beschäftigte des Konzerns und berechtigte Dritte im Rahmen der Tätigkeit bzw. des Anwendungsbereichs • Speicherung: Schutz vor unbefugtem Zugriff • Entsorgung: ordnungsgemäße Entsorgung

INTERNAL

Vertraulich	• Kennzeichnung: Angabe der Vertraulichkeitsstufe „Vertraulich“ oder „Confidential“ auf jeder Seite des Dokuments • Vervielfältigung und Verteilung: nur an eine beschränkte Gruppe von berechtigten Beschäftigten des Konzerns und berechtigte Dritte im Rahmen der Tätigkeit sowie des Anwendungsbereichs. Die Person, die die Informationen verteilt, ist für angemessene Verteilwege verantwortlich, um die Informationen und Daten vor unbefugtem Zugriff und/oder unbefugtem Mithören zu schützen (z.B. mithilfe von Verschlüsselung). • Speicherung: Zugriff nur für eine beschränkte Gruppe von berechtigten Beschäftigten des Konzerns und berechtigte Dritte im Rahmen der Tätigkeit sowie des Anwendungsbereichs (z.B. durch geschlossene Nutzergruppen). Es sind geeignete Speichermedien zu verwenden. • Entsorgung: ordnungsgemäße Entsorgung • Transport/Versand: Vertrauliche Dokumente und Speichermedien müssen in verschlossenen, neutralen Umschlägen versendet werden. Bei Bedarf kann der Zusatz “persönlich” hinzugefügt werden. Dies bedeutet, dass der Umschlag nur von der adressierten Person geöffnet werden darf. • Drucken: Ausdruck nur unter Beaufsichtigung der druckenden Person

INTERNAL

Geheim	• Kennzeichnung: Angabe der Vertraulichkeitsstufe „Geheim“ oder „Secret“ auf jeder Seite des Dokuments • Darüber hinaus sind alle Seiten mit „Seite x von y“ zu kennzeichnen. • Vervielfältigung und Verteilung: nur an eine äußerst begrenzte Gruppe (z.B. namentliche Liste) von berechtigten Beschäftigten des Konzerns und berechtigte Dritte im Rahmen der Tätigkeit bzw. des Anwendungsbereichs und nach vorheriger Genehmigung durch den Informationseigentümer. Alle Daten sind zu verschlüsseln. Je nach Anwendungsfall sind weitere technische bzw. organisatorische Schutzmaßnahmen zu verwenden (z.B. Verbot von Weiterleiten und Ausdrucken, Wasserzeichen). Zur Kommunikation sind geeignete Medien zu verwenden, die ein Mithören verhindern (z.B. verschlüsselte Videokonferenzen). • Speicherung: Zugriff nur für eine äußerst begrenzte Gruppe (z.B. namentliche Liste) von berechtigten Beschäftigten des Konzerns und berechtigte Dritte im Rahmen der Tätigkeit sowie des Anwendungsbereichs (z.B. durch geschlossene Nutzergruppen). Alle Daten sind zu verschlüsseln. • Entsorgung: ordnungsgemäße Entsorgung • Transport: Geheime Dokumente und Speichermedien müssen in neutralen, verschlossenen Außenumschlägen (ohne Zusätze wie “persönlich, geheim, etc.“) versendet werden. In diesen ist ein zweiter innerer Umschlag zu platzieren, welcher mit der Klassifikation “geheim” gekennzeichnet ist. Geheime Unterlagen bzw. elektronische Speichermedien dürfen von dem Gelände des Unternehmens nur von Beschäftigten mitgenommen werden, die hierzu von ihrer jeweiligen Führungskraft schriftlich ermächtigt sind. • Drucken: Ausdruck nur unter Beaufsichtigung der druckenden Person

Die Vorgaben zum Umgang mit Informationen (Kennzeichnung, Vervielfältigung, Verteilung, Speicherung und Entsorgung) gelten ebenfalls für IT-Systeme (z.B. Datenbanken und Sicherungsmedien).

Für Übersetzungen von Dokumenten, die Informationen des Volkswagen Konzerns enthalten, dürfen insbesondere keine öffentlichen Internet-Übersetzungsdienste verwendet werden.

1.3 Weitere Vorgaben

- Informationssicherheitsereignisse (z. B. auftretende Störungen, Verstöße gegen das Informationssicherheits-Regelwerk), welche Informationen oder IT-Systeme des Auftraggebers betreffen, sind unverzüglich der zuständigen Stelle zu melden (siehe Anhang A.3.1).
- Wird ein Angriff mithilfe von Schadsoftware vermutet oder entdeckt, dürfen die betroffenen IT-Geräte und Speichermedien nicht mehr zur Verarbeitung von Volkswagen Konzern Informationen verwendet werden.
- Vermutete Verwundbarkeiten und Schwachstellen von IT-Systemen des Auftraggebers sind unverzüglich der zuständigen Stelle zu melden (siehe Anhang A.3.1).
- Beim Verdacht auf Verlust von vertraulichen oder geheimen Informationen des Auftraggebers, muss dies sofort an den Volkswagen Konzernansprechpartner gemeldet werden.
- Die Weitergabe von Daten oder Informationen an weitere Dritte ist nur mit schriftlicher Freigabe durch den Informationseigentümer zulässig.
- Dokumente und Speichermedien mit schützenswerten Informationen des Volkwagen Konzerns müssen vor Verlust, Zerstörung und Verwechslung sowie vor unbefugtem Zugriff geschützt werden. Sobald die Daten auf dem Speichermedium nicht mehr erforderlich sind, müssen die Daten dort sicher gelöscht werden. Nicht mehr benötigte Speichermedien sind auf sichere Weise zu entsorgen.
- Bei allen Gesprächen und Datenübertragungen (einschließlich Telefonaten, Video- und Webkonferenzen), die vertrauliche oder geheime Informationen des Volkswagen Konzerns betreffen oder enthalten, ist sicherzustellen, dass diese nicht unberechtigt mitgehört oder mitgelesen werden können.
- Vertrauliche oder geheime Informationen dürfen nicht als Bestandteil von Dateinamen oder in E-Mail-Betreffzeilen verwendet werden.
- Die fehlerfreie Verarbeitung von Informationen und der Schutz vor unbefugten Änderungen müssen sichergestellt werden.

2 Zusätzliche Anforderungen an Dritte, die in der Volkswagen Konzern Infrastruktur arbeiten

2.1 Definition

Ein Dritter arbeitet in der Volkswagen Konzern Infrastruktur, wenn:

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

Dies gilt unabhängig davon, ob sich der Dritte auf dem Gelände einer Konzerngesellschaft befindet.

INTERNAL

2.2 Anforderungen

- Regelungen der jeweiligen Konzerngesellschaft bezüglich des Mitbringens von nicht der jeweiligen Konzerngesellschaft gehörenden IT-Geräten auf das Firmengelände oder in Sicherheitsbereiche müssen eingehalten werden.
- Von der jeweiligen Konzerngesellschaft zur Verfügung gestellten IT-Geräte sind sachgemäß zu behandeln und vor Verlust oder unbefugter Veränderung zu schützen.
- Die Vorschriften des Herstellers zum Schutz der IT-Geräte sind einzuhalten.
- Die durch die jeweilige Konzerngesellschaft zur Verfügung gestellten IT-Geräte dürfen nur nach erfolgter Genehmigung vom Werksgelände der Konzerngesellschaft mitgenommen werden.
- Die Bereitstellung oder Installation von Hardware und Software darf nur über den für sie zuständigen Fachbereich der Konzerngesellschaft durchgeführt oder initiiert werden.
- Bezüglich der Nutzung der von der jeweiligen Konzerngesellschaft zur Verfügung gestellten Hardware und Software gelten die Regelungen der jeweiligen Konzerngesellschaft
- Es ist nur die Nutzung von der jeweiligen Konzerngesellschaft zur Verfügung gestellter Hardware, Software und Speichermedien gestattet. Ausnahmen können im Einzelfall mit dem zuständigen Volkswagen Konzernansprechpartner besprochen werden. Ausnahmen zum Zwecke des Zugriffs auf das Konzern-Netzwerk, eines Fernzugriffs oder für mobiles Arbeiten werden in Kapitel 2.4 beschrieben.
- Das Öffnen des von der jeweiligen Konzerngesellschaft zur Verfügung gestellten IT-Gerätes und das Vornehmen von Änderungen an der Hardware (z.B. Ein-/Ausbau von Komponenten) und das Ändern von Sicherheitseinstellungen (z.B. im Webbrowser) ist ausschließlich den zuständigen Stellen des Volkswagen Konzerns gestattet. Das Entfernen von Nutzungsbeschränkungen (z.B. „Jailbreaking“ oder „Betriebssystem-Rooting“) ist nicht gestattet.
- Der Einsatz oder das nachträgliche Verändern von Programmen der jeweiligen Konzerngesellschaft ist nur zulässig, wenn dies von dem zuständigen Volkswagen Konzernansprechpartner genehmigt wurde.
- Auf den von der jeweiligen Konzerngesellschaft zur Verfügung gestellten IT-Geräten dürfen keine Daten von weiteren Kunden, die nicht zum Konzern gehören, verarbeitet werden.
- Jeder Dritte ist dafür verantwortlich, dass Informationen, Programme und IT-Geräte nur für im Rahmen der jeweiligen Aufgabenstellung ordnungsgemäß eingesetzt und genutzt werden.
- Das Versenden von nicht dienstlichen Informationen ist nicht gestattet.
- Der Einsatz privater Software und Daten auf den von der jeweiligen Konzerngesellschaft zur Verfügung gestellten IT-Geräten ist nicht gestattet.
- Das Verwenden von IT-Geräten oder Daten der jeweiligen Konzerngesellschaft durch Beschäftigte des Dienstleisters erfordert die ausdrückliche Zustimmung der jeweiligen Konzerngesellschaft. Die jeweilige Konzerngesellschaft ist ermächtigt, jederzeit den Zugriff oder die Benutzung zu untersagen (z.B. bei Missbrauch).
- Nicht mehr benötigte Hardware (z.B. Laptop, Smartcards, SecurID-Token, USB-Sticks, USB-Platten) und Software ist unverzüglich der jeweiligen Konzerngesellschaft zurückzugeben, spätestens jedoch zu Vertragsende.
- Reparaturen von IT-Geräten, die von der Konzerngesellschaft zur Verfügung gestellt worden sind, dürfen nur durch die Konzerngesellschaft veranlasst werden.

INTERNAL

- Der Verlust von durch die Konzerngesellschaft zur Verfügung gestellter Hardware ist durch den entsprechenden Nutzenden unverzüglich dem zuständigen Volkswagen Konzernansprechpartner zu melden.
- Die Speicherung nicht öffentlich klassifizierter unternehmenseigener Daten ist nur auf genehmigten Speichermedien zulässig (z.B. freigegebene Datei- oder Cloud-Speicherdienste).
- Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten (z. B. Name, Telefonnummer, Mailadresse, Geburtsdatum) ist nur zulässig, sofern
    - eine Einwilligung des Betroffenen (Einzelnen) vorliegt oder
    - dafür eine Rechtsgrundlage vorhanden ist.
- Personenbezogene Daten, die in einer Konzerngesellschaft gespeichert sind, dürfen nur im Rahmen der dienstlichen Tätigkeiten verarbeitet und genutzt werden. Eine Weitergabe dieser Daten an unbefugte Dritte ist nicht zulässig.
- IT-Geräte und Datenträger, auf denen personenbezogene, vertrauliche oder geheime Daten gespeichert sind, dürfen Liegenschaften des Volkswagen Konzerns grundsätzlich nur verschlüsselt verlassen.

2.3 Umgang mit User Accounts

Folgende Vorgaben beim Umgang mit User Accounts und Passwörtern sind durch alle Nutzenden zu befolgen:

- Die Verwendung eines User Accounts einer anderen Person ist nicht gestattet.
- Nicht mehr benötigte User Accounts oder Zugriffsberechtigungen sind umgehend den zuständigen Volkswagen Konzernansprechpartnern zu melden, damit diese gelöscht bzw. gesperrt werden können.
- Die Weitergabe von Authentifizierungsmitteln (z.B. Smartcards, Authenticator Apps und Token) ist nicht gestattet.
- Nicht mehr benötigte Authentifizierungsmittel sind dem zuständigen Volkswagen Konzernansprechpartner unverzüglich zurückzugeben.
- Passwörter und PINs eines User Accounts, der zur persönlichen Verwendung bestimmt ist, dürfen nicht weitergegeben oder geteilt werden.
- Sobald der Verdacht der Kompromittierung oder des Bekanntwerdens eines Passworts oder einer PIN besteht, ist dieses bzw. diese unverzüglich zu ändern.
- Passwörter oder PINs sind mindestens vertraulich klassifiziert.

Für die Festlegung eines Passwortes oder einer PIN müssen folgende Anforderungen erfüllt werden:

- In jedem IT-System, das ein eigenes Passwort verwendet, ist ein separates Passwort zu verwenden.
- Insbesondere ist es nicht gestattet, ein dienstlich genutztes Passwort für private Zwecke zu verwenden.
- Triviale Passwörter (z.B. „Test12345678“) oder Passwörter mit persönlichem Bezug (z.B. Namen, Geburtsdatum) sind nicht zulässig.

  Hinweis: Für ein sicheres Passwort können Sie Eselsbrücken oder Abkürzungen sowie Verfälschungen verwenden (Beispiel: „Jeden Tag gehe ich ins Bad und wasche mich gründlich mit einem Waschlappen!“

wird zum Passwort „JTg11B&wmgmeW!“). Das hier aufgeführte Beispiel darf nicht als tatsächliches Passwort verwendet werden.

2.4 Nutzung von Netzwerkdiensten

Durch vom Volkswagen Konzernunternehmen bereitgestellte netzwerkfähige Geräte dürfen nur mit unternehmensfremden Netzwerken (z. B. Hot Spot, privates WLAN, Mobilfunk) verbunden werden, wenn dieses Vorgehen für das jeweilige Gerät vom Konzernunternehmen explizit freigegeben wurde.

Die Verbindung von netzwerkfähigen Geräten mit dem Konzernnetzwerk ist nur zulässig, wenn dieses Vorgehen für das jeweilige Gerät vom Konzernunternehmen explizit freigegeben wurde.

2.5 Zusätzliche Anforderungen bei mobiler Arbeit

Der Anwender hat eigenverantwortlich darauf zu achten, dass die betroffenen Regelungen zur Daten- und Informationssicherheit sowie zum Datenschutz während mobiler Arbeit uneingeschränkt eingehalten werden. Arbeitsunterlagen, Daten und Informationen dürfen weder an öffentlichen Orten noch in Privaträumen für Dritte sichtbar und zugänglich sein.

Der Anschluss von Hardware (z.B. Maus, Tastatur, USB-Sticks) an der von der Volkswagen Konzerngesellschaft gestellten Hardware ist nur zulässig, wenn diese von der Volkswagen Konzerngesellschaft gestellt worden ist.

Bildausgabegeräte (z.B. Monitore, Projektoren), die nicht von der Volkswagen Konzerngesellschaft gestellt worden sind, können genutzt werden, wenn der Anschluss kabelgebunden erfolgt und keine Funkübertragung genutzt wird.

Nicht von der Volkswagen Konzerngesellschaft bereitgestellte Headsets und Freisprechanlagen dürfen nur über den Kopfhörer-/Mikrofoneingang, jedoch nicht über USB, angeschlossen werden.

Von der jeweiligen Konzerngesellschaft zur Verfügung gestellte IT-Geräte sind physisch gegen Diebstahl und Missbrauch zu schützen:

- Wird ein IT-Gerät unbeaufsichtigt in einem Kraftfahrzeug hinterlassen, muss dies so geschehen, dass es von außen nicht sichtbar ist.
- Auf Flug- und Bahnreisen sind IT-Geräte im Handgepäck zu transportieren.
- Wenn ein IT-Gerät längere Zeit unbeaufsichtigt ist, muss es ausgeschaltet werden.

INTERNAL

3 Zusätzliche Anforderungen an Dritte, die Informationen des Volkswagen Konzerns außerhalb der Volkswagen Konzern Infrastruktur im Zugriff haben

3.1 Definition

Ein Dritter hat dann Informationen des Volkswagen Konzerns außerhalb der Volkswagen Konzern Infrastruktur im Zugriff, wenn dieser Volkswagen Konzern Informationen in seiner eigenen IT-Infrastruktur verarbeitet.

3.2 Anforderungen

- Es gelten die Regularien zur Informationssicherheit des Dritten, soweit nichts anderes vertraglich vereinbart wurde.

4 Zusätzliche Anforderungen an Dritte, die Informationen des Volkswagen Konzerns außerhalb der Volkswagen Konzern Infrastruktur bereitstellen

4.1 Definition

Ein Dritter stellt dann Informationen des Volkswagen Konzerns außerhalb der Volkswagen Konzern Infrastruktur bereit, wenn dieser Volkswagen Konzern Informationen in seiner eigenen IT-Infrastruktur für den Volkswagen Konzern oder weitere Dritte im Auftrag des Volkswagen Konzerns bereitstellt.

4.2 Anforderungen

- Die Vorgaben der Informationssicherheitshandlungsleitlinie Nr. 02.03 für Systembetreiber und Administratoren sind einzuhalten (siehe A.3.2).

INTERNAL

II Zuständigkeiten

Verstöße gegen die Handlungsleitlinien werden individuell nach gültigen gesetzlichen und vertraglichen Bestimmungen geprüft und entsprechend geahndet.

Abweichungen von diesen Handlungsleitlinien, die das Sicherheitsniveau beeinträchtigen, sind nur zeitlich begrenzt und nach Rücksprache mit dem Ansprechpartner der Volkswagen Konzerngesellschaft gestattet.

INTERNAL

A Allgemeines

A.1 Gültigkeit

Diese Informations-Sicherheitsregelung tritt zum Zeitpunkt der Veröffentlichung in Kraft. Aktualisierte Inhalte dieser Regelung sind innerhalb eines Übergangszeitraums von sechs Monaten umzusetzen.

Nächstes Überprüfungsdatum: September 2023

A.2 Dokumenthistorie

Version	Name	Abteilung	Datum	Kommentar
1.0	K-SIS/G1	K-SIS/G1	25. Mai 2004	Initiale Version
2.0	K-SIS/G1	K-SIS/G1	30. Januar 2004	Überarbeitet durch GISSC Prozess
3.0	K-SIS/G1	K-SIS/G1	11. November 2015	Überarbeitet durch GISSC Prozess
4.0	K-FIS	K-FIS	7. August 2018 (review 2.4.19)	Anpassung bzgl. VDA ISA
5.0	K-DS/G	K-DS/G	22. September 2022	Überarbeitung durch Regelungsteam und Freigabe durch K-DS Leitungsrunde

A.3 Gesellschaftsspezifische Ausprägungen

A.3.1 CERT VW - über Enterprise Help Desk (EHD, Tel. +49 531 9 33000, <EHD@volkswagen.de>)

A.3.2 Anforderungen Informationssicherheit und IT-Sicherheit (volkswagen.de)

INTERNAL

VOLKSWAGEN

AKTIENGESELLSCHAFT

Informationssicherheit

Übergreifende Regelungen und Prozesse
- Dienstleistung durch Dritte -

Herausgeber

Informationssicherheit Konzern

Regelung Nr.

03.01.16

Status

Veröffentlicht

Version

3.0

Klassifikation

Intern

Erstellungsdatum

27.09.2022

Veröffentlichungsdatum

06.10.2022

Geltungsbereich

Diese Regelung gilt für die Volkswagen AG (Organisationseinheiten (OE) auf Konzernebene und auf Markenebene der Marke Volkswagen Pkw, der Marke Volkswagen Nutzfahrzeuge sowie der Volkswagen Group Components).

Hinsichtlich der Umsetzung dieser Regelung bei den anderen Volkswagen Konzerngesellschaften gilt die ORL 1 "Organisatorische Regelungen der Volkswagen AG".

©Volkswagen AG, Intern, KSU: 2.1

INTERNAL

Inhalt

INTERNAL

INTERNAL

I Zweck

Im Volkswagen Konzern werden Dritte für Umfänge beauftragt, die ganz oder teilweise IT Leistungen beinhalten, wie Outtasking- (z. B. externe Beratung) oder Outsourcing-Vorhaben (z. B. externes Hosting). Um Informationen umfassend schützen zu können, müssen externe Dienstleister Sicherheitsregelungen und gesetzliche Anforderungen einhalten. Die vorliegende Regelung legt spezifische Anforderungen an die Informationssicherheit und an Prozesse für alle Phasen von Outtasking- und Outsourcing-Vorhaben fest.

1 Dienstleistung durch Dritte

1.1 Ziel

Die vorliegende Regelung legt Sicherheitsanforderungen fest, die bei der Arbeit mit externen Dienstleistern (Dritten) implementiert werden müssen, um zu gewährleisten, dass das Informationssicherheitsniveau innerhalb des Konzerns nicht gesenkt wird. Die Anforderungen dieser Regelung gelten für alle Arten der Dienstleistungserbringung und alle Auftragnehmer.

Bevor der Auftrag für Dienstleistungen an einen externen Dienstleister vergeben wird, muss ein Prozess ein geeignetes Maß an Sicherheit und die Einhaltung interner Regelungen sicherstellen.

Es muss gewährleistet werden, dass die Interessen der Informationssicherheit, des Datenschutzes und der Konzernsicherheit adäquat wahrgenommen werden. Das Gewährleisten der Interessen des Datenschutzes und der Group Security ist durch entsprechende Regelungen dieser Stakeholder unabhängig von dieser Regelung sicherzustellen.

1.2 Gemeinsame Anforderungen bei Outtasking und Outsourcing

1.2.1 Allgemeine Anforderungen

- Die für die Beauftragung von Leistungen im Sinne dieser Regelung verantwortliche Einheit muss sicherstellen, dass Prozesse für die Einhaltung der Anforderungen in dieser Regelung mit der Informationssicherheit abgestimmt, festgelegt und implementiert sind.
- Folgende Anforderungen müssen in diesen Prozessen berücksichtigt werden.
    - Es muss ein Verfahren zur Beauftragung eines Outtasking- und Outsourcing-Vorhabens (im Folgenden allgemein "Vorhaben" genannt[1]) mit Rollen und Verantwortlichkeiten definiert, dokumentiert und etabliert werden.
    - Für sicherheitskritische Vorhaben (Vorhaben mit Zugang zu vertraulichen, geheimen Daten oder Daten mit sehr hohen Anforderungen an die Verfügbarkeit oder Integrität) muss vom Dienstleister ein Verfahren definiert, dokumentiert und etabliert werden, mit dem die Vertrauenswürdigkeit der Mitarbeiter, die der Dienstleister einsetzen wird, durch den Auftraggeber geprüft werden kann (z. B. Zusicherung polizeilicher Führungszeugnisse oder Zusicherung der Vertrauenswürdigkeit durch den Dienstleisters im Rahmen des Vertrags).
    - Die Eigentümer der Daten müssen in die Entscheidung zu Outtasking-/Outsourcing-Vorhaben involviert werden.

[1]Ein Vorhaben endet, wenn der Vertrag ausläuft, gekündigt wird und alle Migrationsschritte abgeschlossen sind.

INTERNAL

- Es muss regelmäßig überprüft werden, ob die für das Vorhaben relevanten Anforderungen an die Informationssicherheit[2] von den beauftragten Dritten eingehalten werden. Hierfür ist ein Verfahren[3] zu entwickeln.
- Organisatorische und technische Änderungen bzgl. der Informationssicherheit innerhalb der Konzerngesellschaft, die für Dritte von Bedeutung sind (z. B. Versionsänderungen von Systemen, Änderungen von Regelungen) sind den davon betroffenen Dritten mitzuteilen.
- Dritte müssen aufgefordert werden, sämtliche Änderungen mit Relevanz bzgl. der Informationssicherheit für die beauftragte Dienstleistung an den Auftraggeber zu melden.

- Wenn personenbezogene Daten von Dritten verarbeitet werden, hat die verantwortliche Konzerngesellschaft dafür Sorge zu tragen, dass lokal geltende gesetzliche und unternehmensspezifische Anforderungen eingehalten werden.
- Der/Die Dritte muss sicherstellen, dass die erforderlichen Maßnahmen zur technischen und organisatorischen Sicherheit für die Verarbeitung personenbezogener Daten unter Einhaltung der entsprechenden Regelungen implementiert werden[4].
- Zusätzliche Anforderungen[5] der Abteilung Group Security müssen eingehalten werden.

1.2.2 Management externer Dienstleister im Rahmen des Projektmanagements

- Für jedes Outtasking- und Outsourcing-Vorhaben muss die Konzerngesellschaft Verantwortliche[6] bestimmen, die für die Einhaltung der Anforderungen in den Phasen "Planung und Konzeption", "Detailplanung", "Migration", "Betrieb" sowie "Fertigstellung" zuständig sind.
- Jede Anforderung an die Informationssicherheit, die der Dienstleister im Rahmen des Vorhabens zu erfüllen hat, muss definiert und dokumentiert werden (z. B. relevante Sicherheitsregelungen und vorhabenspezifische Auflagen).
- Jeder Unterauftragnehmer mit Relevanz für das Vorhaben muss von der entsprechenden Konzerngesellschaft und dem Eigentümer der Daten auf Verlangen gemeldet werden.
- Die dokumentierten Anforderungen an die Informationssicherheit gelten auch für Unterauftragnehmer des Dienstleisters.
- Es sollte eine Konzernmethodik gewählt werden, die ein standardisiertes Management von Dienstleistern sicherstellt[7].

1.2.3 Auswahl von Dienstleistern

- Es dürfen nur Dienstleister gewählt werden, die über den gesamten Lebenszyklus des Vertrags die Erfüllung der Anforderungen an die Informationssicherheit gewährleisten können.
- Es muss ein standardisierter Prozess für die Auswahl von Dienstleistern in Übereinstimmung mit den Sicherheitsregelungen implementiert werden[8].
- Wenn personenbezogene Daten verarbeitet werden, dürfen nur Dienstleister ausgewählt werden, die die Anforderungen des Datenschutzes erfüllen.

[2] Siehe Kapitel 1.2.2
[3] Z. B. im Rahmen des Projektmanagementprozesses
[4] Siehe Anhang B.2.1.2
[5] Siehe Anhang A.1.7
[6] Z. B. Projektmanager
[7] Z. B. Leistungsbaukasten
[8] Siehe Anhang B.2.1.3

INTERNAL

- Vor Vertragsabschluss sicherheitskritischer Vorhaben muss mittels des definierten Verfahrens[9] die Vertrauenswürdigkeit der Mitarbeiter sichergestellt werden, die der Dienstleister einsetzen wird.
- Für externes Hosting gelten zusätzliche Anforderungen[10].

1.2.4 Vertragsabschluss

Verträge mit Dienstleistern müssen mindestens Folgendes enthalten:

- Alle für den Dienstleister relevanten Anforderungen an die Informationssicherheit des Vorhabens
- Implementierte Sicherheitsmaßnahmen der Dienstleister mit Relevanz für den Vertrag[11]
- Anforderungen an die Art und Weise des Informationsaustauschs zwischen den Vertragspartnern
- Eigentums- und Nutzungsrechte der Informationen, die im Rahmen des Vorhabens
  - dem Dienstleister zur Verfügung gestellt werden
  - vom Dienstleister erstellt werden oder
  - an den Dienstleister ausgelagert werden
- Mitwirkungs- und Sorgfaltspflichten des Dienstleisters, die mindestens folgende Aspekte umfassen müssen:
  - Geheimhaltung (NDA[12])
  - Einhaltung der für das Vorhaben geltenden Gesetze (z. B. Bundesdatenschutzgesetz)
  - Einhaltung aller relevanten Anforderungen der Unternehmensregelungen zur IT-Sicherheit
  - Zusicherung der Vertrauenswürdigkeit der externen Mitarbeiter des Vorhabens
  - Zusicherung, dass die externen Mitarbeiter des Vorhabens ausreichende Schulungen zu den für ihre Aufgaben relevanten Informationssicherheitsrisiken erhalten haben
- Anforderung, dass der Dienstleister regelmäßig Berichte über Vorfälle, Änderungen, Risiken und Dienstleistungsunterbrechungen an die genannte verantwortliche Person der Konzerngesellschaft übermitteln muss. Zusätzlich muss der Dienstleister diese Person direkt über größere Vorfälle und Sicherheitsschwachstellen informieren (je nach Kritikalität des Vorfalls/der Schwachstelle).
- Pflichten bei regulärer und außerordentlicher Vertragsbeendigung, die mindestens folgende Aspekte umfassen müssen:
  - Vollständige Übergabe aller Ergebnisse, Informationen und Tools, die für die Fortführung des Vorhabens benötigt werden (z. B. Dokumentationen oder Verfahrensbeschreibungen) oder für den Volkswagen Konzern innerhalb einer definierten Periode relevant sind
  - Rückgabe von Hard- und Software, die Eigentum des Volkswagen Konzerns sind
  - Sichere Löschung von Passwörtern und Benutzerkennungen, die den Zugang zur IT des Volkswagen Konzerns ermöglichen, aus Systemen des externen Dienstleisters
  - Rückgabe von Eigentum (insbesondere Token, Zutrittskarten, Schlüssel, ...)
  - Sicheres Löschen aller Datenbestände des Vorhabens beim Dienstleister[13] nach Bestätigung durch den Auftraggeber

[9] Siehe Kapitel 1.2.1 1.2.1
[10] Siehe Kapitel 1.4
[11] Gemäß Anhang A.1.7 ORL13
[12] Vertraulichkeitsvereinbarung
[13] Siehe Anhang A.1.2 Regelung Nr. 02.02 IS Handlingsleitlinie für Beschäftigte

INTERNAL

- Pflichten bei der Beauftragung von Unterauftragnehmern, die mindestens folgende Aspekte umfassen müssen:
  - Einholen der Zustimmung für den Einsatz genannter Unterauftragnehmer für definierte Aufgaben von der entsprechenden Konzerngesellschaft, mindestens jedoch Meldung dieser Unterauftragnehmer auf Verlangen
  - Verpflichtung des Unterauftragnehmers auf die Erfüllung aller Anforderungen, die auch der direkte Auftragnehmer zu erfüllen hat
  - Regelungen bezüglich Haftung und Vertragsverletzungen
- Rechte und Erlaubnis zur Durchführung von Audits beim Dienstleister. Der Dienstleister muss auch die Erlaubnis für Audits beim Unterauftragnehmer sicherstellen.
- Eigentumsrückgabe bei Vertragsende
- Zusätzliche Anforderungen der Abteilung Group Security müssen eingehalten werden[14].
- Geltende unternehmensspezifische Anforderungen müssen eingehalten werden.
- Für externes Hosting gelten zusätzliche Anforderungen[15].

1.2.5 Betrieb während der Laufzeit des Vertrags

- Während des Betriebs müssen alle vertraglichen Anforderungen[16] eingehalten werden.
- Beide Parteien müssen eine verantwortliche Kontaktperson für das Vorhaben benennen.
- Der Verantwortliche der Konzerngesellschaft agiert als Kontaktperson zwischen dem Vertragspartner und dem lokal Verantwortlichen für Informationssicherheit.
- Der Verantwortliche der Konzerngesellschaft muss prüfen, dass der Dienstleister sicherstellt, dass seine Mitarbeiter die relevanten Anforderungen an die Informationssicherheit sowie die vertraglichen Anforderungen kennen und einhalten.

1.2.6 Beendigung des Vorhabens

- Bei Abschluss des Vorhabens müssen die Anforderungen aus dem Vertrag[17] in Bezug auf die Beendigung des Vorhabens erfüllt werden. Des Weiteren müssen alle Zutritts-, Zugangs- und Zugriffsrechte unverzüglich entzogen werden[18], sofern die gesetzlich geforderte Nachvollziehbarkeit dadurch nicht eingeschränkt wird.

1.3 Zusätzliche Anforderungen für das Outsourcing

1.3.1 Planung und Konzeption

- Die für die Informationssicherheit (oder IT-Sicherheit) verantwortliche Einheit[19] muss bereits bei der Planung und Konzeption eines Outsourcing-Vorhabens einbezogen werden. Dies gilt auch für weitere relevante Abteilungen/Rollen (z. B. Datenschutzbeauftragte, Konzernsicherheit).
- Es muss eine Risikoanalyse[20] für das Outsourcing-Vorhaben durchgeführt werden. In die Risikoanalyse müssen sämtliche Informationen, Services und IT-Komponenten einbezogen werden,

[14] Siehe Anhang A.1.7 ORL 13
[15] Siehe Kapitel 1.4
[16] Siehe Kapitel 1.2.4
[17] Siehe Kapitel 1.2.4
[18] Siehe Anhang A.1.3 Informationssicherheit Regelung Nr. 03.01.05 Identity und Access Management
[19] Siehe Anhang B.2.1.1.
[20] Siehe Anhang A.1.4 Informationssicherheit - Regelung Nr. 03.01.15 Risikomanagement in der Informationssicherheit

INTERNAL

die von dem Outsourcing-Vorhaben unmittelbar betroffen sind. Der Outsourcing-Gegenstand muss exakt definiert werden.

1.3.2 Vertragsabschluss

- Die vertraglichen Vereinbarungen müssen Testkriterien enthalten, um die Implementierung der Anforderungen an die Informationssicherheit zu prüfen.
- Dem Unternehmen, das für den Outsourcing-Gegenstand verantwortlich ist, muss es erlaubt sein, regelmäßige Prüfungen zur Einhaltung der Regelungen zur Informationssicherheit im Rahmen des Outsourcing-Vorhabens durchzuführen.
- Diese Prüfungen können an einen Drittanbieter ausgelagert werden.

1.3.3 Detailplanung

- Der Dienstleister muss einen Ansprechpartner und Vertreter für alle Aspekte der Informationssicherheit und des Datenschutzes festlegen.
- Sowohl die verantwortliche Gesellschaft als auch der Dienstleister müssen auf der Grundlage der ermittelten Sicherheitsanforderungen ein Sicherheitskonzept für das Outsourcing-Vorhaben erstellen. In diesem Sicherheitskonzept müssen mindestens folgende Aspekte berücksichtigt werden:
  - Schnittstellen zwischen Gesellschaft und Dienstleistern
  - Maßnahmen für alle folgenden Phasen des Outsourcing-Vorhabens, die zur Erfüllung der Sicherheitsanforderungen notwendig sind
  - Tests, mit denen die Umsetzung und Wirksamkeit der definierten Maßnahmen während und nach der Migration überprüft werden kann
  - Das Sicherheitskonzept des Dienstleisters muss außerdem eine Schnittstelle zu folgenden Einheiten der Gesellschaft aufweisen:
    - Incident Management
    - Change Management
    - Informationssicherheits-Risikomangement bzw. IT-Risikomanagement und
    - IT Service Continuity Management
- Im Rahmen der Detailplanung ist ein Migrationsplan mit Rollen und Verantwortlichkeiten zu definieren und dokumentieren, der die vollständige Implementierung der Sicherheitskonzepte umfasst.

1.3.4 Migration

- Die Umsetzung der Maßnahmen muss gemäß dem definierten Migrationsplan erfolgen.
- Eine Freigabe für die Implementierung darf erst nach erfolgreichem Abschluss der in den Sicherheitskonzepten definierten Tests erfolgen.

1.3.5 Betrieb

- Zwischen dem Verantwortlichen für das Vorhaben und dem Dienstleister muss ein regelmäßiger Informationsaustausch über den Status der Informationssicherheit (z. B. aktualisierte Regelungen, aktualisierte Anforderungen usw.) stattfinden. Der Verantwortliche der Konzerngesellschaft muss

INTERNAL

die Anpassung des Vertrags initiieren, sofern Änderungen der Informationssicherheit oder gesetzliche Anforderungen dies erforderlich machen.

- Änderungen am Outsourcing-Gegenstand müssen vor der Umsetzung durch den gleichen Prozess wie ein neues Outsourcing-Verfahren laufen, um darin die notwendigen Anpassungen der bereits erfolgten Schritte des Outsourcing-Verfahrens vorzunehmen.
- Der Dienstleister muss zum Implementierungsstatus regelmäßig Bericht erstatten.
- Der Dienstleister wirkt aktiv bei der Untersuchung von Sicherheitsvorfällen mit und stellt ohne schuldhaftes Verzögern relevante Informationen zur Verfügung.
- Sämtliche durch den Dienstleister durchgeführte Tätigkeiten (z. B. Systemwartungen) sind durch diesen dem Risiko für die Informationssicherheit angemessen zu dokumentieren.
- Das Sicherheitskonzept und definierte, vertraglich vereinbarte Dienste in Zusammenhang mit der Informationssicherheit müssen mindestens einmal jährlich auf Vollständigkeit und Aktualität hin überprüft werden. Der Verantwortliche des Vorhabens und der Dienstleister sind für die Ausführung entsprechender Maßnahmen verantwortlich.
- Der Dienstleister überwacht die Wirksamkeit der von ihm implementierten Sicherheitsmaßnahmen und schlägt Maßnahmen für die Einhaltung bzw. – falls erforderlich – zur Verbesserung des Sicherheitsniveaus vor.

1.3.6 Beendigung des Outsourcing-Vorhabens

- Die Übergabe des Outsourcing-Gegenstands an einen anderen Dienstleister muss wie ein neues Outsourcing-Vorhaben behandelt werden.
- Kommt es zu einer Beendigung des Outsourcing-Vorhabens (Insourcing), müssen die Anforderungen aus den Phasen "Detailplanung" und "Migration" erfüllt werden.
- Bei der Erneuerung des Vertrags muss geprüft werden, ob die Regelungen für die Informationssicherheit und gesetzliche Regelungen weiterhin wie vereinbart gültig sind. Ist dies nicht mehr der Fall, müssen der Vertrag und die technischen sowie organisatorischen Sicherheitsmaßnahmen entsprechend angepasst werden.

1.4 Zusätzliche Anforderungen bei externem Hosting

Folgende Auflagen existieren zum externen Hosting inkl. Cloud-Diensten von Daten:

- IT-Sicherheitsregelungen des Volkswagen Konzerns müssen beachtet werden, insbesondere bezüglich Zugriffsschutz, vom Regelwerk geforderter Authentifikation und der Ausgestaltung der physischen Sicherheit. Bei einem externen Hosting ist über die IT-Sicherheitsregelungen des Konzerns hinaus eine Verschlüsselung des Speichermediums einzusetzen[21].
- Für das Cloud Computing müssen entsprechend der Beschreibung in der Definition von Cloud Computing[22] Anwendungen und Infrastrukturkomponenten bereitgestellt werden. Gesellschaftsspezifische Regelungen zum Einsatz von Cloud Computing in Verbindung mit personenbezogenen Daten sind zu beachten[23].

[21] A.1.5 Informationssicherheit - Regelung Nr. 03.01.02 Kryptographie
[22] Siehe Anhang A.1.6
[23] B.2.1.5

INTERNAL

- Der Konzerngesellschaft muss grundsätzlich die Möglichkeit für ein Vor-Ort-Audit der Umgebung eingeräumt werden. Dies gilt auch für Unterauftragnehmer, zumindest bzgl. der Auditierung durch einen unabhängigen Dritten gemäß internationaler IT-Sicherheitsstandards.
- Der durch die für die Informationssicherheit verantwortliche Einheit der betreffenden Marke definierte Prozess für Remote-Audits bzw. Vor-Ort-Audits ist zu befolgen. Die Prozessbeschreibung ist durch die für die Informationssicherheit verantwortliche Einheit der betreffenden Marke zur Verfügung zu stellen (z.B. in einem Wiki). Ergibt sich bei einem Audit ein mangelhafter Reifegrad, so ist das resultierende Risiko gemäß Konzern-Risikomanagement-Prozess vom Fachverantwortlichen der betreffenden Marke zu behandeln. Die für die Informationssicherheit verantwortliche Einheit der betreffenden Marke behält sich ein Veto-Recht auf das eingestellte Risiko vor.
- Das Sicherheitsniveau des Anbieters ist von diesem durch entsprechende ISMS-Zertifizierungen vor Erbringen der Dienstleistung und regelmäßig dabei nachzuweisen. Diese Zertifizierungen erfolgen zulasten des Anbieters. Je nach erforderlichem IT-Sicherheitsniveau können unterschiedliche Zertifizierungen erforderlich sein. Dies legt die für die Informationssicherheit verantwortlichen Einheit[24] fest.
- Der für die Informationssicherheit verantwortlichen Einheit[25] ist eine mit dem für die IT- und Anwendungsarchitektur zuständigen Bereich abgestimmte Dokumentation der geplanten Infrastruktur vorzulegen.
- Das Vorhaben eines externen Hosting ist mit dem Eigentümer der Daten, der für die Informationssicherheit verantwortlichen Einheit und bedarfsweise weiteren Stakeholdern (zum Beispiel dem Datenschutz, dem Betriebsrat und der Rechtsabteilung der betroffenen Gesellschaften) abzustimmen.
- Für Netzwerkverbindungen sind die Anforderungen der Regelung „Network Access“[26] einzuhalten.
- Im Rahmen der Beauftragung muss eine Applikationssicherheitsüberprüfung durch einen unabhängigen Dritten durchgeführt werden, deren Ergebnis angemessen zum Schutzbedarf ist. (d.h. Penetrationtest nach OWASP ASVS oder FedRAMP oder einem anderen international anerkannten Standard)
- Ein externes Hosting geheimer Daten ist nur zulässig bei:
    - jährlicher Einzelfallbewertung durch die für die Informationssicherheit verantwortlichen Einheit[27]
    - Akzeptanz durch den Dateneigentümer (TMK)
    - Aufnahme in das Risikomanagement.

[24]Siehe Anhang B.2.1.4
[25]Siehe Anhang B.2.1.4
[26] Siehe Anhang A.1.9 Informationssicherheit - Regelung Nr. 03.02.04 Netzwerkzugänge
[27]Siehe Anhang B.2.1.4

INTERNAL

II Verantwortlichkeiten

II.I Kapitel 1: Dienstleistung durch Dritte

Diese Regelung ist von allen Bereichen die mit externen Dienstleistern zusammen arbeiten anzuwenden und einzuhalten.

INTERNAL

Anhang

INTERNAL

A Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheit - Regelung Nr. 03.01.09 Ausnahmegenehmigungen

A.1.2 Informationssicherheit - Handlungsleitlinien Nr. 02.02 für Beschäftigte

A.1.3 Informationssicherheit - Regelung Nr. 03.01.05 Identity- u. Access Management

A.1.4 Informationssicherheit - Regelung Nr. 03.01.15 Risikomanagement in der Informationssicherheit

A.1.5 Informationssicherheit - Regelung Nr. 03.01.02 Kryptographie

A.1.6 Siehe Anhang im Intranet > Regelung Nr. 03 01 16 Third Party Service Delivery Management_Anhang Cloud Computing.xlsx

A.1.7 ORL 13 Sicherheit in der Volkswagen AG

A.1.8 ORGA 27 Antrag: Information Security Supplier Assessment

A.1.9 Informationssicherheit - Regelung Nr. 03.02.04 Netzwerkzugänge

A.2 Referenzen zu Standards

Die folgende Tabelle zeigt die Referenzen zu den Standards ISO/IEC 27001:2013, ISO/IEC 27001:2005 und VDA.

Thema	Kapitel	ISO 27001:2013	ISO 27001:2005	VDA(2014)
Monitoring and review of supplier services	1.2, 1.3	A.15.2.1	A.10.2.2	15.2
Managing changes to supplier services	1.2, 1.3	A.15.2.2	A.10.2.3	-

A.3 Anlagen

A.3.1 Anlage 1 Feedbackformular

Das Feedbackformular für Verbesserungsvorschläge zu den Regelungen kann im Downloadbereich der Konzern Informationssicherheit Website:

https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk

heruntergeladen werden.

Bitte senden Sie das ausgefüllte Formular an: VWAG R: WOB, IT Security Regulations itsr@volkswagen.de .

INTERNAL

A.4 Abkürzungen und Definitionen

Term	Definition
CISO	Chief Information Security Officer
Outsourcing	Outsourcing beinhaltet die Auslagerung aller oder Teile von Aufgaben und Geschäftsprozessen einer Organisation an einen externen Dienstleister. Outsourcing kann sowohl Dienste als auch die Verwendung und den Betrieb von Hardware und Software betreffen.
Outtasking	Im Gegensatz zu Outsourcing versteht man unter Outtasking, dass bestimmte Aufgaben durch einen externen Dienstleister durchgeführt werden. Die Kontrolle über die Prozesse verbleibt jedoch bei Volkswagen. Unter diesen Aufgaben versteht man externe Beratung, Hilfe bei Softwareentwicklung, Support im Betrieb etc.

A.5 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig. Für neue Gesellschaften sind die Inhalte dieser Regelung innerhalb einer Übergangsfrist von einem halben Jahr umzusetzen.

Nächster Überprüfungstermin: 06.10.2023

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[28].

[28] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

INTERNAL

A.6 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	ISSO	K-SIS/G	06.10.2014	Durch GISSC freigegebene Version
2.0	K-FIS	K-FIS/G	07.11.2018	Anpassung bzgl. geheime Daten
2.1	K-FIS	K-FIS/G	28.09.2021	Ergänzung nach viertem Spiegelstrich in Kapitel 1.4 eingefügt
3.0	Alpers, Mareike Barbric, Mirko Bickel, Holger, Dr.	K-DAI/P K-DS/P K-DS/P	27.09.2022	Notwendige Anpassungen im Rahmen der zyklischen Überprüfung

INTERNAL

B Spezifische Ausprägungen

B.1 Konzernweit

Dieses Kapitel beinhaltet spezifische Ausprägungen die innerhalb des gesamten Konzerns gelten. Diese Ausprägungen dürfen durch die Gesellschaften nicht geändert werden.

B.1.1 Kapitel 1: Dienstleistung durch Dritte

-

B.2 Gesellschaftsweit

Dieses Kapitel beinhaltet spezifische Ausprägungen die innerhalb der Gesellschaft gültig sind. Diese Ausprägungen müssen durch die Gesellschaften auf die jeweiligen Gegebenheiten angepasst werden. Bei manchen Ausprägungen ist zur Information in kursiver Schrift angegeben welche Vorgaben für Volkswagen Marke gelten.

B.2.1 Kapitel 1: Dienstleistung durch Dritte

B.2.1.1 K-DS unter Verwendung von dort festgelegten Kontaktmöglichkeiten und Prozesse

B.2.1.2 ORL 50 Schutz Personenbezogener Daten, BDSG

B.2.1.3 Standardisierten Prozess für die Auswahl von Dienstleistern: Vergabe von Konzern-IT-Support Dienstleistungen an Dritte für Systeme mit schützenswerten Daten

B.2.1.4 Zuständige Stelle für Informationssicherheit: K-DS

B.2.1.5 Die Speicherung oder Verarbeitung von personenbezogenen Daten durch Cloud-basierte Anwendungen oder Infrastrukturkomponenten ist nur unter Einhaltung der EU-Datenschutzverordnung und den Datenschutzbestimmungen der jeweiligen Länder zulässig.

INTERNAL

VOLKSWAGEN

AKTIENGESELLSCHAFT

Informationssicherheit

Übergreifende Regelungen und Prozesse
- Cloud Security -

Herausgeber

Group Information Security

Regulation Nr.

03.01.17

Status

Veröffentlicht

Version

3.4

Klassifikation

Internal

Erstellungsdatum

21.09.2022

Veröffentlichungsdatum

29.09.2022

Geltungsbereich

Diese Regelung gilt für die Volkswagen AG (Organisationseinheiten (OE) auf Konzernebene und auf Markenebene der Marke Volkswagen Pkw, der Marke Volkswagen Nutzfahrzeuge sowie der Volkswagen Group Components).

Hinsichtlich der Umsetzung dieser Regelung bei den anderen Volkswagen Konzerngesellschaften gilt die ORL 1 "Organisatorische Regelungen der Volkswagen AG".

©Volkswagen AG, Intern, KSU: 2.1

Inhaltsverzeichnis

I Zweck

Diese Sicherheitsleitlinie hat das Ziel einen Überblick über relevante Sicherheitsanforderungen, Prozesse und Rahmenbedingungen für alle Plattformen der Group IT Cloud (GITC)[1] und deren relevanten Dienste zu geben. Diese Vorschriften sind obligatorisch und müssen von allen Personen, die sich mit den Cloud-Themenbereichen befassen, beachtet werden, insbesondere:

- Account Owner, die für ein GITC-Account verantwortlich und rechenschaftspflichtig sind (z. B. Subskription, Tenant , ...)
- Plattform Owner, die für GITC-Plattformen (PaaS) verantwortlich sind
- Service Owner, die GITC-Cloud-Services für den Volkswagen-Konzern bereitstellen
- Service Owner, die Cloud-Services für den Volkswagen-Konzern bereitstellen
- Externe Dienstleister, die an der GITC-Cloud-Plattform oder an Services für die Volkswagen-Konzern arbeiten (SaaS)
- Applikationsverantwortliche, die auf GITC-Plattformen für den Volkswagen-Konzern Daten migrieren/bereitstellen.

[1] GITC umfasst private und public Clouds, die im Volkswagen-Konzern verwendet werden.

1 Allgemeine Anforderungen

Wenn nicht ausdrücklich für die GITC spezifiziert, gelten die Sicherheitsanforderungen und -vorschriften aus den Rahmenbedingungen der Sicherheitsrichtlinien der Group IT. Insbesondere die folgenden Leitlinien und Vorschriften liefern Hinweise für den Umgang mit Informationssicherheit:

- Regelung Nr. 02-03: IS-Leitlinien für Systembetreiber und Administratoren
- Regelung Nr. 02-04: IS-Leitlinien für Systementwickler
- Regelung Nr. 03-01-16: Management der Dienstleistungserbringung durch Dritte
- Group IT-Architektur Rahmenleitprinzipien - Richtlinie

Darüber hinaus gelten die Anforderungen hinsichtlich der Datenspeicherung gemäß „Klassifizierungssystematik für Unterlagen (KSU)“ wie in ORL 24 definiert.

1.1 Nutzungsbedingungen

Services, die in Cloud-Umgebungen entwickelt und bereitgestellt werden, müssen mit den allgemeinen „Cloud-Nutzungsbedingungen“ übereinstimmen, die im Firmen-Repository dokumentiert sind.

1.2 Genehmigung von Cloud-Services

Verfügbare und genehmigte Cloud-Services und die entsprechenden Regeln für die Servicenutzung sind im Portfolio für Cloud-Services des Unternehmens dokumentiert:

- Alle Services müssen in der auf der jeweiligen Profilseite des Dienstes beschriebenen Weise genutzt werden.
- Alle Dienste müssen im Portfolio für Cloud-Services dokumentiert werden.
- Alle Services müssen vor ihrer Nutzung vom Verantwortlichen der IT-Sicherheitsabteilung durch eine dokumentierte Genehmigung autorisiert werden.

1.3 Service Härtung

Alle Konzepte und Konfigurationen müssen mit den CIS-Benchmarks und CIS-Einstellungen übereinstimmen und entsprechend gehärtet werden.

1.4 Vertraulichkeit und Verbindlichkeit von GITC Cloud Services

Die folgenden Vertraulichkeitsregeln sind verbindlich.

Die Klassifizierung für die Nutzung der verfügbaren GITC-Services ist je nach Cloud-Typ und Service-Modell obligatorisch. Das Schutzziel hinsichtlich der Vertraulichkeit in Abhängigkeit vom Cloud-Typ finden Sie im Anhang A1.16 zur Informationssicherheits-Regelung Nr. 03.01.16 „Management der Dienstleistungserbringung durch Dritte“.

2 GITC Onboarding

2.1 Initiales Lieferanten-Onboarding

Für jeden Dienst müssen ein Betriebskonzept, ein Supportprozess und ein Service Owner (Managementverantwortung) definiert werden.

Verträge mit externen Dienstleistern (IaaS, PaaS, SaaS), die für GITC relevant sind, müssen mit den verfügbaren Standard-Beschaffungsprozessen übereinstimmen.[2]

Die folgenden Anforderungen müssen berücksichtigt werden:

- Im Allgemeinen:
  - Verträge für Software, Lizenzen oder zusätzliche Services müssen gemäß IT-PEP verwaltet werden
  - Open-Source-Services müssen konform sein und insbesondere auf mögliche Lizenzverletzungen geprüft werden
  - Vertraulichkeitsvereinbarungen[3]
  - Datenverarbeitungsvereinbarung (DPA)[4] wie von der DSGVO gefordert (ohne Datenschutz-verträge dürfen keine personenbezogenen Daten in Cloud-Umgebungen verarbeitet werden)
- für externe Lieferanten
  - IT Security Regelung Nr. 02-06: IS-Leitlinien für Dritte, die die Volkswagen-Infrastruktur nutzen, ist obligatorisch
  - TISAX-Zertifizierung für externe Lieferanten, die auf Volkswagen-Daten zugreifen, ist obligatorisch[5]
  - Ein Cloud Vendor Assessment (CVA) ist für Cloud-Services (PaaS, SaaS) obligatorisch
  - Onboarding aller Service-Provider-Mitarbeiter, die mit der Volkswagen Infrastruktur arbeiten (Volkswagen-Kunden, Volkswagen-Dienstleister) oder Zugang zum Volkswagen-Netzwerk haben (On-Premise, extern gehostet oder Cloud), muss über die ONE.Konzern Business Plattform (ONE.KBP) und entsprechend dem B2B-Identity Process erfolgen.[6]

Diese Prozesse stellen sicher, dass obligatorische Sicherheitsanforderungen in Verträgen mit externen Parteien berücksichtigt werden.[7]

2.2 Projekt Onboarding

Um ein sicheres Onboarding auf bestehenden Plattformen zu gewährleisten, müssen die spezifischen Plattformanforderungen für Onboarding befolgt werden. Der Cloud-Onboarding-Prozess ist ebenfalls Teil des IT-PEP.[8]

Das sichere Onboarding der Nutzer muss den IAM-Anforderungen entsprechen (z. B. Informations-sicherheits-Regelung Nr. 03.01.05 Authentisierung und IAM).

Im Allgemeinen gelten für alle Migrationen oder Deployments von Anwendungen für GITC, Meilensteine mit verbindlichen Ergebnissen und Genehmigungen gemäß dem IT-PEP-Prozess. Darüber hinaus ist es für jedes

[2] Einkaufsprozesse und Anforderungen des Unternehmens müssen berücksichtigt werden.
[3] ORL 13 Sicherheit in der Volkswagen Aktiengesellschaft. Für die Volkswagen Group siehe auch KRL 13 Appendix 2.
[4] s. auch AVV “Auftragsverarbeitungsvertrag”.
[5] ORL 13 Sicherheit in der Volkswagen Aktiengesellschaft. Für die Volkswagen Group s. auch KRL 13 Appendix 2.
[6] Der B2B-Identity Prozess wird nicht bei allen Marken verwendet. In diesen Fällen ist der jeweils korrespondierende Prozess anzuwenden.
[7] Einkaufsprozesse und Anforderungen des Unternehmens müssen berücksichtigt werden.
[8] Weitere Informationen zum Secure Onboarding finden sich im Group IT Cloud in Group WIKI.

Projekt obligatorisch, mindestens einen technischen Risikoeintrag für das Projekt selbst in der Risikomanagementlösung des Unternehmens zu erstellen.[9]

[9] Diese Regelung gilt für die Marke VW (z. B. IRMA). Umfang und Einträge der Risiken in entsprechenden Risk Management Systemen (RKS/IKS) unterliegen jedoch den von einer Marke oder Gesellschaft geforderten Risikorichtlinien.

3 GITC Service Design & Implementierung

3.1 Entwicklungsmethodik

Die Entwicklung und Deployments von GITC-Services muss dem IT-PEP Prozess entsprechen.

3.2 Sichere Softwareentwicklung

Es gelten die Sicherheitsanforderungen, wie sie in der IS-Leitlinie 02.04 „Informationssicherheitsleitlinien für Systementwickler“ und der Vorschrift 03.04.02 - Bereitstellung sicherer Anwendungen als Teil der Rahmenbedingungen der Group-IT-Sicherheitspolitik R6 definiert sind.

Bei der Entwicklung und dem Testen von Anwendungen sind die folgenden Kriterien zu berücksichtigen und die Entwickler müssen sich der folgenden Inhalte bewusst sein:

- OWASP Application Security Verification Standard (ASVS), Level 2 (oder höher)
  https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
- OWASP Top 10
  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Es wird erwartet, dass ein gleichwertiges Verfahren von den Anbietern von Standardsoftware befolgt wird.

Hinweis: Alle vertraulichen Informationen und Anmeldedaten müssen auf sichere Art und Weise gehandhabt werden. Beispielsweise muss sichergestellt werden, dass Passwörter, die von technischen Benutzern in DevOps-Workflows verwendet werden, nicht im Klartext gespeichert werden.[10]

Teil der Cloud-Softwareentwicklung ist ein sicherer Build- und Deployment-Prozess.

> Als Beispiel soll eine Continuous Integration/Continuous Delivery (CI/CD)-Pipeline verwendet werden, um Builds, Tests, (Sicherheits-)Scans und den Einsatz in verschiedenen Umgebungen zu automatisieren.

Applikationsverantwortliche von GITC-Services sind für die Überprüfung des Quellcodes, einschließlich der verwendeten Open-Source-Artefakte, verantwortlich.

Vor dem Deployment des Codes (binär) gemäß dem IT-PEP Prozess und der o.g. Vorschrift ist eine Sicherheits-Quellcodeanalyse mit automatisierter Prüfung und Auswertung der Ergebnisse durchzuführen. Ergebnisse müssen fixiert und in das Risikomanagement mit definierten Maßnahmen und Zeitrahmen einbezogen werden.

Penetrationstests (manuelle und automatische Inspektion) der Systeme umfassen Netzwerk- und Applikationstests. Die Tests werden von einer unabhängigen Drittpartei oder Organisationseinheit durchgeführt bevor der Service bereit gestellt wird und danach regelmäßig, wie im IT PEP Prozess festgelegt. Aufgedeckte Schwachstellen müssen behoben und in das Risikomanagement einbezogen werden. Maßnahmen und Zeitrahmen sind festzulegen.

Cloud-Penetrationstests müssen im Einklang mit den Gesetzen und Vorschriften der Cloud-Anbieter stehen.

[10] s. auch die Passwort Policy (A01.070).

3.3 Images und Repositories

Zentral zur Verfügung gestellte Images und Repositories für GITC (z. B. OS Image Factory) sind gemäß den entsprechenden Gruppen-/Markenverfahren zu verwenden.[11]

3.4 Ressourcen-Tagging

Alle in GITC erstellten Ressourcen müssen gemäß der GITC Tagging-Richtlinie gekennzeichnet werden.

Die Tags werden verwendet, um den Cloud-Ressourcen Metadaten zuzuweisen.

3.5 Informationssicherheitsrisikoanalyse

Bevor ein GITC-Service eingerichtet werden kann, muss eine dedizierte und dokumentierte Bestands- und Risikobewertung durchgeführt werden. Als Teil des ISMS müssen alle relevanten Risiken dokumentiert werden. Dazu gehören zum Beispiel:

- relevante Bedrohungsszenarien
- Auswirkungen von Bedrohungen

3.6 Netzwerk Kommunikation

Alle erlaubten Kommunikationen werden in einer Kommunikationsmatrix dokumentiert, die wiederum von einem zuständigen CISO genehmigt werden müssen.

Die in der Matrix genehmigte Kommunikation muss durch den Einsatz einer hostbasierten Firewall abgesichert werden.[12]

Einzelheiten zu Einschränkungen und Kommunikationsmustern finden sich in der A.1.18 Group IT Architecture - Secure Environments Architecture - Policy

3.7 Netzwerk Audit

Das Netzwerk-Audit muss regelmäßig in Übereinstimmung mit der Kommunikationsmatrix durchgeführt werden. Eine verantwortliche Person für das Netzwerk-Audit ist zwingend erforderlich. Das Audit darf nicht von den Projekten selbst durchgeführt werden.

[11] Zentral bedeutet, Images pro Foundation, die entweder konzernweit oder von einer Marke bereitgestellt werden.
[12] Dies kann entweder via einer Cloud- / Hypervisor-basierenden Firewall (z. B. Security Groups, NACL) oder einer host-basierten Firewall erreicht werden. Der Gebrauch letzterer wird bevorzugt, da sie die Möglichkeit unterbindet, das Filtering innerhalb der gesicherten Entität auszuschalten und somit eine strikte Trennung der Zuständigkeiten ermöglicht. Die gleiche Netzwerktrennung muss für alle Arten von Overlays implementiert werden, z.B. für Container.

4 GITC Monitoring

4.1 Compliance Monitoring

Die Konfiguration der GITC-Services muss im Einklang mit definierten Compliance-Regelsätzen (siehe Kapitel 1.4) stehen und der Ausnahmevorschrift (Informationssicherheits-Regelung Nr. 03.01.09 Ausnahmeprozess) sowie der Informationssicherheits-Regelung Nr. 03.01.04 Sicherheitsprotokollierung und Monitoring folgen.

Der Service Owner für GITC-Service muss die rechtzeitige Behebung festgestellter Abweichungen von Compliance-Regelsätzen unterstützen.

4.2 Security Monitoring

Alle kritischen GITC-Services auf allen Ebenen (IaaS, PaaS, SaaS) müssen überwacht werden, und die obligatorischen Protokollquellen müssen an ein SIEM-System (Security Incident and Event Management) angeschlossen werden. Die Anwendungen müssen kontinuierlich überwacht werden, um schnell auf Sicherheitsvorfälle reagieren zu können (siehe Informationssicherheits-Regelung Nr. 03.01.18 über das Management von Informationssicherheitsvorfällen und Schwachstellen).[13]

Für jeden Dienst müssen kritische Sicherheitsereignisse und ihre Auswirkungen identifiziert und in den Katalog der Sicherheitsrisiken der Cloud aufgenommen und vom Service Owner entsprechend überwacht werden.

[13] Betriebliches Monitoring in Bezug auf Verfügbarkeit ist hier ausgeklammert.

5 Schwachstellen-Management

Schwachstellen-Management (Vulnerability Management) ist für alle GITC-Plattformen obligatorisch. Das Ziel der Implementierung von Scans in mehreren Phasen des Cloud-Lifecycle ist es, Schwachstellen zu scannen und zu melden, um einen einwandfreien, sicheren und konformen Betrieb der folgenden Elemente zu unterstützen:

- Images/Container
- Web-Applikationen
- Accounts und Instanzen
- Software und Source Code.

Der vereinfachte Lifecycle des Schwachstellenmanagements umfasst die folgenden Schritte:

- Schwachstellenidentifikation
- Bewertung
- Reporting
- Behebung und Mitigierung

5.1 Schwachstellen-Scans

Schwachstellen-Scans müssen in Abhängigkeit von der Umgebung regelmäßig durchgeführt werden. Die spezifischen Scan-Anforderungen sind in den Cloud-Sicherheitsrichtlinien definiert.

Die folgenden Elemente sollten im Scope von Schwachstellen-Scans enthalten sein:

- Assets wie Container und Instanzen
- Webseiten
- Registries
- Container-Images
- Netzwerk
- Software & Source Code

Die Visibilität der Accounts ist obligatorisch.

5.2 Schwachstellenbehebung und/oder -mitigierung

Sicherung eines aktiven Lifecycle-Management und Patch-Prozesses (siehe unten). Die verwendeten Softwareprodukte müssen immer auf dem neuesten Stand gehalten werden. Schwachstellen, die als „kritisch oder „hoch“ eingestuft werden, müssen sofort beseitigt werden (siehe Informationssicherheits-Regelung Nr. 03.01.18: Management von Informationssicherheitsvorfällen und Schwachstellen). Wenn das Patchen keine Option ist, muss sichergestellt werden, dass Mitigierungsfaktoren vorhanden sind, und dass diese im Risikomanagementkatalog dokumentiert werden.

6 Patch-Management

Im Betriebskonzept ist zu berücksichtigen, dass ein Lifecycle- und Patch-Management für alle Assets in der Cloud gewährleistet ist. Als Teil des Lifecycle-Management sind Maßnahmen zur Pflege und Bereinigung festzulegen und regelmäßig zu befolgen.

Patch Management beschreibt den Rahmen für das Patchen aller Assets, einschließlich Betriebssystem, Container, Instanzen, Software, Accounts usw. Für die allgemeine Definition von Assets siehe Informationssicherheits-Regelung Nr. 03.01.13 Asset-Management.

Es gilt die Regelung für Änderungs- und Patch-Management, die von allen für den Betrieb von IT-Systemen verantwortlichen Stellen zu beachten ist (siehe Informationssicherheits-Regelung Nr. 03.01.08 Änderungs- und Patch-Management). Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur vorübergehend nach Rücksprache mit der Group Information Security zulässig.

7 Backup und Recovery

Das Schutzniveau für gesicherte Daten in Cloud-Systemen muss an Informationssicherheitsstandards und -vorschriften angepasst werden.

Als Teil eines Betriebskonzepts für Cloud-Services und -Anwendungen muss ein Backup- und Recovery-Prozess definiert werden. Der Account Owner hat dafür zu sorgen, dass die notwendigen Backup- und Wiederherstellungsmaßnahmen gemäß den Sicherungs- und Wiederherstellungsvorschriften getroffen und getestet werden (siehe Informationssicherheits-Regelung Nr. 03.01.06 Backup und Archivierung).

Als Teil der Betriebsprozesse und des Geschäftskontinuitätsmanagements muss für jeden Dienst, der in Bezug auf die Verfügbarkeit als kritisch identifiziert wurde, ein Disaster-Recovery-Plan (DRP) definiert werden.

Anhang

A Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheits-Leitlinien Nr. 02.02 für Beschäftigte

A.1.2 Informationssicherheits-Leitlinien Nr. 02.03 für Systembetreiber und Administratoren

A.1.3 Informationssicherheits-Leitlinien Nr. 02.04 für Systementwickler

A.1.4 Informationssicherheits-Leitlinien Nr. 02.06 für Dienstleister

A.1.5 Informationssicherheits-Regelung Nr. 03.01.04 Sicherheitsprotokollierung und -monitoring

A.1.6 Informationssicherheits-Regelung Nr. 03.01.05 Authentifizierung und IAM

A.1.7 Informationssicherheits-Regelung Nr. 03.01.06 Backup und Archivierung

A.1.8 Informationssicherheits-Regelung Nr. 03.01.08 Change und Patch Management

A.1.9 Informationssicherheits-Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.10 Informationssicherheits-Regelung Nr. 03.01.13 Asset Management

A.1.11 Informationssicherheits-Regelung Nr. 03.01.16 Dienstleistung durch Dritte

A.1.12 Informationssicherheits-Regelung Nr. 03.01.18 Information Security Incident and Vulnerability Management

A.1.13 Informationssicherheits-Regelung Nr. 03.04.02 – Bereitstellen sicherer Applikationen

A.1.14 Informationssicherheits-Regelung - Business Process Manual for CIS Security Settings

A.1.15 Informationssicherheits-Regelung - Glossary

A.1.16 Group Cloud Security Policies

A.1.17 Group IT Architecture Guiding Principles Frame - Policy

A.1.18 Group IT Architecture - Secure Environments Architecture - Policy

A.1.19 Platform Delivery Center (PDC)

A.1.20 Group IT Cloud in Group WIKI

A.1.21 Group Security (Konzernsicherheit)

A.2 Anlagen

A.2.1 Anlage 1 Feedbackformular

Das Feedbackformular für Verbesserungsvorschläge zu den Regelungen kann im Downloadbereich der Konzern Informationssicherheit Website:

https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk

heruntergeladen werden.

Bitte senden Sie das ausgefüllte Formular an: VWAG R: WOB, IT Security Regulations itsr@volkswagen.de .

A.3 Abkürzungen und Definitionen

Siehe A.1.15 Information Security Glossary

A.4 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig.
Für neue Gesellschaften sind die Inhalte dieser Regelung innerhalb einer Übergangsfrist von einem halben Jahr umzusetzen.

Nächste Überprüfung: 29.09.2023

A.5 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	K
1.0	K-FIS	K-FIS/G	18.09.2019	Initial Version as developed by ODP/K-FIS-Team
2.0	K-FIS	K-FIS/G	07.01.2020	Scope definition and feedback from version 1
3.0	K-FIS, Audi	K-FIS/P, K-FIS-I, I/BT-C1	20.05.2020	Revised general edition for cloud security (provided by GISP 2020)
3.3	VW, Audi	K-FIS/G, K-FIS-I, I/BT-C1	26.01.2021	Group-wide general edition of regulation for cloud security after Veto Process
3.4	K-DS/G	K-DS/G	21.09.2022	Redaktionelle Überarbeitung