VOLKSWAGEN GROUP

IS-Regelung 02.06

Handlungsleitlinie für Dritte

Version: 5.1
Beginn der Gültigkeit: 29.06.2023

Verantwortlicher Bereich: Information Security Governance – K-DS/G
itsr@volkswagen.de

Herausgeber: Information Security Governance – K-DS/G
(itsr@volkswagen.de)

Inhalt

Hinweise zum Dokument

Änderungen im Regelungstext sind mit Schriftfarbe #E67364 markiert.

Zur besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers verzichtet. Gemeint sind männliche, weibliche und diverse Beschäftigte gleichermaßen.

1 Zweck

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.

1.1 Dokumentenstruktur und Zielgruppe

Diese Handlungsleitlinie richtet sich an die Geschäftsleitung der Dritten. Die Geschäftsleitung der Dritten hat sicherzustellen, dass deren Beschäftige und Erfüllungs-/Verrichtungsgehilfen, die Informationen des Volkswagen Konzerns verarbeiten, auf diese Handlungsleitlinie verpflichtet werden.
Diese Handlungsleitlinie gilt nicht für Kunden einer Volkswagen Konzerngesellschaft.
Dieses Dokument enthält drei Kapitel. Die folgende Tabelle führt die Dokumentenstruktur und die jeweilige Zielgruppe pro Kapitel auf.

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

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

2 Geltungsbereich

Diese Anweisungen gelten für alle Dritte, die nach Volkswagen Definition als Intern, Vertraulich oder Geheim klassifizierte Informationen für den Volkswagen Konzern entsprechend vertraglicher Vereinbarungen verarbeiten.

3 Allgemeine Anforderungen an alle Dritte

3.1 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 sich an bestimmten Meilensteinen ändern.

Werden vom Dritten Dokumente oder Informationen für den Volkswagen Konzern

erstellt, ist die Klassifikation nach Vertraulichkeit beim Ansprechpartner des Volkswagen Konzerns zu erfragen und entsprechend zu kennzeichnen.

3.2 Weitere Vorgaben

- Informationssicherheitsereignisse (z. B. auftretende Störungen, Verstöße gegen das Informationssicherheits-Regelwerk, Cyberattacken), welche Informationen oder IT-Systeme des Auftraggebers betreffen, sind unverzüglich der zuständigen Stelle mit den erforderlichen Informationen zur Beurteilung der Kritikalität zu melden (siehe Anhang B.1.1). Weitere Informationen zum Ereignis sind auf Anfrage dem Auftraggeber zur Verfügung zu stellen.
- 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 B.1.1).
- Beim Verdacht auf Verlust von internen, vertraulichen oder geheimen Informationen des Auftraggebers, muss dies sofort an den Ansprechpartner der beauftragenden Volkswagen Konzerngesellschaft gemeldet werden.
- Die Weitergabe von Daten oder Informationen an weitere Dritte ist nur mit schriftlicher Freigabe durch den Informationseigentümer (siehe Anhang B.1.3) 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 (durch siebenfaches überschreiben oder durch einen Degaußer) gelöscht werden. Nicht mehr benötigte Speichermedien sind physisch zu zerstören.
- 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.

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

4.1 Definition

Ein Dritter arbeitet in der Volkswagen Konzern Infrastruktur, wenn:

- IT-Geräte (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 oder
- über das Internet bereitgestellte zugriffsgeschützte Applikationen einer Volkswagen Konzerngesellschaft genutzt werden. Dies betrifft keine

Applikationen die vom Anwender in seiner Rolle als Endkunde genutzt werden.

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

4.2 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 Ansprechpartner im beauftragenden Fachbereich der Konzerngesellschaft 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 Ansprechpartner im beauftragenden Fachbereich der Konzerngesellschaft 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 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 Dritten 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.
- Der Verlust von durch die Konzerngesellschaft zur Verfügung gestellter Hardware ist durch den entsprechenden Nutzenden unverzüglich dem zuständigen Ansprechpartner im beauftragenden Fachbereich der Konzerngesellschaft 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 vertraglich vereinbarten Tätigkeiten verarbeitet und genutzt werden. Eine Weitergabe dieser Daten an Unbefugte 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.

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

Informationen müssen während des gesamten Lebenszyklus entsprechend ihrer aktuellen Vertraulichkeitseinstufung vor einem Zugriff durch Unbefugte 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: Gemäß ISO/IEC 21964, Schutzklasse 1
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: Gemäß ISO/IEC 21964, Schutzklasse 2 • 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

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: Gemäß ISO/IEC 21964, Schutzklasse 3 • 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. • 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.

4.4 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 Ansprechpartner im beauftragenden Fachbereich der Konzerngesellschaft 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 Ansprechpartner im beauftragenden Fachbereich der Konzerngesellschaft 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.

4.5 Nutzung von Netzwerkdiensten

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

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

4.6 Zusätzliche Anforderungen bei mobiler Arbeit

Die Beschäftigten des Dritten haben eigenverantwortlich sicherzustellen, 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 Unbefugte sichtbar und zugänglich sein und auch nicht mitgehört werden. Zudem muss Schutz vor Aufzeichnungen durch Spracherkennungsgeräte gewährleistet werden.

Geheime Informationen dürfen grundsätzlich nicht während der mobilen Arbeit bearbeitet werden.

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.

5 Zusätzliche Anforderungen an Dritte, die Informationen des Volkswagen Konzerns außerhalb der Volkswagen Konzern Infrastruktur im Zugriff haben oder bereitstellen

5.1 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 oder für den Volkswagen Konzern oder weitere Dritte im Auftrag des Volkswagen Konzerns hostet.

5.2 Anforderungen

- Es gelten die Regularien zur Informationssicherheit des Dritten, soweit nichts anderes vertraglich vereinbart wurde.

Zuständigkeiten

Verstöße gegen diese Handlungsleitlinie werden individuell nach gültigen gesetzlichen und vertraglichen Bestimmungen geprüft und entsprechend geahndet. Abweichungen von dieser Handlungsleitlinie, die das Sicherheitsniveau beeinträchtigen, sind nur nach Rücksprache mit dem Ansprechpartner der Volkswagen Konzerngesellschaft gestattet und immer zeitlich zu begrenzen.

Anhang

A Allgemeines

A.1 Feedback

Feedback oder Verbesserungsvorschläge können an folgende E-Mail Adresse gesendet werden: VWAG R: WOB, IT Security Regulations itsr@volkswagen.de.

Um die Änderungsvorschläge besser zuordnen zu können, geben Sie bitte folgende Informationen an:

- Nummer und Name der Regelung
- Kapitel/ Unterkapitel
- Grund der Änderung
- Änderungsvorschlag

Alle Änderungsvorschläge werden gemäß des Prozesses zur Erstellung, Freigabe und Veröffentlichung der Volkswagen AG Regelungen bewertet.

A.2 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: Juni 2024

A.3 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. 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
5.1	K-DS/G	K-DS/G	29. Juni 2023	Überarbeitung durch Regelungsteam und Freigabe durch K-DS Leitungsrunde

B Gesellschaftsspezifische Ausprägungen

B.1 Gesellschaftsspezifische Ausprägungen

B.1.1 CERT VW - über Enterprise Help Desk (EHD, Tel. +49 531 9 33000, <EHD@volkswagen.de>)

B.1.2 Anforderungen Informationssicherheit und IT-Sicherheit (volkswagen.de)

B.1.3 Der Informationseigentümer (z.B. Leiter der Organisationseinheit) ist im eigenen Bereich für die Klassifikation und die Einhaltung der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) verantwortlich.