VOLKSWAGEN GROUP

IS-Regelung 02.04

Handlungsleitlinie für Systementwickler

Version: 4.3
Beginn der Gültigkeit: 22.02.2024

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

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

Inhalt

1 Zweck 4
2 Geltungsbereich 4
3 Asset-Management 4
4 Kommunikations- und Betriebsmanagement 4
5 Zugangskontrolle 5
6 Beschaffung, Entwicklung und Wartung von IT-Systemen 5
6.1 Sicherheitsanforderungen für IT-Systeme 5
6.1.1 Vertraulichkeit 6
6.1.2 Integrität 6
6.1.3 Verfügbarkeit 7
6.2 Verarbeitung in Anwendungen 8
6.3 Kryptographische Maßnahmen 8
6.4 Sicherheit von IT-Systemdateien 9
6.4.1 Schutz von IT-Systemtestdaten 9
6.4.2 Zugriffskontrolle auf Quellcode 9
6.5 Sicherheit in Entwicklungs- und Unterstützungsprozessen 9
7 Compliance und Einhaltung gesetzlicher Verpflichtungen 10
Zuständigkeiten 11
Anhang 12
A Allgemeines 12
A.1 Mitgeltende Dokumente 12
A.2 Feedback 12
A.3 Gültigkeit 12
A.4 Abkürzungen und Definitionen 12
A.5 Dokumenthistorie 13
B Gesellschaftsspezifische Ausprägungen 14
B.1 Gesellschaftsspezifische Ausprägungen 14

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 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.1.1).

2 Geltungsbereich

Diese Handlungsleitlinie gilt für die Volkswagen Aktiengesellschaft, d.h. für Konzernfunktionen, die Marke Volkswagen Pkw, die Volkswagen Nutzfahrzeuge und die Volkswagen Group Components. Alle IT-Systementwickler (gemäß Definition in A.4) müssen diese Leitlinie erfüllen und einhalten.

3 Asset-Management

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

4 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 B.1.6). Dabei sind die Vorgaben aus der Regelung Nr. 03.01.16 Dienstleistung durch Dritte zu befolgen.

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.

5 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.

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. 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“).

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 • Ablageverschlüsselung

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
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)

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:

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

6.2 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 B.1.4).

6.3 Kryptographische Maßnahmen

Grundlegende Entscheidungen zur Strategie, Verwendung und zum Umgang mit kryptographischen Methoden sind durch die zuständigen Stellen festzulegen (siehe Anhang B.1.5).

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

6.4 Sicherheit von IT-Systemdateien

6.4.1 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.1.7) 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.

6.4.2 Zugriffskontrolle auf Quellcode

Quellcode ist entsprechend der jeweiligen Datenklassifikation (siehe Kapitel 6.1) zu klassifizieren und zu schützen.

6.5 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.

7 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.

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 B.1.1) gestattet.

Anhang

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:
IS Regelungen - Informationssicherheitsregelwerk - Group Wiki (volkswagen-net.de)

A.2 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.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: Februar 2025

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 • 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. September2022	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
4.2	K-DS/G	K-DS/G	03. August 2023	Geltungsbereich geändert
4.3	K-DS/G	K-DS/G	22.02.2024	Freigabe K-DS Leitungsrunde

B Gesellschaftsspezifische Ausprägungen

B.1 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.1.1 zuständige Stelle bei Abweichungen von diesen Handlungsleitlinien, die 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: Service Catalog - Volkswagen Service Portal (service-now.com)

B.1.2 Veröffentlicht im Group Wiki:

Informationssicherheitsregelwerk (DE) - Informationssicherheit - Group Wiki (volkswagen-net.de)

B.1.3 Für Marke Volkswagen dokumentiert in der ORL 18

B.1.4 Die verwendete Anwendungssoftware muss gemäß BV 2/80 „Unterrichtung und Beratung über Systemvorhaben der Informationsverarbeitung" mit dem Betriebsrat beraten werden.

B.1.5 Zuständigkeiten: Informationssicherheitsorganisation des Konzerns, IT Projects, Architectures & Standards

B.1.6 Zuständigkeiten: Informationssicherheitsorganisation des Konzerns

B.1.7 Datenschutzmanager-Organisation (DSMO): Ansprechpartner für Ihren Fachbereich finden Sie im Datenschutz-Wiki. Für weitere Informationen siehe auch: ORL 50 „Datenschutz und Datenschutz-Governance"