Informationssicherheitsheitshandlungsleitlinien für Systementwickler

Gültig ab:	31.03.2017	Status:	Veröffentlicht
Geändert am:	01.10.2020	Version:	4.0
Herausgeber:	CISO (B/FP)	Klassifikation:	Intern – KSU 2.1

Geltungsbereich
Die Handlungsleitlinien gelten für AUDI BRUSSELS und werden durch konkrete IT-Regelungen im Einzelfall ausgestaltet.

Inhaltsverzeichnis

I. Zweck

Dieses Dokument basiert auf den obersten Vorgaben zur Informationssicherheit im Volkswagen Konzern.

In dieser Informationssicherheitshandlungsleitlinie werden die Regeln für die Informationssicherheit definiert, die von Systementwicklern[1] in ihrem Zuständigkeitsbereich für IT-Systeme und die IT-Infrastruktur zu befolgen sind.

Darüber hinaus gilt für die Zielgruppe der Systementwickler die Informationssicherheitshandlungsleitlinie für Mitarbeiterinnen und Mitarbeiter. Systementwickler müssen sich über alle (rollenspezifischen) Vorgaben informieren und diese einhalten, wenn sie in zusätzlichen Rollen arbeiten.

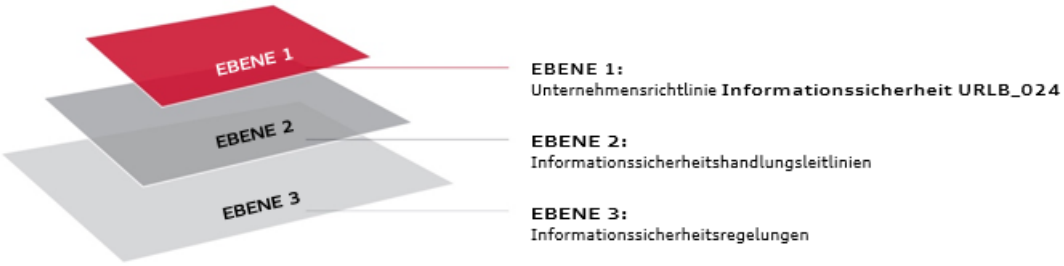
Zweck der Informationssicherheitshandlungsleitlinien ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Schutz der Rechte und Interessen der Gesellschaft und aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit einer Konzerngesellschaft 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).

1. Kontext

Die folgende Übersicht zeigt die Einordnung der Informationssicherheitshandlungsleitlinien in das Informationssicherheitsregelwerk.



Informationssicherheitsregelwerk

2. Management von organisationseigenen Werten

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

[1] Definition in A.2

3. Betriebs- und Kommunikationsmanagement

Sicherheitsrelevante Tätigkeiten (wie z. B. die Verwaltung kryptographischer Schlüssel, der Sicherheitsinfrastruktur oder von Sicherheitssystemen) dürfen erst durch Lieferanten/Subunternehmer ausgeführt werden, nachdem die zuständige Stelle dies genehmigt hat (siehe Anhang, B.1.2). Dabei sind die Vorgaben aus Regelung 03.01.16 Dienstleistungserbringung durch Dritte zu befolgen.

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

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

Die Systemplanung (funktionale Spezifikation, Systementwurf, Systemimplementierung) und die Systemabnahme (Systemeinführung) sind entsprechend den konzernweit geltenden Standards zur Systementwicklung IT-PEP auszuführen. Hierfür steht eine für AUDI BRUSSELS adaptierte Version des IT-PEP zur Verfügung.

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

4. Zugangskontrolle

Für den Zugriff auf Informationen sind, auf Grundlage einer Risikobewertung, durch den Informationseigentümer Mechanismen zur Authentifizierung und Autorisierung zu erstellen. Dazu zählt die Implementierung der durch den Informationseigentümer spezifizierten Rollen und Berechtigungen (Berechtigungskonzept).

Der Systemverantwortliche ist verantwortlich für die Implementierung eines sicheren Anmeldeverfahrens (z. B. starke Authentifizierung mittels Smartcard), das den Regelungen entspricht.[2]

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).

Die für die jeweiligen Systeme zuständigen Personen müssen mittels geeigneter Systemimplementierungen die festgelegten Mindestanforderungen an Passwörter (siehe „Informationssicherheitshandlungsleitlinie für Mitarbeiterinnen und Mitarbeiter“) umsetzen.

Alle Anmeldeinformationen (z. B. Passwörter oder Schlüssel) sind mindestens als „vertraulich“ zu klassifizieren und entsprechend zu behandeln. Der Eigentümer der mittels dieser Anmeldeinformationen zugänglichen Informationen kann diese als „geheim“ klassifizieren.

Anmeldeinformationen sind vor unbefugtem Zugriff zu schützen. Passwörter in Systemen, Anwendungen, Datenbanken und Token müssen als nicht umkehrbare Hash-Werte gespeichert werden. Im Idealfall sollten sie als Hash mit „Salt“[3] oder in Form anderer sichererer Alternativen gespeichert werden. 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 Systemen muss eine gegenseitige (bidirektionale) Authentifizierung (wie z. B. TLS) verwendet werden.

[2] Siehe Informationssicherheitshandlungsleitlinie für Systembetreiber und Administratoren

[3] „Salt“ bezeichnet eine zufällig erzeugte Zeichenfolge in der Kryptographie, die vor der Anwendung einer Hash-Funktion an einen Klartext angehängt wird, um die Entropie zu verbessern.

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.

5. Beschaffung, Entwicklung und Wartung von Informationssystemen

5.1. Sicherheitsanforderungen für Informationssysteme

Bevor ein IT-System entwickelt und eingesetzt wird, sind alle erforderlichen Informations-Sicherheitsmaßnahmen 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 Informationssicherheitshandlungsleitlinie für Mitarbeiterinnen und Mitarbeiter, Abschnitt „Klassifizierung von und Umgang mit Informationen“).

5.1.1. Schutz der 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	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheitspatches)
Intern	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheitspatches) • Zugriffskontrolle entsprechend dem Grundsatz "Kenntnis, nur wenn nötig" • Ein-Faktor-Authentifizierung (z. B. User-ID und Passwort)
Vertraulich	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheitspatches) • Zugriffskontrolle entsprechend dem Grundsatz "Kenntnis, nur wenn nötig" • Zwei-Faktor- Authentifizierung (z. B. Smartcard mit 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	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheitspatches) • Zugriffskontrolle entsprechend dem Grundsatz "Kenntnis, nur wenn nötig" • Zwei-Faktor- Authentifizierung (z. B. Smartcard mit PIN), insbesondere für den Zugriff auf Anwendungen • Transportverschlüsselung • Ablageverschlüsselung

5.1.2. Schutz der Integrität

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

Klassifizierung	Definition
Gering	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheitspatches)
Mittel	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheitspatches) • Zugriffskontrolle entsprechend dem Grundsatz "Kenntnis, nur wenn nötig" • Ein-Faktor- Authentifizierung (z. B. User-ID und Passwort) • Datenbanken: Der Schutz der referentiellen Integrität muss aktiviert sein.
Hoch	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheitspatches) • Zugriffskontrolle entsprechend dem Grundsatz "Kenntnis, nur wenn nötig" • 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. Feldgrenzen-Überprüfung, Beschränkung von Feldern auf 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 mit PIN) für Schreibzugriffe • Generierung und Verifizierung von digitalen Signaturen für gespeicherte Daten oder 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. Schutz der Verfügbarkeit

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

Klassifizierung	Definition
Gering	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheitspatches) • Wiederherstellungsmaßnahmen in 72 Stunden oder später. Dazu sind geeignete Maßnahmen zu implementieren.
Mittel	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheitspatches) • 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 Sicherheitspatches) • 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 Sicherheitspatches) • Wiederherstellungsmaßnahmen innerhalb 1 Stunde (BIA-IT: Stufe 1). Dazu sind geeignete Maßnahmen zu implementieren.

5.2. Korrekte Verarbeitung in Anwendungen

Die Sicherheit von IT-Systemen ist durch die Implementierung der Maßnahmen aus den konzernweit geltenden Standards zur Systementwicklung IT-PEP sicherzustellen. Hierfür steht eine für AUDI BRUSSELS adaptierte Version des IT-PEP zur Verfügung.

Für alle Beratungstätigkeiten zur Einführung von IT-Systemen gelten die Regelungen und betriebsinternen Vereinbarungen von AUDI BRUSSELS (siehe Anhang, B.1.3).

5.3. Kryptographische Maßnahmen

Grundlegende Entscheidungen zur Strategie, Verwendung und dem Umgang mit kryptographischen Methoden sind durch die zuständigen Stellen (siehe Anhang, B.1.4) zu treffen.

Die Vorgaben der Regelung zu Kryptographie[4] sind zu befolgen. Es dürfen ausschließlich die darin festgelegten Methoden verwendet werden.

5.4. Sicherheit von Systemdateien

5.4.1. Schutz von Test-Daten

Entwicklungs-, Test- und produktive IT-Systeme sind voneinander zu trennen.

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

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

Wenn Einzelpersonen Zugriff auf personenbezogene, vertrauliche oder geheime Daten erhalten, die sie nicht zur Ausführung ihrer vertraglichen Tätigkeiten benötigen, müssen die Daten so unkenntlich

[4] Regelung 03.01.02 Kryptographie

gemacht werden, dass die Originaldaten nicht identifizierbar sind, bevor sie vom produktiven IT-System in die Testumgebung 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.

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 Testsystemen zu implementieren, wenn Kopien der produktiven Daten genutzt werden.

5.4.2. Zugangskontrolle zu Quellcode

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

5.5. Sicherheit bei 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 vorgenommen, sind deren Auswirkungen auf vorhandene Regelungen und Sicherheitsmaßnahmen zu ermitteln. Eine Änderung darf nur durchgeführt werden, wenn sie laut Lizenzen und Wartungsverträgen gestattet ist.

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.

Bei Fragen zu länderspezifischen Bestimmungen sind die zuständigen Stellen (siehe Anhang, B.1.5) zu kontaktieren.

II. Verantwortlichkeiten

Verstöße gegen die Handlungsleitlinien werden individuell nach geltenden betrieblichen und rechtlichen Vorschriften und Vereinbarungen geprüft und entsprechend geahndet.

Abweichungen von dieser Handlungsleitlinie, die das Sicherheitsniveau beeinträchtigen, sind nur temporär und nach Rücksprache mit den zuständigen Stellen (siehe Anhang, B.1.6) gestattet.

Anhang

A Allgemeines

A.1 Gültigkeit

Diese Regelung tritt zum Zeitpunkt der Veröffentlichung in Kraft.

Nächster Überprüfungstermin: 01.10.2023

A.2 Abkürzungen und Definitionen

Abkürzung/ Bezeichnung	**Erklärung**
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 Systemarchitect • Softwarearchitect • IT Systementwickler • Softwareentwickler • Applicationsentwickler • Programmierer • Tester

A.3 Dokumentenhistorie

Version	**Name**	**OE**	**Datum**	**Bemerkung**
2.0	Hernot, Annick	B/F-R	31.03.2017	Freigabe
3.0	Hernot, Annick	B/F-R	30.04.2020	Review
4.0	Walter, Andreas	B/FP	01.10.2020	Review, Änderung Herausgeber

B Spezifische Ausprägungen

B.1 Unternehmensspezifisch

B.1.1 Die Bekanntgabe von Informationen hinsichtlich Änderungen bzw. Aktualisierungen erfolgen ausschließlich über das Audi mynet.

B.1.2 LISSC (Local Information Steering Committee) via ISB (Informationssicherheitsbeauftragten)

B.1.3 Prozessstandard IT-PEP und URLB_065 IT-Steuerung

B.1.4 IT-Sicherheit (B/FP)

B.1.5 Rechtsservice (B/F-R)

B.1.6 IT-Sicherheit (B/FP)