Informationssicherheitshandlungsleitlinien für Systementwickler_innen

Gültig ab:	20.10.2006	Status	Veröffentlicht
Geändert am:	01.03.2022	Version:	5.0
Herausgeber:	I/FL-81, Datenschutz- / Datensicherheits-management, Office des DSB	Regelung Nr.	02.04

Geltungsbereich
Die Handlungsleitlinien gelten für die AUDI AG und sind im gesamten Audi Konzern anzuwenden und durch konkrete IT-Regelungen im Einzelfall auszugestalten.

Inhaltsverzeichnis

I. Zweck

In dieser Informationssicherheitshandlungsleitlinie werden die organisatorischen Vorgaben und Regeln für die Informationssicherheit definiert, die von IT-Systementwickler_innen (siehe Anhang. A.3) in ihrem Zuständigkeitsbereich für IT-Systeme und die IT-Infrastruktur zu befolgen sind.

Darüber hinaus gilt für die Zielgruppe der IT-Systementwickler_innen die Informationssicherheitshandlungsleitlinie für Beschäftigte bzw. für Dritte, sofern der_die IT-Systementwickler_in Beschäftigter einer Partnerfirma ist. Systementwickler_innen müssen sich über alle (rollenspezifischen) Vorgaben informieren und diese einhalten, wenn sie in zusätzlichen Rollen arbeiten.

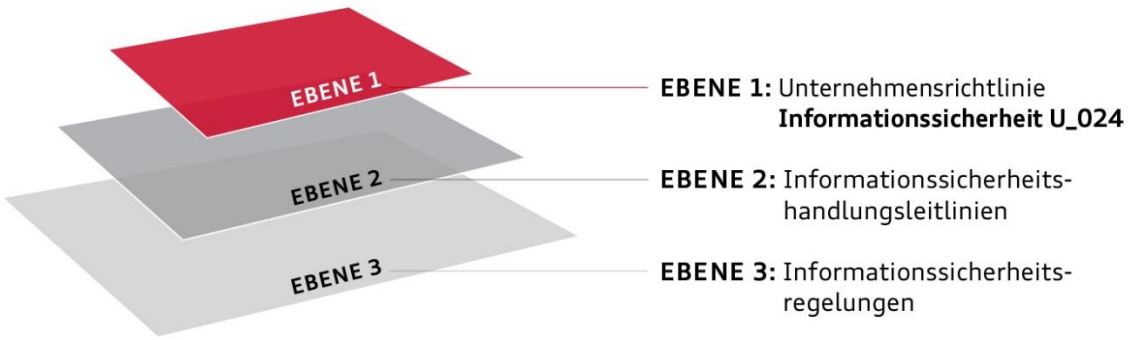
Zweck dieser Informationssicherheitshandlungsleitlinie ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Schutz der Rechte und Interessen der Gesellschaft und aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit einer Konzerngesellschaft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



Informationssicherheitsregelwerk

Ebene 1 Informationssicherheit U_024
Definiert die grundlegenden Ziele, Strategien und Verantwortlichkeiten zur Gewährleistung eines Mindestniveaus der Informationssicherheit.

Ebene 2 Informationssicherheitshandlungsleitlinien:
Ausgestaltung der U_024 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_die jeweilige Informationseigentümer_in. 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, B.1.2). Dabei sind die Vorgaben aus der Regelung (siehe Anhang, A.1.1) 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 Informationseigentümer_innen 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 Authentifizierungsinformationen, Integritätsprüfungen) vor unbefugten Zugriffen und Änderungen zu schützen.

4. Zugangskontrolle

Für den Zugriff auf Informationen sind, auf Grundlage einer durch den_die Informationseigentümer_in 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 (wie z. B. TLS) verwendet werden.

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

5. Beschaffung, Entwicklung und Wartung von Informationssystemen

5.1. Sicherheitsanforderungen für IT-Systeme

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 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 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	• IT-Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Need to know " • Zwei-Faktor-Authentifizierung (z. B. Smartcard mit PIN), insbesondere für den Zugriff auf Anwendungen • Transportverschlüsselung • Ablageverschlüsselung

5.1.2. 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	• 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 mit PIN) für Schreibzugriffe • Generierung und Verifizierung von digitalen Signaturen für gespeicherte Daten, bzw. vergleichbare Sicherheitsmaßnahmen • 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) • 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, B.1.3).

5.3. Kryptographische Maßnahmen

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

Die Vorgaben der Regelung (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_die Informationseigentümer_in 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 Test- und Entwicklungssystemen zu implementieren und den vorgesehenen testenden Personen zuzuweisen, 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 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.

II. Verantwortlichkeiten

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.1.5) gestattet.

Anhang

A Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheitsregelung Nr. 03.01.16 Dienstleistungserbringung durch Dritte

A.1.2 Informationssicherheitsregelung Nr. 03.01.05 IAM

A.1.3 Informationssicherheitsregelung Nr. 03.01.02 Kryptographie

A.1.4 Glossar für Informationssicherheitshandlungsleitlinien

https://portal.epp.audi.vwg/wps/poc?uri=audi-np:oid:1551257182834@oid:Z7_3Q9IGGC000C870QI440ST620E7&epp-media=/content/aepc/mynet/de/2682/628/_jcr_content.download.pdf/d2233326-ec47-4a6d-9f75-551fb7bbbeb4/it-sec_2_glossar_fuer_sicherheitshandlungsleitlinien_audi.pdf

A.2 Gültigkeit

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

Nächster Überprüfungstermin: 01.03.2025

A.3 Abkürzungen und Definitionen

Abkürzung/ Bezeichnung	**Erklärung**
IT-Systementwickler_in	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_in • IT Systemarchitekt_in • Softwarearchitekt_in • Systementwickler_in • IT-Softwareentwickler_in • Applikationsentwickler_in • Programmierer_in • Tester_in

A.4 Dokumentenhistorie

Version	**Name**	**OE**	**Datum**	**Bemerkung**
2.0	Fröhlich	I/GA-2	12.03.2013	Versionsfreigabe
3.0	Fröhlich	I/GG-81	24.10.2016	Überarbeitung
4.0	Fröhlich	I/GG-81	25.07.2018	Umbenennung IT-Sicherheitsregelwerk in Informationssicherheitsregelwerk; Neuordnung Schutzziele
5.0	Fröhlich	I/FL-81	01.03.2022	Überarbeitung

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 Verantwortlichkeit: Organisationseinheit (OE) IT Sicherheit.

B.1.3 IT-Systeme, die mitbestimmungspflichtige Tatbestände beinhalten, sind in den BR-IT-Ausschüssen zu beraten.

B.1.4 Verantwortlichkeit: Organisationseinheit (OE) IT Sicherheit

B.1.5 Verantwortlichkeit: OE Datenschutz- / Datensicherheitsmanagement, Office des DSB