Informationssicherheitshandlungsleitlinien für Systembetreiber_innen und Administrator_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.	02.03

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

Inhaltsverzeichnis

I. Zweck

In dieser Informationssicherheitshandlungsleitlinie werden die Regeln für die Informationssicherheit definiert, die von Systembetreiber_innen und Administrator_innen 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.1.1).

Darüber hinaus gilt für die Zielgruppe der Systembetreiber_innen und Administrator_innen die Informationssicherheitshandlungsleitline für Beschäftigte bzw. für Dritte, sofern der_die Systembetreiber_in oder Administrator_in Beschäftigter einer Partnerfirma ist.

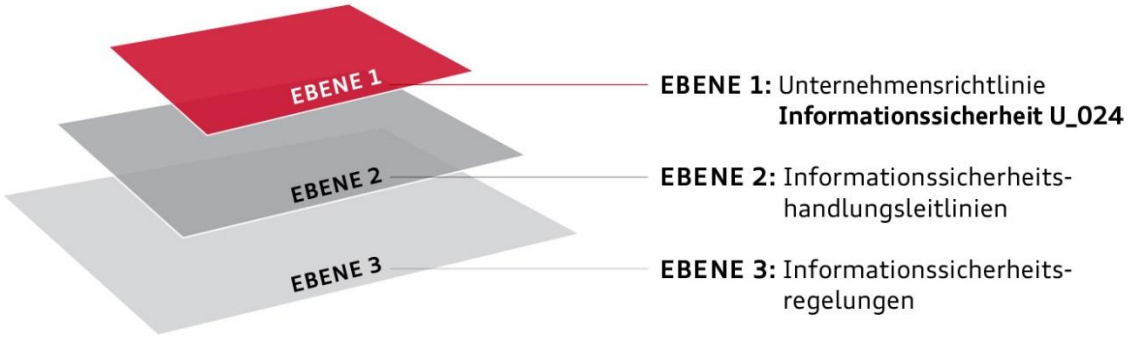
Zweck dieser Informationssicherheitshandlungsleitlinie ist der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Schutz der Rechte und Interessen des Gesellschaft und aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit einer Konzerngesellschaft 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.1.2).

1. Kontext

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



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

Alle unternehmenseigenen IT-Systeme (siehe Anhang, B.1.3) 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_die jeweilige Informationseigentümer_in. 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
- 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_in

3. Physische Sicherheit und Umgebungssicherheit

Geschäftskritische IT-Systeme müssen gegen Stromausfälle geschützt werden (z. B. mithilfe einer unterbrechungsfreien Stromversorgung).

Der_die Systembetreiber_in 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.:

- Wartung von IT-Geräten entsprechend den Herstellervorgaben
- Betrieb von IT-Geräten entsprechend den Spezifikationen der Hersteller_innen (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 Verantwortlichkeiten

4.1.1. Dokumentierte Betriebsverfahren

Der_die Systembetreiber_in 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, B.1.4). Der_die Systembetreiber_in 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.1.1) sind zu befolgen.

4.1.3. Aufgabentrennung

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

Darüber hinaus sind Aufgaben aufzuteilen, falls andernfalls ein erhöhtes Risiko für absichtlichen oder versehentlichen Missbrauch auf Kosten des Konzerns bestünde („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 Produktionsanlagen, bei denen dies nicht ohne übermäßigen 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_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.

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.1.5). Dabei sind die Vorgaben aus Regelung (siehe Anhang, A.1.3) 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 Informationseigentümer_innen zu spezifizieren. Zur Inbetriebnahme

neuer IT-Systeme ist eine dokumentierte und durchgeführte Übergabe an den_die Systembetreiber_in durchzuführen.

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.1.6) 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.1.4).

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.1.5) 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 Nutzenden auf IT-Systeme, die als „geheim“ klassifizierte Informationen verarbeiten, muss protokolliert werden. Die Protokolle (Logs) sind entsprechend der betrieblichen Regelungen der Gesellschaft aufzubewahren (siehe Anhang, A.1.2).

Folgende Inhalte müssen Protokolle mindestens enthalten:

- 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 Informations-Sicherheitsvorfällen zu prüfen.

Bei der Prüfung von Protokollen sind die erforderlichen Genehmigungsverfahren zu befolgen (siehe Anhang, B.1.7).

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. Systemadministrator_innen 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, die der_die Informationseigentümer_in dazu berechtigt hat.

4.9.4. Administrator- und Betreiberprotokolle

Alle Tätigkeiten von Administrator_innen und Systembetreiber_innen 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_innen 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_innen zum Zwecke der Fehlerbehebung unternehmen, sind zu dokumentieren.

4.9.6. Zeitsynchronisation

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

5. Zugriffskontrolle

5.1. Geschäftsanforderungen für die Zugriffskontrolle

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

Die durch den_die Informationseigentümer_in 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_die Informationseigentümer_in („Vier-Augen-Prinzip“) bewilligt werden. Ausnahmen sind zentrale Dienste (z. B. das Intranet). Die Delegation der 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 zu welchem Zeitpunkt an wen verteilt wurden.
- Für diese Dokumentation gelten dieselben Aufbewahrungsfristen wie für die Aufbewahrung von Benutzeranträgen.

Es sind Vorgehensweisen für die Vergabe 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 werden, sind zu sperren.

Für Passwörtern 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).

- 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 Nutzende 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 Nutzenden mit privilegierten Rechten

5.3.1. Allgemeine Vorgaben

Folgende Vorgaben sind durch alle Systembetreiber_innen und Administrator_innen zu befolgen:

- Die Vorgaben aus der Informationssicherheitshandlungsleitlinie für Beschäftigte (Umgang mit Passwörtern) bzw. für Dritte, sofern der_die Systembetreiber_in oder Administrator_in 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 Nutzenden zugewiesen werden, die die obligatorische Schulung zur Informationssicherheitssensibilisierung für Administrator_innen (siehe Anhang, A.1.6) abgelegt haben.

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 Konten

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_der individuellen Administrator_in 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, B.1.8) sind zu befolgen.

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

- Wartung und Fehlerbehebung
- Verwaltung von Zugriffsrechten für Nutzende in der eigenen Organisationseinheit für den Zugriff auf Daten der eigenen Organisationseinheit. Für die Vergabe von Zugriffsrechten für Daten der eigenen Organisationseinheit an Nutzende, 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 Kund_innen (z. B. zur Fehlerbehebung) ist die vorherige Genehmigung durch den zuständigen Nutzenden 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 Administrator_innen ohne Genehmigung durch die Führungskraft
- 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 Nutzenden, 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, B.1.7).
- Erstellen von lokalen Konten

5.4. Netzwerkzugriffskontrolle

Nur angemeldete und berechtigte Nutzende dürfen Zugriff auf das konzerninterne Netzwerk erhalten. Die Vorgaben aus der Regelung (siehe Anhang, A.1.7) sind zu befolgen.

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.1.7) 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 Regelung (siehe Anhang, A.1.8).

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 Nutzende beschränkt werden.

Der_die IT-Systemverantwortliche 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 Authentisierung

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, B.1.9) 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 IAM-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 Nutzende 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.

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 von der zuständigen Stelle (siehe Anhang B.1.10) durchzuführen.
- Es muss ein Nachweis über das sichere Löschen verwahrt werden.
- Zum sicheren Löschen dürfen nur genehmigte Werkzeuge verwendet werden (siehe Anhang B.1.11).

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_die Hersteller_in 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 Informations-Sicherheitsmaßnahmen zu identifizieren und zu implementieren (z. B. IT-Systemhärtung oder Patch-Management).

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.

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.1.9) sind einzuhalten.

6.3. Sicherheit von Systemdateien

6.3.1. Kontrolle von betrieblicher Software

Software darf ausschließlich durch berechtigte Beschäftigte installiert werden (siehe Anhang, B.1.12).

Neue oder geänderte Programme dürfen erst in laufenden Systemen eingesetzt werden, wenn sie entsprechend den gültigen Changemanagement-Prozessen (siehe Anhang, A.1.1) erfolgreich getestet und freigegeben wurden. Die Version bzw. der Status der Korrektur der verwendeten Software ist entsprechend den unternehmensspezifischen Regelungen (siehe Anhang, B.1.13) zu dokumentieren und zu archivieren.

6.3.2. Zugangskontrolle zu Quellcode

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

6.4. Sicherheit bei Entwicklungs- und Unterstützungsprozessen

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.1.1) 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 die Geschäftskontinuität, wie in der Regelung (siehe Anhang, A.1.10) beschrieben, sichergestellt werden kann.

8. Compliance und Einhaltung von 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. Dies gilt insbesondere bei der Nutzung im Ausland.

Bei Fragen zu länderspezifischen Bestimmungen sind die entsprechenden Stellen zu kontaktieren (siehe Anhang, B.1.14).

Es sind zufällige Stichprobenprüfungen für ihre IT-Systeme durchzuführen, 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, B.1.7).

In IT-Systemen entdeckte Sicherheitslücken sind 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.

II. Verantwortlichkeiten

Bei mitbestimmungspflichtigen Sachverhalten ist die Einbindung der betriebsverfassungsrechtlichen Gremien sicherzustellen.

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

Abweichungen von dieser Handlungsleitline, die das Sicherheitsniveau senken, sind nur temporär und nach Rücksprache mit den zuständigen Stellen (siehe Anhang, B.1.15) gestattet.

Anhang

A Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheitsregelung Nr. 03.01.08 Change und Patch Management

A.1.2 Informationssicherheitsregelung Nr. 03.01.05 IAM

A.1.3 Informationssicherheitsregelung Nr. 03.01.16 Dienstleistung durch Dritte

A.1.4 Informationssicherheitsregelung Nr. 03.01.01 Anti-Malware und Systemschutz

A.1.5 Informationssicherheitsregelung Nr. 03.01.06 Backup und Archivierung

A.1.6 Informationssicherheitsregelung Nr. 03.01.10 Awareness und Schulung

A.1.7 Informationssicherheitsregelung Nr. 03.02.04 Netzwerkzugänge

A.1.8 Informationssicherheitsregelung Nr. 03.02.02 Trennung und Zonierung

A.1.9 Informationssicherheitsregelung Nr. 03.01.02 Kryptographie

A.1.10 Informationssicherheitsregelung Nr. 03.01.14 IT Service Continuity Management

A.1.11 Glossar für Informationssicherheitshandlungsleitlinien

https://portal.epp.audi.vwg/wps/poc?uri=audi-np:oid:1551257182834@oid:Z7_3Q9IGGC0O0C870QI440ST620E7&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.

Nächster Überprüfungstermin: 01.03.2025

A.3 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 Speicherprogrammierbare Steuerungen (SPS) und Robotersteuerungen sind in verschließbaren Schränken aufzubewahren oder durch entsprechende anderweitige geeignete Maßnahmen zu sichern. Der Zugang ist nur Berechtigten zu ermöglichen.

Speicherprogrammierbare Steuerungen (SPS) und Robotersteuerungen sind in Netzen zu betreiben, in denen nur die Kommunikation erlaubt ist, die für den Betrieb unbedingt erforderlich ist.

B.1.2 Die Bekanntgabe von Informationen hinsichtlich Änderungen bzw. Aktualisierungen erfolgen ausschließlich über das Audi mynet.

B.1.3 Ein IT-System ist ein Gesamtsystem bestehend aus sämtlichen Hardware- und Software-Komponenten inklusive deren Kommunikationsbeziehungen untereinander.

B.1.4 Die Dokumentation ist gemäß U_014 „Unterlagen: Umgang und Aufbewahrung“ zu archivieren.

B.1.5 Verantwortlichkeit: Organisationseinheit (OE) IT Security

B.1.6 Die Freigabe von Virenschutzsoftware erfolgt durch das Anti Virus Emergency Response Team (AVERT).

B.1.7 Personenbezogene Audits sind schriftlich vom_von der Beauftragten für den Datenschutz genehmigen zu lassen. Die Einbindung der zuständigen Personalleitung und des Betriebsrats ist sicherzustellen.

B.1.8 Passwörter für Administrator-Konten müssen sicher verwaltet werden (z. B. Password Vault).

B.1.9 Verantwortlichkeit: Organisationseinheit (OE) IT Security

B.1.10 Das sichere Löschen bzw. Verschrotten von Speichermedien erfolgt durch IT Client Services.

B.1.11 z. B. das Programm „Blancco“

B.1.12 Verantwortlichkeit: Beschäftigte, die aufgrund ihrer definierten Aufgabenstellung, Installationsrechte genehmigt erhalten haben, z. B. OfficeServices, CAT-Shop, Keyuser

B.1.13 Die Versions-/Korrekturstände sind gemäß U_014 „Unterlagen: Umgang und Aufbewahrung“ zu archivieren.

B.1.14 Verantwortlichkeit: OE Zentraler Rechtsservice.

B.1.15 Verantwortlichkeit: Organisationseinheit (OE) Datenschutz- / Datensicherheitsmanagement, Office des DSB