Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren

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 ... 3
1. Kontext ... 3
2. Organisation der Informationssicherheit ... 3
3. Asset-Management ... 4
4. Physische und Umgebungssicherheit ... 4
5. Betriebs- und Kommunikationsmanagement ... 4
5.1. Betriebliche Verfahren und Verantwortlichkeiten ... 4
5.1.1. Dokumentierte Betriebsprozesse ... 4
5.1.2. Änderungsmanagement ... 4
5.1.3. Aufgabentrennung ... 5
5.1.4. Trennung von Entwicklungs-, Test- und Produktiveinrichtungen ... 5
5.2. Serviceerbringung durch Dritte ... 5
5.3. Systemplanung und Abnahme ... 5
5.4. Schutz vor Schadsoftware und Mobile Code ... 5
5.5. Datensicherung ... 6
5.6. Netzwerksicherheitsmanagement ... 6
5.7. Elektronische Mitteilungen/Nachrichten (Messaging) ... 6
5.8. Öffentlich verfügbare Informationen ... 6
5.9. Überwachung ... 6
5.9.1. Auditprotokolle ... 6
5.9.2. Überwachung der Systemnutzung ... 6
5.9.3. Schutz von Protokollinformationen ... 6
5.9.4. Administrator- und Betreiberprotokolle ... 7
5.9.5. Fehlerprotokolle ... 7

5.9.6. Zeitsynchronisation ... 7
6. Zugriffskontrolle ... 7
6.1. Geschäftsanforderungen für die Zugriffskontrolle ... 7
6.2. Benutzerverwaltung ... 7
6.3. Pflichten von Nutzern ... 8
6.3.1. Allgemeine Anforderungen ... 8
6.3.2. Generierung von Passwörtern (persönliche Administrator-Konten und systembezogene Konten) ... 8
6.3.2.1. Persönliche Administrator-Konten ... 9
6.3.2.2. Systembezogene Konten ... 9
6.3.3. Verwendung von Administrator-Konten ... 9
6.4. Netzwerkzugriffskontrolle ... 10
6.5. Zugriffskontrolle auf Betriebssysteme ... 10
6.5.1. Sichere Anmeldeverfahren ... 10
6.5.2. Benutzeridentifikation und Authentisierung ... 10
6.5.3. Systeme zur Verwaltung von Passwörtern ... 10
6.5.4. Verwendung von Systemwerkzeugen ... 10
6.5.5. Session Time-out ... 11
6.5.6. Sicheres Löschen von Datenträgern ... 11
6.6. Mobile Computing und Telearbeit ... 11
7. Beschaffung, Entwicklung und Wartung von Informationssystemen ... 12
7.1. Sicherheitsanforderungen von Informationssystemen ... 12
7.1.1. Schutz der Vertraulichkeit ... 12
7.1.2. Schutz der Integrität ... 12
7.1.3. Schutz der Verfügbarkeit ... 13
7.2. Kryptographische Maßnahmen ... 13
7.3. Sicherheit von Systemdateien ... 13
7.3.1. Kontrolle von Software im Betrieb ... 13
7.3.2. Zugangskontrolle zu Quellcode ... 13
7.4. Sicherheit bei Entwicklungs- und Unterstützungsprozessen ... 13
7.5. Umgang mit Patches und Schwachstellen ... 14
8. Sicherstellung des Geschäftsbetriebs (Business Continuity Management) ... 14
9. Einhaltung von Vorgaben ... 15
II. Verantwortlichkeiten ... 15
Anhang 16
A Allgemeines ... 16
A.1 Gültigkeit ... 16
A.2 Dokumentenhistorie ... 16
B Spezifische Ausprägungen ... 16
B.1 Unternehmensspezifisch ... 16

I. Zweck

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

In dieser Informationssicherheitshandlungsleitlinie werden die organisatorischen Vorgaben und die Regeln für die Informationssicherheit definiert, die von den Systembetreibern und Administratoren beim Umgang mit Informationen und IT-Geräten (z. B. PCs, Workstations, Laptops, Smartphones oder Tablet-PCs) zu befolgen sind. Für den Schutz von Speicherprogrammierbaren Steuerungen (SPS) und Robotersteuerungen gelten innerhalb dieser Handlungsleitlinien die Regelungen im Anhang, B.1.1.

Darüber hinaus gilt für die Zielgruppe der Systembetreiber und Administratoren die Informationssicherheitshandlungsleitlinie für Mitarbeiterinnen und Mitarbeiter.

Zweck der Informationssicherheitshandlungsleitlinien sind der Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sowie der Schutz der Rechte und Interessen des Unternehmens und aller natürlichen und juristischen Personen, die eine Geschäftsbeziehung mit AUDI BRUSSELS eingehen und/oder Tätigkeiten für AUDI BRUSSELS ausführen.

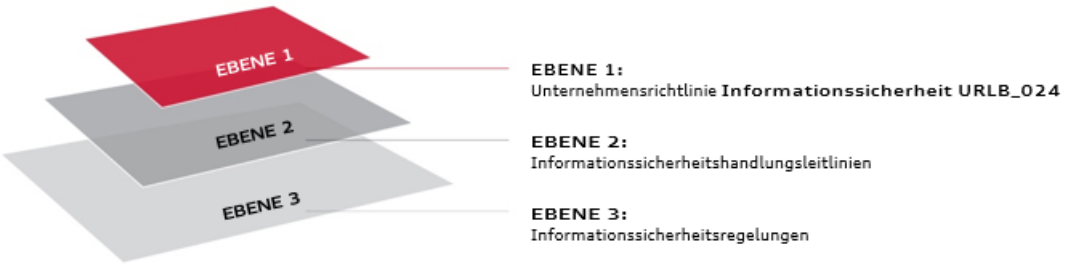
Die Inhalte dieses Dokuments basieren auf der internationalen Norm ISO/IEC 27002:2013.

Dieses Dokument und alle zugehörigen Änderungs- und Aktualisierungsmitteilungen werden über die üblichen Verteilwege kommuniziert (siehe Anhang B.1.2).

Die Pflichten der Revisionsabteilung des Konzerns sind nicht Teil dieser Regelung.

1. Kontext

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



Informationssicherheitsregelwerk

2. Organisation der Informationssicherheit

Bevor Partnerunternehmen eine Verbindung mit dem Konzernnetz herstellen, müssen sie eine unterzeichnete Geheimhaltungsvereinbarung (siehe Anhang, B.1.3) sowie ein gültiges Sicherheitszertifikat (z. B. in Übereinstimmung mit einer Selbstbewertung, die auf der Informationssicherheitsbewertung (Information Security Assessment, ISA) des Verbands der Automobilindustrie (VDA) basiert) vorlegen. Die entsprechenden Nachweise müssen vom auftraggebenden Fachbereich angefordert werden.

3. Asset-Management

Alle IT-Systeme (siehe Anhang, B.1.4) 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.

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 (Application Owner / LCM)
- die Geschäftsprozesse, denen die IT-Systeme zugeordnet sind
- Betriebsstandort (z. B. Rechenzentrum)
- Geschäftsprozess-Zugehörigkeit
- Klassifizierung von Daten sowie, falls erforderlich, Hinweise zu spezifischen Schutzanforderungen und Schutzmaßnahmen
- Existenz personenbezogener Daten
- Informationseigentümer
- Business Process Owner

4. Physische und Umgebungssicherheit

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

Strom- und Telekommunikationsleitungen, die zur Übermittlung von Daten bzw. zur Stromversorgung von Informationssystemen dienen, müssen mit geeigneten Maßnahmen vor Unterbrechung und Beschädigung geschützt werden. Dazu zählt auch die Zugriffskontrolle für Verteilerschränke.

Der Systembetreiber sorgt 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 (z. B. Temperatur, Luftfeuchtigkeit)
- Schutz von IT-Geräten vor unbefugtem Zugriff, Manipulation, Beschädigung oder schädlichen Umgebungsbedingungen (z. B. Feuer, Wasser, Schmutzbelastung)

5. Betriebs- und Kommunikationsmanagement

5.1. Betriebliche Verfahren und Verantwortlichkeiten

5.1.1. Dokumentierte Betriebsprozesse

Der Systembetreiber ist dafür verantwortlich, dass alle für den Betrieb von IT-Systemen erforderlichen Anleitungen (z. B. Handbücher, betriebliche Service-Handbücher, Funktionshandbücher), 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.1.5). Der Systembetreiber ist verpflichtet, die festgelegten betrieblichen Verfahren zu befolgen (z. B. zum Change-Prozess).

5.1.2. Änderungsmanagement

Änderungen an laufenden IT-Systemen sind vor ihrer Implementierung in diesen Systemen im Rahmen eines festgelegten Prozesses zu planen, zu testen, freizugeben und zu dokumentieren. Die Vorgaben aus der Regelung für das Patchmanagement[1] sind zu befolgen.

[1] Regelung Nr. 03.01.08 Change- und Patchmanagement

5.1.3. Aufgabentrennung

Der Einsatz unterschiedlicher Mitarbeiter 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 von AUDI BRUSSELS bestünde („Zwei-Personen-Regel“).

Vor der Implementierung von Software sind sämtliche Zuständigkeiten zu definieren (u. a. Zuständigkeit für Produktentwicklung, Spezifikationen, Produktauswahl, Tests, Freigabe, Installation und Betrieb).

5.1.4. Trennung von Entwicklungs-, Test- und Produktiveinrichtungen

Entwicklungsumgebungen, Testumgebungen und laufende IT-Systeme sind voneinander zu trennen. Eine Ausnahme sind Produktionsanlagen, bei denen dies nicht ohne übermäßigen Aufwand möglich wäre.

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

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

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

5.2. Serviceerbringung durch Dritte

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.1.6). Dabei sind die Vorgaben aus Regelung 03.01.16 Dienstleistungserbringung durch Dritte zu befolgen.

5.3. 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 Informationseigentümern zu spezifizieren. Zur Inbetriebnahme neuer IT-Systeme ist eine dokumentierte und durchgeführte Übergabe an den Systembetreiber durchzuführen.

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.

5.4. Schutz vor Schadsoftware und Mobile Code

Werden IT-Geräte mit Schadcode (Malware) infiziert, sind sie unter Abschätzung möglicher Auswirkungen (z. B. Produktionsausfälle) vom Netzwerk zu trennen.

IT-Geräte und IT-Systeme sind mithilfe von Antivirus-Software oder anderen Schutzmaßnahmen, die durch die zuständige Stelle (siehe Anhang, B.1.7) genehmigt wurden, vor Schadsoftware zu schützen. Die jeweiligen Schutzmaßnahmen sind zu dokumentieren und auf dem aktuellen Stand zu halten.

5.5. Datensicherung

Alle Betreiber von IT-Systemen müssen für ausreichende Datensicherungen sorgen, damit eine gegebenenfalls erforderliche Wiederherstellung von Informationen in einem angemessenen Zeitrahmen möglich ist. Die Vorgaben aus der Regelung für Datensicherungen sind zu befolgen.[2]

5.6. Netzwerksicherheitsmanagement

Nach der Installation von Netzwerkkomponenten (z. B. Router) sind umgehend deren systemspezifische Schutzfunktionen (z. B. Passwortschutz) zu aktivieren.

Alle aktiven Netzwerkkomponenten sind mithilfe eines Managementsystems zentral zu verwalten und zu überwachen, um Fehler oder kritische Ereignisse rechtzeitig erkennen zu können.

5.7. Elektronische Mitteilungen/Nachrichten (Messaging)

Der Systemeigentümer ist für die Zuverlässigkeit von Kommunikationsdiensten (z. B. E-Mail) verantwortlich. Für E-Mail-Services ist Folgendes zu gewährleisten:

- Verantwortlichkeit des E-Mail-Absenders
- Systemgenerierte E-Mails müssen einer verantwortlichen Person zugeordnet werden können.
- E-Mail-Postfächer sind vor unbefugtem Zugriff zu schützen.

5.8. Öffentlich verfügbare Informationen

Für den Zugriff aus öffentlich erreichbaren IT-Systemen auf interne Netzwerke dürfen ausschließlich sichere Gateway-Komponenten verwendet werden.

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

Auf Server-Seite (nicht auf Client-Seite) müssen Integritätsprüfungen durchgeführt werden.

5.9. Überwachung

5.9.1. Auditprotokolle

Der Zugriff von Nutzern auf IT-Systeme, die geheime Informationen enthalten, muss protokolliert werden. Die Protokolle sind entsprechend der betrieblichen Regelungen der Gesellschaft aufzubewahren.

Folgende Inhalte müssen Protokolle mindestens enthalten:

- eindeutige Identifizierung der protokollierten Person (z. B. Name oder ID)
- Protokoll der Zugriffsversuche auf das System
- Protokoll der Zugriffe auf Daten und andere Ressourcen

5.9.2. Überwachung der Systemnutzung

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.1.8).

5.9.3. 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. Systemadministratoren dürfen die Protokollierung nicht unbemerkt deaktivieren können.

[2] Regelung 03.01.06 Backup und Archivierung

Falls in Protokollen geheime 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 Informationseigentümer dazu berechtigt hat.

5.9.4. Administrator- und Betreiberprotokolle

Alle Tätigkeiten von Systembetreibern in IT-Systemen, die vertrauliche oder geheime Informationen enthalten, müssen protokolliert werden.

Mindestens für IT-Systeme, in denen geheime Informationen verarbeitet werden, müssen Aktivitätsprotokolle der Systembetreiber so gespeichert werden, dass auch Personen mit erweiterten Zugriffsrechten die Protokollinformationen nicht ändern oder löschen können.

Folgende Inhalte müssen Protokolle mindestens enthalten:

- eindeutige Identifizierung der protokollierten Person (z. B. Name oder ID)
- Beginn und Ende der Aktivität im IT-System
- Grund für die Aktivität (z. B. Systemfehler, Änderungen, Aktualisierungen)
- vorgenommene Tätigkeiten

5.9.5. Fehlerprotokolle

Alle durch Nutzer gemeldete Fehler und Funktionsstörungen sind zu protokollieren. Alle Maßnahmen, die Betreiber zum Zwecke der Fehlerbehebung unternehmen, sind zu dokumentieren.

5.9.6. Zeitsynchronisation

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

6. Zugriffskontrolle

6.1. Geschäftsanforderungen für die Zugriffskontrolle

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

Die durch den Informationseigentümer spezifizierten Rollen und Berechtigungen müssen implementiert werden.

Ein Antrag auf Zugriffsrechte für IT-Systeme muss schriftlich unter Verwendung des entsprechenden Formulars bzw. über ein festgelegtes und genehmigtes IT-System erfolgen. 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 Informationseigentümer („Zwei-Personen-Regel“) 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.

6.2. Benutzerverwaltung

Es sind Vorgehensweisen für die Vergabe von Passwörtern und die Verteilung von Identifikationsmitteln (z. B. SmartCards oder SecurID-Karten) zu definieren und zu veröffentlichen.

Nach der Installation eines 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 Nutzerberechtigungen von Mitarbeitern externer Lieferanten/Partnerunternehmen für IT-Systeme auf die Dauer eines Projekts zu beschränken (maximal ein Jahr).

Bei der Generierung von Passwörtern sind die folgenden Mindestanforderungen zu erfüllen (dieses Kapitel gilt nicht für PINs):

- Es muss sichergestellt werden, dass Passwörter bei der ersten Anmeldung an einem System sowie spätestens nach einem Jahr geändert werden.
- 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 Systemen muss sicher verschlüsselt erfolgen. Ist dies nicht möglich, sind Einmalpasswörter zu verwenden.

Für den Umgang mit Passwörtern sind die folgenden Mindestanforderungen zu erfüllen:

- Konten, die mehr als 400 Tage nicht verwendet werden, sind zu sperren.
- Vordefinierte bzw. Standard-Passwörter in Systemen müssen in individuelle Passwörter geändert werden.
- 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.
- Jeder Nutzer muss jederzeit die Möglichkeit haben, sein Passwort zu ändern.
- Passwörter dürfen bei der Eingabe an Bildschirmen nicht als Klartext angezeigt werden.

6.3. Pflichten von Nutzern

6.3.1. Allgemeine Anforderungen

Folgende Vorgaben sind durch alle Systembetreiber und Administratoren zu befolgen:

- Die Vorgaben aus der Informationssicherheitshandlungsleitlinie für Mitarbeiterinnen und Mitarbeiter (Umgang mit Passwörtern) sind zu befolgen.
- Die Vorgaben aus der Passwort-Regelung sind zu befolgen und in Systemen und Anwendungen umzusetzen. In allen Systemen/Anwendungen müssen die Anforderungen an Passwörter aus der Regelung durchgesetzt werden.
- Administrator-IDs dürfen nur für administrative Tätigkeiten verwendet werden. Routinetätigkeiten, für die keine Administratorrechte erforderlich sind, müssen mit Benutzerkennungen mit eingeschränkten Rechten durchgeführt werden.
- Passwörter für Administrator-Konten müssen für alle Konten unterschiedlich sein. Zusätzliche Konten können beispielsweise dann erforderlich sein, wenn Anwendungen oder Systeme nicht an den zentralen Authentifizierungsdienst angeschlossen sind, oder für unterschiedliche Rollen (Nutzer/Administrator).

6.3.2. Generierung von Passwörtern (persönliche Administrator-Konten und 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 Systeme, die vom VW-Konzern bereitgestellt werden, und Systeme, die von Dritten bereitgestellt werden (z. B. Anwendungen, Registrierungsdienste im Internet), generiert werden.

[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.

- Passwörter müssen mindestens einmal jährlich geändert werden.

6.3.2.1. Persönliche Administrator-Konten

Administrator-Konten dürfen ausschließlich Nutzern zugewiesen werden, die die obligatorische Schulung zur Informationssicherheitssensibilisierung für Administratoren[4] abgelegt haben. Diese Schulung ist spätestens nach zwei Jahren zu wiederholen.

Passwörter für persönliche Administrator-Konten mit erweiterten Zugriffsrechten für administrative Tätigkeiten in IT-Systemen müssen aus mindestens 15 Zeichen bestehen und mindestens 3 der folgenden 4 Zeichenarten enthalten:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen

6.3.2.2. Systembezogene Konten

Passwörter für systembezogene Konten zur automatischen Anmeldung an Systemen müssen aus mindestens 16 Zeichen bestehen und mindestens 3 der folgenden 4 Zeichenarten enthalten:

- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen

Die Verfügbarkeit von systembezogenen Passwörtern ist durch die für das System verantwortliche Person zu gewährleisten (z. B. durch das Hinterlegen von Passwörtern).

6.3.3. Verwendung von Administrator-Konten

Administrative Funktionen (wie z. B. die Nutzerverwaltung) dürfen nur für die jeweilige Aufgabe und unter Verantwortung des individuellen Administrators verwendet werden. Administrative Berechtigungen sind entsprechend den Grundsätzen „geringste Berechtigung“ und „Kenntnis nur wenn nötig“ mithilfe von funktions-/rollenspezifischen Profilen zu beschränken.

Es dürfen nur persönliche Administrator-Konten verwendet werden.

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

- Wartung und Fehlerbehebung
- Verwaltung von Zugriffsrechten für Nutzer in der eigenen Organisationseinheit für den Zugriff auf Daten der eigenen Organisationseinheit. Für die Vergabe von Zugriffsrechten für Daten der eigenen Organisationseinheit an Nutzer, 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 Kunden (z. B. zur Fehlerbehebung) ist die vorherige Genehmigung durch den zuständigen Nutzer erforderlich. Für die Installation von Standardsoftware oder Sicherheits-Updates über die zentrale Softwareverteilung ist keine Genehmigung erforderlich.

Folgende administrative Tätigkeiten sind nicht zulässig:

- Entfernen von Nutzergruppen oder Systemkonten zentraler Stellen aus der Gruppe der lokalen Administratoren ohne Genehmigung durch den Vorgesetzten
- 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 Nutzern[5], 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.1.8).

[4] Siehe Regelung 03.01.10 Awareness und Training
[5] Beispiel: das persönliche Netzlaufwerk

- Erstellen von lokalen Konten

6.4. Netzwerkzugriffskontrolle

Nur angemeldete und berechtigte Nutzer dürfen Zugriff auf das konzerninterne Netzwerk erhalten. Die Vorgaben aus der Regelung für den Netzwerkzugriff[6] sind zu befolgen.

Zugriffe auf das Konzernnetz (Intranet) von außerhalb müssen über „Wissen und Besitz" geschützt werden (Beispiel: PKI-Karte, wobei „Wissen" = Kenntnis der PIN und „Besitz" = Eigentum der Karte (Kartenbesitzer)). Datenübertragungen sind durch sichere Verschlüsselung zu schützen. Die Vorgaben aus der Regelung für die Remotezugänge sind zu befolgen.

Im Netzwerk müssen geeignete Maßnahmen zur Identifizierung von Systemen umgesetzt werden.

Alle nicht benötigten Dienste und Ports sind zu deaktivieren.

Es ist eine Risikobewertung zur Ermittlung potentieller Bedrohungen für ein System durchzuführen.

Sämtliche erforderliche Netzwerkkommunikation ist zu dokumentieren.

Jedes System ist in ein Netzwerksegment einzugliedern, welches das erforderliche Sicherheitsniveau bietet. Details hierzu finden sich in der Regelung für Trennung und Zonierung[7].

6.5. Zugriffskontrolle auf Betriebssysteme

6.5.1. Sichere Anmeldeverfahren

Der Zugriff auf IT-Systeme, die nicht-öffentliche Daten enthalten, muss durch geeignete Mittel (z. B. Authentifizierung) abgesichert und auf berechtigte Nutzer beschränkt werden.

Der Systembetreiber ist verantwortlich für die Implementierung sicherer Anmeldeverfahren (z. B. starke Authentifizierung mittels PKI-Karte) entsprechend der jeweiligen Datenklassifizierung.

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).

Soweit technisch machbar, müssen Konten nach 5 fehlgeschlagenen Anmeldeversuchen gesperrt werden. Außerdem ist eine Passworthistorie von mindestens 5 Passwörtern einzurichten und die Mindestanforderungen an Passwörter sind umzusetzen.

6.5.2. Benutzeridentifikation und Authentisierung

Soweit technisch machbar, muss für administrative Aufgaben eine starke Authentifizierung eingerichtet werden (Zwei-Faktor-Authentifizierung über „Wissen und Besitz"). 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.

6.5.3. Systeme zur Verwaltung von Passwörtern

Die für die jeweiligen Systeme zuständigen Personen müssen die in der Passwort-Regelung[8] festgelegten Mindestanforderungen an Passwörter umsetzen.

6.5.4. Verwendung von Systemwerkzeugen

Es müssen geeignete Maßnahmen (z. B. Entzug entsprechender Berechtigungen) getroffen werden, um zu verhindern, dass unbefugte Nutzer sicherheitsrelevante System- und Anwendungseinstellungen (beispielsweise über Systemwerkzeuge) ändern können.

[6] Regelung Nr. 03.02.04 Netzwerkzugänge
[7] Regelung Nr. 03.01.19 Virtualisierung
[8] Regelung 03.01.05 Authentifizierung und IAM

6.5.5. Session Time-out

Dialogsitzungen, die nach einem längeren Zeitraum nicht mehr aktiv verwendet werden, müssen deaktiviert oder durch geeignete Mittel geschützt werden.

6.5.6. 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 durchzuführen.
- Es muss ein Nachweis über das sichere Löschen verwahrt werden.
- Zum sicheren Löschen dürfen nur genehmigte Werkzeuge verwendet werden).

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 Hersteller 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.

6.6. Mobile Computing und Telearbeit

Durch das Unternehmen bereitgestellte IT-Geräte dürfen nur dann mit externen Netzwerken verbunden werden (z. B. öffentliche Hotspots oder private WLAN-Netze), wenn dadurch eine Verbindung mit dem Konzernnetzwerk hergestellt werden soll. Dies darf nur für die Dauer der Verbindung mit dem Konzernnetzwerk geschehen.

7. Beschaffung, Entwicklung und Wartung von Informationssystemen

7.1. Sicherheitsanforderungen von Informationssystemen

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 „Kennzeichnung von und Umgang mit Informationen“).

7.1.1. 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 Sicherheits-Patches)
Intern	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Kenntnis, nur wenn nötig“ • Ein-Faktor-Authentifizierung (z. B. User-ID und Passwort)
Vertraulich	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Kenntnis, nur wenn nötig“ • 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	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • Zugriffskontrolle entsprechend dem Grundsatz „Kenntnis, nur wenn nötig“ • Zwei-Faktor-Authentifizierung (z. B. Smartcard und PIN), insbesondere für den Zugriff auf Anwendungen • Transportverschlüsselung • Datenspeicherverschlüsselung

7.1.2. Schutz der 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	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches)
Mittel	• Systemhärtung (nur benötigte Dienste und aktuelle Sicherheits-Patches) • 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 Sicherheits-Patches) • 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. 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)

7.1.3. 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
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.

7.2. Kryptographische Maßnahmen

Die Vorgaben aus der Regelung für Kryptographie[9] sind einzuhalten.

7.3. Sicherheit von Systemdateien

7.3.1. Kontrolle von Software im Betrieb

Software darf ausschließlich durch berechtigte Mitarbeiter installiert werden (siehe Anhang, B.1.10).

Neue oder geänderte Programme dürfen erst in laufenden Systemen eingesetzt werden, wenn sie entsprechend den gültigen Änderungsmanagement-Prozessen[10] erfolgreich getestet und freigegeben wurden. Die Version bzw. der Status der Korrektur der verwendeten Software ist entsprechend den unternehmensspezifischen Regelungen (siehe Anhang, B.1.11) zu dokumentieren und zu archivieren.

7.3.2. Zugangskontrolle zu Quellcode

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

7.4. 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.

[9] Regelung: 03.01.02 Kryptographie
[10] Regelung: 03.01.08 Change- und Patch-Management

7.5. Umgang mit Patches und 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 für das Patchmanagement[10] sind zu befolgen.
Regelmäßige Überprüfungen auf Verwundbarkeiten müssen durchgeführt werden.

8. Sicherstellung des Geschäftsbetriebs (Business 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 für das IT Service Continuity Management[11] beschrieben sichergestellt werden kann.

[11] Regelung: 03.01.14 IT Service Continuity Management

9. Einhaltung von Vorgaben

Bei der Nutzung von Verschlüsselung und/oder elektronischen Signaturen (siehe Anhang, B.1.12) 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.1.13).

Alle IT-Systembetreiber müssen zufällige Stichprobenprüfungen für ihre IT-Systeme durchführen, 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.1.8).

Alle IT-Systembetreiber sind verpflichtet, in IT-Systemen entdeckte Sicherheitslücken 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 Mitarbeiter die Werkzeuge für Systemaudits verwenden.

Die unbegrenzte Auditberechtigung der Revisionsabteilung ist hiervon nicht betroffen.

II. Verantwortlichkeiten

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

Abweichungen von dieser Leitlinie, die das Sicherheitsniveau beeinträchtigen, sind nur temporär und nach Rücksprache mit den zuständigen Stellen (siehe Anhang, B.1.9) gestattet.

Anhang

A Allgemeines

A.1 Gültigkeit

Diese Regelung tritt zum Zeitpunkt der Veröffentlichung in Kraft.

Nächster Überprüfungstermin: 01.10.2023

A.2 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 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 bei Bedarf Rechtsabteilung (B/F-R) kontaktieren

B.1.4 Ein IT-System ist ein Gesamtsystem bestehend aus sämtlichen Hardware- und Software-Komponenten inklusive deren Kommunikationsbeziehungen untereinander.

B.1.5 URLB_014

B.1.6 LISSC (Local Information Steering Committee) via ISB (Informationssicherheitsbeauftragten)

B.1.7 Die Freigabe von Virenschutzsoftware erfolgt durch das Anti Virus Emergency Response Team (AVERT) des VW-Konzerns.

B.1.8 Einbindung und Freigabe DPO und Rechtsabteilung (B/F-R)

B.1.9 IT-Sicherheit (B/FP)

B.1.10 Verantwortlichkeit: Mitarbeiterinnen und Mitarbeiter, die aufgrund ihrer definierten Aufgabenstellung, Installationsrechte genehmigt erhalten haben, z. B. IT (B/FP), Locadmins, Application Owners, Instandhaltungen

B.1.11 URLB_014

B.1.12 -

B.1.13 Rechtsabteilung (B/F-R)