# Informationssicherheit

# Übergreifende Richtlinien und Prozesse

# Regelung Nr. 03.01.01

# Anti Malware & Systemschutz

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

# Inhalt

# I. Zweck

Der Zweck dieser Regelung ist die Festlegung von Grundsätzen und Anforderungen an die Sicherheit von Systemen bei der AUDI BRUSSELS. Diese Regelung umfasst den Schutz vor Schadsoftware und beinhaltet Regelungen zur Systemhärtung.

Im Sinne dieser Regelung bedeutet der Begriff „Informationssicherheit“ IT-Sicherheit als Bestandteil einer ganzheitlichen Informationssicherheit.

# 1. Schutz vor Schadsoftware

## 1.1. Ziel

Dieses Kapitel definiert organisatorische und technische Maßnahmen zum Schutz von Daten und Systemen im Netzwerk der AUDI BRUSSELS. Daten müssen vor Infektionen bzw. Manipulationen durch Computerviren und verwandte Schadsoftware (z. B. Würmer, Trojanische Pferde) – im Folgenden „Schadsoftware“ genannt - sowie deren Auswirkungen geschützt werden.

Kommunikationsgeräte sind u.a. Server, embedded Systeme, Workstations, Notebooks, Smartphones und andere mobile sowie virtuelle Endgeräte und Systeme, auf welchen ein Betriebssystem (z.B. Windows, Mac OS, Linux, iOS) installiert ist, welches potentiell anfällig gegen Schadsoftware ist.

## 1.2. Allgemeine Anforderungen

### **1.2.1** Verhindern einer Infektion durch Schadsoftware

- Von Benutzern modifizierbarer Inhalt muss mindestens einmalig beim Passieren von Sicherheitsbereichen auf Schadsoftware überprüft werden.
- Alle innerhalb des Netzwerks der AUDI BRUSSELS eingesetzten Kommunikationsgeräte müssen mit einer von der zuständigen Stelle[1] freigegebenen, dokumentierten[2] Schutzsoftware gegen Schadcode versehen werden. Die Implementierung von vergleichbaren oder alternativen Schutzverfahren muss durch die zuständige Stelle[3] freigegeben werden. Freigegebene Schutzsoftware gegen Schadcode oder freigegebene, alternative Verfahren werden im Folgenden als Schutzsoftware bezeichnet. Es dürfen nur freigegebene Versionen der jeweiligen Schutzsoftware eingesetzt werden. Schutzsoftware muss entsprechend der Vorgaben und Spezifikationen der zuständigen Stelle[4] konfiguriert sein.

[1] Siehe B.1.1

[2] Zum Beispiel siehe BoS (Book of Standards)

[3] Siehe Anhang B.1.1

[4] Siehe Anhang B.1.1

- Signaturen/Definitionen, Scan Engine und alle Komponenten der Schutzsoftware müssen automatisch aktualisiert werden.
- Fehlende, fehlgeschlagene oder beschädigte Updatemechanismen der Schutzsoftware gegen Schadcode müssen der zuständigen Stelle[5] gemeldet werden.
- Bei der Prüfung auf Schadsoftware sollten zusätzlich heuristische Verfahren eingesetzt werden.
- Geräte ohne Schutzsoftware und ohne täglich aktualisierte Signaturen/Definitionen dürfen nicht im Netzwerk der AUDI BRUSSELS betrieben werden. Technologien oder Prozesse sind zu implementieren, um den Betrieb solcher Geräte im Netzwerk der AUDI BRUSSELS zu verhindern.
- Jede Schutzsoftware, die auf Kommunikationsgeräten mit Anbindung an das Netzwerk der AUDI BRUSSELS betrieben wird muss über ein zentrales Managementsystem verwaltet werden. Die Installation individueller Managementsysteme muss durch die zuständige Stelle[6] freigegeben werden.
- Hardware, die nicht über ausreichend Ressourcen (z.B. CPU Rechenleistung, Speicher, Plattenplatz) zum Betrieb aktueller Schutzsoftware verfügt, ist nicht für den Einsatz im Netzwerk der AUDI BRUSSELS geeignet und muss daher aufgerüstet oder ersetzt werden.
- Server Systeme, die Bestandteil der Infrastruktur zum Schutz vor Schadsoftware sind (z.B. Anti-Malware-Gateways/Server und Managementsysteme) müssen dem IT-Betrieb[7] übergeben werden, damit angemessene Backups sichergestellt sind und alle Daten, die durch Schadsoftware zerstört wurden wiederhergestellt werden können.
- Der IT-Betrieb[8] muss dafür Sorge tragen, dass durch ihn installierte, gewartete oder entwickelte Software den aktuellen Sicherheitsstandards[9] entspricht. Insbesondere darf Software, die nicht mit Standard-Sicherheitseinstellungen oder Schutzsoftware kompatibel ist, nicht eingesetzt werden.
- Da Schadsoftware in vielen Fällen bekannte Sicherheitslücken ausnutzt, sind Sicherheitsupdates von Software-Herstellern zeitnah einzuspielen und somit erkannte Schwachstellen umgehend zu beheben.
- Zum Schutz vor Schadsoftware, die über E-Mail verbreitet wird, muss ein mehrstufiges Schutzkonzept verwendet werden. Alle ein- und ausgehenden E-Mails müssen auf dem SMTP-gateway, dem E-Mail Server und auf dem Empfängersystem auf Schadsoftware überprüft werden. Aus technischen Gründen müssen verschlüsselte E-Mails bei der frühestmöglichen Gelegenheit nach dem Entschlüsseln überprüft werden. Spätestens muss dies auf dem Empfangssystem erfolgen.

[5] Siehe Anhang B.1.3

[6] Siehe Anhang B.1.5

[7] Siehe Anhang B.1.6

[8] Siehe Anhang B.1.6

[9] Siehe BoS (Book of Standards)

- Es sollten zwei verschiedene Anbieter (two vendor strategy) für E-Mail Server und SMTP-Gateways eingesetzt werden.

## 1.3. Organisatorische Anforderungen

- Die Richtlinien und Standards[10] der zentralen Organisation zum Schutz vor Schadsoftware (IT-Sicherheit) sind einzuhalten.
- Analyse, Bewertung und Veröffentlichung von Warnungen vor Schadsoftware erfolgen durch die zentrale Organisation zum Schutz vor Schadsoftware (IT).
- Das zentrale Anti-Malware Managementsystem der AUDI AG muss durch die zuständige Stelle betrieben werden (IT).
- Das lokale Anti-Malware Managementsystem muss durch die zuständige lokale Stelle betrieben werden (IT-Betrieb).
- Die Hardware für das zentrale Managementsystem und dessen Datenbank muss physikalisch in unterschiedliche Lokationen getrennt sein.
- Es müssen lokale Ansprechpartner[11] definiert werden. Deren Kontaktdaten müssen der zentralen Organisation zum Schutz vor Schadsoftware (IT-Sicherheit) bekanntgeben werden. Folgende Aufgaben müssen von den lokalen Ansprechpartnern umgesetzt werden:
    - Definition, Test und Anwendung von geeigneten Eskalationsverfahren bei:
        - Vermuteten Infektionen mit Schadsoftware
        - Warnungen vor Schadsoftware
        - Infektionen mit Schadsoftware
        - CERT-Sicherheitsvorfällen
    - Bei Security Incidents (z.B. Malware) muss eine Rückmeldung über durchgeführte Aktionen an die zentrale Organisation zum Schutz vor Schadsoftware (IT-Sicherheit bzw. das CERT) gegeben werden. Die Regelmäßigkeit der Rückmeldungen wird je nach Priorität des Vorfalls basierend auf der Regelung für Information Security Incident Management (A.1.7) festgelegt.
    - Sicherstellen einer kompletten Verteilung und regelmäßigen Aktualisierung der Schutzsoftware. Die durch die zentrale Organisation zum Schutz vor Schadsoftware definierten Standards müssen bekannt sein und eingehalten werden.
    - Sicherstellen einer flächendeckenden Überwachung der Schutzsoftware und zugehöriger Ereignisse.
    - Sicheres Weiterleiten verdächtiger Dateien an die zentrale Organisation zum Schutz vor Schadsoftware (IT-Sicherheit).

[10] Siehe Anhang B.1.7

[11] Siehe Anhang B.1.3

- Bereitstellen einer 24/7 Notfallrufnummer in der zentralen Kontaktdatenbank[12] der zuständigen IT-Sicherheit.
- Bei der Nutzung von Managementinstanzen, welche nicht durch die zentrale Organisation zum Schutz vor Schadsoftware bereitgestellt und betreut werden, sind durch die lokalen Ansprechpartner Berichte zu erstellen, welche einen Aufschluss über die aktuelle Bedrohungslage geben. Diese Berichte müssen regelmäßig zum Monatsanfang angefertigt und bereitgestellt werden. Die sich daraus ergebenden Maßnahmen sind so bald wie möglich von den lokalen Ansprechpartnern umzusetzen.
- Lokale Ansprechpartner müssen regelmäßig im Umgang mit den bereitgestellten Managementsystemen geschult werden.
- Das bereitgestellte zentrale Anti-Malware Managementsystem der AUDI BRUSSELS muss verwendet werden. Ausnahmen müssen über den Prozess für Ausnahmegenehmigungen[13] beantragt werden.

## 1.4. Anforderungen an Anti-Malware Produkte

Jedes in der AUDI BRUSSELS eingesetzte Anti-Malware Produkt muss von der zuständigen Stelle[14] freigegeben werden und mindestens die folgenden Anforderungen erfüllen:

- Zertifizierung des Anti-Malware Produkts durch eine angesehene dritte Partei (z. B. ICSA- Zertifizierung)
- Aktive Benachrichtigung durch den Hersteller bei Malware Ereignissen oder Warnungen (z. B. per E-Mail oder telefonisch)
- Erfassung sicherheitsrelevanter Anwendungsereignisse (z.B. Infektionen, Updatefehler)
- Kompatibilität mit den in der AUDI BRUSSELS und AUDI AG eingesetzten Standardapplikationen[15]
- Möglichkeit der zentralen Administration, sowie der Erstellung von Berichten und Auswertungen
- Automatisches Update der Signaturen/Definitionen und Scan Engines ohne Unterbrechung der Überprüfung und ohne das Sicherheitsniveau zu senken
- Automatisches Update der Signaturen/Definitionen mindestens 1mal täglich; zusätzlich muss der Anwender auch ohne lokale Administratorenrechte dazu in der Lage sein, eine Aktualisierung durchzuführen
- Verfügbarkeit eines Zugriffsscans: real time / on-access-scanner (OAS)
- Verfügbarkeit eines Anforderungsscans: on-demand-scanner (ODS)
- Schutz der Konfigurationsparameter, Dateien und Registrierungseinträge gegen unbefugte Änderung oder Deaktivierung

[12] Bereitschaftstelefonnummernliste des Operating

[13] Siehe Anhang A.1.1

[14] Siehe Anhang B.1.8

[15] Wie im “Book of Standards” definiert

- Unterstützung gängiger Betriebssysteme (inklusive Windows, Mac OS, Unix/Linux, Android) und virtuelle Umgebungen
- Unterstützung sofortiger und planmäßiger automatischer Aktualisierungen bei Bekanntwerden neuer Bedrohungen
- Ein Roll-back der Malware Signaturen/Definitionen auf einen vorherigen Versionsstand muss sowohl über das lokale System als auch über das Managementsystem möglich sein
- Das Produkt muss Anti-Spyware Funktionalität beinhalten
- Das Produkt muss die Möglichkeit zum Ausschluss bestimmter Pfade, URLs, Prozesse, Verzeichnisse und Dateitypen von der Überprüfung bieten
- Die Scan Engine ist so zu konfigurieren, dass diese während des Bootvorgangs so schnell wie möglich startet und beim Herunterfahren so spät wie möglich beendet wird.

## 1.5. Mindestanforderungen für die Konfiguration von Anti-Malware Produkten

In der AUDI BRUSSELS eingesetzte Anti-Malware Produkte müssen entsprechend der in den folgenden Kapiteln definierten Mindestkonfigurationsanforderungen eingerichtet sein.

### 1.5.1 Konfiguration für Client-Rechner (Arbeitsplatzrechner) und Server

Auf Client-Rechnern und Servern muss Anti-Malware Software wie hier definiert konfiguriert sein:

- Der Zugriffsscanner/Echtzeitschutz muss automatisch beim Start des Systems gestartet werden.
- Alle Dateien müssen durch den Zugriffsscanner (OAS) beim Öffnen (Lesen) und beim Schreiben überprüft werden.
- Am Netzwerk angeschlossene Systeme müssen sicherheitsrelevante Ereignisse automatisch an das zentrale Managementsystem weiterleiten.
- Infizierte Dateien müssen automatisch bereinigt werden. Ist dies nicht möglich, müssen infizierte Dateien in ein Quarantäneverzeichnis verschoben oder gelöscht werden. Ist dies nicht möglich muss der Zugriff und vor allem die Ausführung dieser Dateien verhindert werden.
- Malware Funde sollten dem Benutzer durch einen Warnhinweis angezeigt werden.
- Benutzern darf kein Zugriff auf die Dateien im Quarantäneverzeichnis möglich sein (z.B. Der User kann zwar das Verzeichnis öffnen, darf jedoch keine Dateien ausführen).
- Am Netzwerk angeschlossene Systeme müssen mindestens einmal täglich und automatisch ihre Signaturen/Definitionen aktualisieren.
- Systeme, die nicht an das Netzwerk angeschlossen sind, müssen mindestens einmal im Monat mit den aktuellen Signaturen/Definitionen aktualisiert werden.
- Benutzern darf es nicht möglich sein die Schutzsoftware zu deaktivieren.
- Anforderungsscans müssen regelmäßig (z. B. wöchentlich) durchgeführt werden und sämtliche lokalen Laufwerke, Datenträger, Prozesse und den Speicher des Systems

beinhalten. Abweichungen für Clients und Systeme der Produktion, z.B. aufgrund der hohen Anforderung an die Verfügbarkeit, müssen von der zuständigen Stelle[16] genehmigt und dokumentiert werden.

- Weitere gesellschaftsspezifische Regelungen[17] müssen befolgt werden.

Die Anti-Malware Software muss das System im Ganzen schützen. Die Anti-Malware Software darf nicht annehmen oder sich darauf verlassen, dass andere Systeme bestimmte Dateien überprüfen.

### 1.5.2 Spezifische Merkmale für Unix Server

- Ein Unix-Server, der gemäß den Härtungsrichtlinien gehärtet wurde und keine Daten zur Verwendung auf Client-Systemen bereitstellt, benötigt keinen Malware-Scanner auf dem System
- Die Betreiber eines Unix Servers, der Daten für die Speicherung oder Verarbeitung auf Client-Systemen bereitstellt, müssen den Malware-Schutz implementieren. Eines der folgenden Verfahren kann verwendet werden:
    - Scannen des Inhalts auf den Netzwerkgeräten (z.B. SSL-Terminator, Load-Balancer, usw.)
    - Scannen über einen Reverse Proxy
    - Batch Scans auf Unix-Ebene
- Ein Samba-Sever muss Dateisysteme mit Schreibberechtigung für Clients auf Malware untersuchen.

### 1.5.3 Konfiguration für E-Mail-Server

Schutzsoftware für E-Mail Server muss so konfiguriert werden, dass:

- Eingehende und ausgehende E-Mails inkl. Dateianhänge (auch komprimierte Dateien) müssen auf Viren überprüft werden (OAS). Ausgenommen hierzu sind verschlüsselte E-Mails. Diese müssen nach der Entschlüsselung auf dem Endgerät überprüft werden.
- Mit Viren infizierte E-Mails oder Dateianhänge müssen gemäß gesellschaftsspezifischen Regelungen[18] gelöscht werden. Dem Benutzer sollte eine Warnmeldung gesendet werden.
- Sicherheitsrelevante Ereignisse müssen automatisch an das Managementsystem weitergeleitet und durch die verantwortliche Stelle[19] überprüft werden.
- Signaturen/Definitionen müssen automatisch mindestens einmal täglich aktualisiert werden.

Das Betriebssystem des Servers muss gegen Infektionen durch Schadsoftware mit Hilfe von lokal installierter Schutzsoftware gesichert sein.

---

[16] Siehe Anhang B.1.8

[17] Siehe Anhang B.1.7

[18] Siehe Anhang B.1.10

[19] Siehe Anhang B.1.8

### 1.5.4 Konfiguration für Smartphones und Tablet Computer

- Smartphones müssen zentral verwaltet werden (z.B. MobileIron)

Ähnliche Geräte, wie beispielsweise Tablet Computer, müssen mit Schutzsoftware versehen sein. Diese muss wie im Folgenden beschrieben konfiguriert sein:

- Alle Dateien müssen durch den Zugriffsscanner (OAS) beim Öffnen (Lesen) und beim Schreiben überprüft werden.
- Infizierte Dateien müssen automatisch bereinigt werden. Ist dies nicht möglich, müssen infizierte Dateien in ein Quarantäneverzeichnis verschoben oder gelöscht werden. Ist dies nicht möglich muss der Zugriff und vor allem die Ausführung dieser Dateien verhindert werden.
- Infektionen und Abweichungen von der erforderlichen Sicherheitskonfiguration müssen automatisch an das zentrale Managementsystem gemeldet werden.
- Signaturen/Definitionen müssen regelmäßig aktualisiert werden (mindestens bei der Synchronisation).

Wenn die Implementierung von Schutzsoftware aus technischen Gründen nicht möglich ist, sind spezifische Schutzmaßnahmen (z.B. Applikationskontrolle, Härtung des Betriebssystems) in Absprache mit der zuständigen Stelle[20] einzusetzen.

### 1.5.5 Synchronisation von PDAs

- PDAs dürfen nur mit Systemen die mit einer Schutzsoftware versehen sind synchronisiert werden.

### 1.5.6 Konfiguration für mobile Datenträger

Mobile Datenträger (wie z. B. USB-Sticks oder externe Festplatten) dürfen nur an Endgeräte der AUDI BRUSSELS angeschlossen werden, wenn diese über die zuständige Stelle[21] bereitgestellt wurden. Mobile Datenträger müssen automatisch auf Schadsoftware überprüft werden, wenn sie mit einem Client verbunden werden.

### 1.5.7 Konfiguration für Produktionssysteme (Shop Floor)

Um Produktionssysteme (Shop floor Systeme) vor Schadsoftware zu schützen, muss Schutzsoftware eingesetzt werden. Shop floor Systeme sind alle Systeme, die in Netzwerkbereichen betrieben werden, welche für Produktionszwecke vorgesehen sind.

Alle Systeme auf denen für die Fahrzeug- oder Komponentenproduktion relevante Anwendungen laufen, müssen entsprechend der Regelungen für Client-Rechner und Server in Kapitel 1.5.1 konfiguriert sein.

[20] Siehe Anhang B.1.11

[21] Siehe Anhang B.1.12

Zusätzlich gelten die folgenden Anforderungen:

- Shop floor Systeme dürfen mit der vorherigen Signatur/Definition (lediglich eine Version vor der aktuellen) betrieben werden, um Kompatibilitätstests zu ermöglichen.
- Abweichungen vom Standardprozess müssen durch die zuständige Stelle[22] genehmigt werden.
- Wenn die Implementierung von Schutzsoftware aus technischen Gründen nicht möglich ist, müssen spezifische Schutzmaßnahmen (z.B. Applikationskontrolle, Härtung des Betriebssystems) in Absprache mit der zuständigen Stelle[23] genehmigt und umgesetzt werden. Härtungsmechanismen dürfen durch Applikationen nicht umgangen werden können.
- Sowohl Schutzsoftware und Application Whitelisting muss über ein zentrales Managementsystem verwaltet und überwacht werden. Hierbei muss das zentrale Managementsystem der zentralen Organisation zum Schutz vor Schadsoftware eingesetzt werden. Ist dies technisch nicht umsetzbar, muss nach Rücksprache mit der zuständigen Stelle[24] und unter Berücksichtigung der im Kapitel 1.2 genannten Auflagen eine eigene Managementlösung aufgebaut werden. Ist es nicht ökonomisch eine dedizierte Management Lösung (z.B. für <10 Systeme) einzurichten, kann auf diese Anforderung verzichtet werden. Allerdings muss ein zentral gesteuertes Incident-Response-Handling möglich sein. Die Entscheidung zu dieser Thematik ist von der zuständigen lokalen Stelle zu treffen. In jedem Fall muss zusätzlich ein Verfahren für eine monatliche Berichterstattung an die zuständige Stelle[25] eingerichtet werden.

### 1.5.8 Konfiguration von Embedded Systemen

Es gelten die folgenden Anforderungen:

- Sollte die Implementierung von Antimalware (wie in Kapitel 1.5.1 definiert) aufgrund von technischen Gründen nicht möglich sein, sind spezifische Schutzmaßnamen in Koordination mit der zuständigen Stelle zu implementieren[26].

  Diese können beinhalten:

  - Applikationskontrolle/Anwendungssperre
  - Isolation des Systems
  - Härtung (Deaktivieren von Schnittstellen oder Diensten)
  - Sicherheitsmaßnahmen für die Infrastruktur oder Architektur (weitere Sicherheitsschichten, Netzwerktrennung, erweitertes Monitoring)

[22] Siehe Anhang B.1.13

[23] Siehe Anhang B.1.14

[24] Siehe Anhang B.1.15

[25] Siehe Anhang B.1.16

[26] Siehe Anhang B.1.17

### 1.5.9 Ausnahmen von der Mindestkonfiguration

Ausnahmen müssen über den definierten Prozess für Ausnahmegenehmigungen[27] beantragt werden.

[27] Siehe Anhang A.1.1

# 2. Systemhärtung

## 2.1. Ziel

IT-Komponenten, Betriebssysteme, Datenbanken und Applikationen verfügen häufig über Funktionalitäten, die im konkreten Einsatzkontext gar nicht benötigt werden. Dies erhöht unnötigerweise die Anzahl möglicher Schwachstellen. Im Rahmen der Systemhärtung werden deshalb alle überflüssigen Funktionen entfernt oder deaktiviert und somit die Wahrscheinlichkeit eines erfolgreichen Angriffs reduziert. Dieses Dokument definiert hierfür lediglich Mindestsicherheitsanforderungen. Systeme mit höheren Sicherheitsanforderungen (z.B. Systeme die geheime Daten verarbeiten) müssen durch weitere Maßnahmen, entsprechend des Informationssicherheitsregelwerkes[28] und dem Resultat einer Risikoanalyse, gehärtet werden.

## 2.2. Erstellung, Freigabe und Ausnahmen

Alle Anforderungen und Anweisungen zur Systemhärtung müssen in technologie-/produktspezifischen Regelungen festgelegt und dokumentiert werden. Alle in der AUDI BRUSSELS betriebenen IT-System-Komponenten müssen nach diesen Regelungen gehärtet werden.

In diesem Sinne zählen zu den IT-System-Komponenten:

- Betriebssysteme (z.B. Windows, Red Hat Linux, Solaris, HP-UX)
- Anwendungen
- Datenbanksysteme (z.B. Microsoft SQL Server, Oracle, IBM DB2)
- Netzwerkkomponenten (z.B. Cisco, Juniper, Nortel)
- Middleware Komponenten (z.B. Apache Webserver, Tomcat Servlet Container)

Sofern eine technologie-/ produktspezifische Regelung bereits verfügbar ist (Siehe Anhang A.2.2), muss das System entsprechend konfiguriert sein. Andernfalls muss vom verantwortlichen Systembetreiber eine technologie-/produktspezifische Regelung erstellt und anschließend durch die zuständige Stelle[29] freigegeben werden.

Jegliche Ausnahmen, die das Sicherheitsniveau reduzieren, müssen über den definierten Prozess für Ausnahmegenehmigungen[30] beantragt werden.

[28] Siehe Anhang A.1.4

[29] Siehe Anhang B.2.1

[30] Siehe Anhang A.1.1

## 2.3. Anforderungen zur Systemhärtung

Es dürfen nur IT-Komponenten bei der AUDI BRUSSELS betrieben werden, die entsprechend der jeweiligen technologie-/produktspezifischen Regelungen[31] gehärtet sind.

Nicht benötigte Programme, Dienste oder technische Prozesse müssen deinstalliert oder deaktiviert werden.

Konfigurationsdaten und weitere Informationen über die IT-Komponente (z. B. Patch-Level) müssen anhand von Härtungsrichtlinien[32] vor unberechtigtem Zugriff geschützt werden. Dies gilt sowohl für Konfigurationsdateien als auch für Dienste, die diese Informationen preisgeben können.

[31] Siehe Anhang A.2.2

[32] Siehe Anhang A.2.2

# II. Verantwortlichkeiten

## II.I Kapitel 1: Schutz vor Schadsoftware

Diese Regelung ist von allen Planern, Bereitstellern und Betreibern von IT-Systemen anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

## II.II Kapitel 2: Systemhärtung

Diese Regelung ist von allen Planern, Bereitstellern und Betreibern von IT-Systemen anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

# Anhang

# A. Allgemeines

## A.1 Mitgeltende Dokumente

### A.1.1 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

### A.1.2 Informationssicherheitshandlungsleitlinien für Führungskräfte

### A.1.3 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

### A.1.4 Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren

### A.1.5 Informationssicherheitshandlungsleitlinien für Systementwickler

### A.1.6 Informationssicherheitshandlungsleitlinien für Partnerfirmen

### A.1.7 Informationssicherheit Regelung Nr. 03.01.18 Informationssicherheitsvorfalls- und Schwachstellenmanagement

## A.2 Anlagen

### A.2.1 Anlage 1 Feedbackformular

Das Feedbackformular für Änderungsvorschläge zu Regelungen kann von der MyNet-Webseite Gesellschaften → Audi Brussels → Organisation → Finanz (B/F) → IT (B/FP) → IT-Sicherheit → Regelwerk heruntergeladen werden.

Das Feedback-Formular ist folgendermaßen auszufüllen:

Die Spalten 2 bis 6 müssen für jede vorgeschlagene Änderung ausgefüllt werden. Änderungen, für die nicht alle Spalten 2 bis 6 ausgefüllt sind, werden automatisch ohne weitere Prüfung abgelehnt.

Spalte 3: Folgende Kommentararten sind möglich: a=allgemein, f=fachlich, r=redaktionell

Spalte 4: Bitte bisherigen Text, Tabelle oder Bild einfügen

Spalte 5: Bitte vollständig umformulierten Text, geänderte Tabelle oder geändertes Bild einfügen

Spalte 6: Bitte begründen Sie die gewünschte Änderung möglichst ausführlich.

Bitte senden Sie das ausgefüllte Formular an: it-security.audibx@audi.de

### A.2.2 Anhänge zur Regelung Anti Malware & Sytemschutz (volkswagen-security-settings.zip)

## A.3 Quellen und Referenzen

### A.3.1 ISO 27001 A.10.4 Protection about malicious and mobile code

### A.3.2 ISO 27001 A.10.3 System planning and acceptance

### A.3.3 BSI M 2.70 Entwicklung eines Konzepts für Sicherheitsgateways

### A.3.4 BSI M 2.160 Regelungen zum Schutz vor Schadprogrammen

## A.4 Abkürzungen und Definitionen

| Abkürzung / Begriff | Erklärung |
|---|---|
| Schutzsoftware gegen Schadcode | Software auf einem System, die bei Zugriff oder auf Anforderung eine Überprüfung auf Schadsoftware durchführt. |
| Schadcode | Schadcode ist eine generelle Bezeichnung für Anwendungen, die Schaden auf einem System verursachen können oder dieses infizieren. Beispiele für Schadcode sind Trojanische Pferde, Würmer oder Logikbomben. |
| Schutzsoftware | Schutzsoftware gegen Schadcode oder vergleichbare alternative Schutzmaßnahmen (z.B. Application Control) |

## A.5 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig.

Bereits bestehende Ausnahmeregelungen sind spätestens bei der nächsten Änderung (z.B. Verlängerung, Änderung der Auflagen) an diese Regelung anzupassen.

Nächster Überprüfungstermin: 06.08.2021

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular.

## A.6 Dokumentenhistorie

| Version | Name | Org.-Einheit | Datum | Bemerkung |
|---|---|---|---|---|
| 1.0 | Andreas Walter | B/FP | 07.08.2019 | Veröffentlicht |
| | | | | |
| | | | | |

# B. Spezifische Ausprägungen

## B.1 Kapitel 1: Schutz vor Schadsoftware

### B.1.1 IT-Sicherheit

### B.1.2 IT-Sicherheit

### B.1.3 IT Services, bei Produktionsgeräten ggf. die jeweiligen Instandhaltungen und Planungen

### B.1.4 Nicht Referenziert

### B.1.5 IT-Sicherheit

### B.1.6 IT Services, bei Produktionsgeräten ggf. die jeweiligen Instandhaltungen und Planungen

### B.1.7 Keine weiteren Details

### B.1.8 IT-Services

### B.1.9 IT-Sicherheit

### B.1.10 Keine weiteren Details

#### B.1.11 IT-Sicherheit

#### B.1.12 IT, bei Produktionsgeräten ggf. die jeweiligen Instandhaltungen und Planungen

#### B.1.13 IT-Sicherheit

#### B.1.14 IT-Sicherheit

#### B.1.15 IT-Sicherheit

#### B.1.16 IT-Sicherheit

#### B.1.17 IT-Sicherheit

#### B.1.18 IT-Sicherheit

## B.2 Kapitel 2: Systemhärtung

### B.2.1 IT-Sicherheit