# Informationssicherheit

# IT Systemkomponenten

# Regelung Nr. 03.03.04

# Multifunktions- und Peripheriegeräte

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 Sicherheitsanforderungen an den Betrieb von Multifunktions- und Peripheriegeräten.

Als Multifunktions- und Peripheriegeräte werden im Rahmen dieser Regelung[1] folgende Geräte definiert:

- Drucker
- Kopierer
- Scanner
- Faxgeräte
- Multifunktionsgeräte
- Kameras / Webcams
- Mobile Datenträger[2]

# 1. Multifunktionsgeräte (Drucker, Kopierer, Scanner, Fax, E-Mail)

## 1.1. Ziel

Das Ziel dieses Kapitels ist die Festlegung notwendiger Informationssicherheitsanforderungen für den Betrieb von Netzwerkdruckern, Kopierern, Scannern, Faxgeräten und Multifunktionsgeräten.

## 1.2. Allgemeine Anforderungen

Die nachfolgenden Anforderungen gelten für Netzwerkdrucker, Kopierer, Scanner, Faxgeräte und Multifunktionsgeräte. Alle genannten Geräte werden nachfolgend unter dem Begriff Multifunktionsgeräte zusammengefasst.

- Multifunktionsgeräte müssen zentral registriert und verwaltet werden.
- Multifunktionsgeräte müssen so konfiguriert sein, dass die Anforderungen an den Umgang mit Informationen gemäß den Informationssicherheitshandlungsleitlinien[3] erfüllt sind.
- Anwender müssen im sicheren Umgang mit Multifunktionsgeräten geschult werden (z. B. Benutzerhandbuch).
- Anwender müssen darauf hingewiesen werden, Ausdrucke zeitnah vom Drucker abzuholen. Nicht abgeholte Dokumente sind vom Drucker zu entfernen und sicher aufzubewahren oder zu entsorgen[4].
- Der Zutritt zu Räumen in denen sich Multifunktionsgeräte befinden sollte beschränkt sein.

[1] Für kabellose Geräte: A.1.4

[2] Detaillierte Definition in Kapitel 3

[3] Siehe Anhang A.1.2

[4] Siehe Anhang A.1.2

- Die Verwendung[5] von Multifunktionsgeräten darf nur nach erfolgter Authentifizierung auf Geräteebene möglich sein (wenn technisch möglich).
- Multifunktionsgeräte müssen vor physischer Manipulation geschützt werden (z. B. durch Schlösser oder Siegel), wenn sich diese in öffentlich zugänglichen Bereichen befinden oder dies durch eine Risikobetrachtung erforderlich ist (z.B. in besonderen Sicherheitsbereichen).
- Es dürfen nur Protokolle und Ports verwendet werden, die von der verantwortlichen Stelle[6] freigegeben sind.
- Es muss ein Prozess zur Wartung und Reparatur von Multifunktionsgeräten definiert und dokumentiert sein. Dieser Prozess muss Maßnahmen zum Vorgehen während dieser Tätigkeiten beinhalten.
- Für Multifunktionsgeräte die häufig in Gebrauch sind müssen Wartungsverträgen mit angemessenen Reaktionszeiten vereinbart sein.

### 1.2.1 Administration und Konfiguration

- Für den administrativen Zugriff auf Multifunktionsgeräte sind die Anforderungen der Informationssicherheitshandlungsleitlinie für Systembetreiber und Administratoren[7] einzuhalten.
- Default Passwörter müssen vor der Produktivsetzung geändert werden.
- Sicherheitsrelevante Konfigurationseinstellungen (z. B. Netzwerkeinstellungen) dürfen nicht von normalen Anwendern geändert werden können.
- Konfigurationseinstellungen von Multifunktionsgeräten müssen zentral definiert und administriert werden.
- Ein Backup der Konfiguration muss verfügbar sein.
- Alle Multifunktionsgeräte müssen gemäß den zentral vorgegebenen Vorgaben konfiguriert sein.
- Die Konfiguration muss regelmäßig überprüft und bei Bedarf auf die definierten Einstellungen zurückgesetzt werden.
- Alle Informationen in den lokalen Cache-Speichern von Multifunktionsgeräten müssen nach deren Verarbeitung automatisch gelöscht werden.
- Multifunktionsgeräte dürfen nicht an öffentliche Netzwerke (z. B. Internet) angebunden werden.
- Für den Betrieb nicht notwendige Funktionen (z. B. Aktive Protokolle) und Schnittstellen (z. B. USB) müssen deaktiviert werden.
- Speichermedien (z. B. interne Festplatten) von Multifunktionsgeräten müssen verschlüsselt sein. Falls vorhanden, sollten weitere Verschlüsselungsmechanismen (z. B. RAM Verschlüsselung) eingesetzt werden.

[5] Die Kopierfunktion ist hiervon ausgenommen.

[6] Siehe Anhang B.1.1

[7] Siehe Anhang A.1.3

- Die Anforderungen der Informationssicherheitshandlungsleitlinien[8/9] bezüglich Beschaffung, Betrieb und Entsorgung müssen eingehalten werden.
- Interne Speichermedien von Multifunktionsgeräten müssen vor der Rückgabe an den Lieferanten bzw. vor der Außerbetriebnahme oder Recycling auf sichere Weise gelöscht oder zerstört werden[10/11].
- Die Netzwerkeinstellungen von Multifunktionsgeräten müssen vor der Rückgabe an den Lieferanten bzw. vor der Außerbetriebnahme oder Recycling auf die Standardwerte zurückgesetzt werden.

## 1.3. Geräte mit Druckfunktion

- Die Funktion direkt am Gerät, den letzten Druckvorgang zu wiederholen muss deaktiviert sein.
- Der Zugriff auf Ausdrucke muss entsprechend der Datenklassifikation auf autorisierte Personen beschränkt sein. Dies kann durch Benutzerauthentisierung am Gerät (z. B. Print-to-Me) oder über Einschränkung des physischen Zugangs zum Gerät realisiert werden.
- Die “Print-to-Me-Funktion” muss als Standardauswahl am Client eingestellt sein.

## 1.4. Geräte mit Scanfunktion

- Die scan-to-file Funktion darf nur nach erfolgreicher Authentifikation direkt am Gerät möglich sein.
- Ausschließlich authentifizierte Benutzer dürfen Zugriff auf die gescannten Dateien haben.
- Das Gerät muss so konfiguriert werden, dass bei Verwendung der scan-to-email Funktion Dateien nur an interne Adressen gesendet werden können.

## 1.5. Geräte mit Faxfunktion

- Die Verwendung der Faxfunktion darf nur nach erfolgreicher Authentifikation direkt am Gerät möglich sein (wenn technisch möglich).
- Falls bei beiden Kommunikationspartnern vorhanden, müssen Verschlüsselungsmechanismen eingesetzt werden.
- Die Funktion direkt am Gerät, den letzten Druckvorgang zu wiederholen muss deaktiviert sein.
- Der Zugriff auf das Journal sollte geschützt sein.

[8] Siehe Anhang A.1.2

[9] Siehe Anhang A.1.3

[10] Siehe Anhang A.1.2

[11] Siehe Anhang A.1.3

## 2. Bildaufzeichnungsgeräte

Die Sicherheitsanforderungen für Bildaufzeichnungsgeräte bei der AUDI BRUSSELS werden durch die zuständige Stelle[12] geregelt.

[12] Siehe Anhang B.2.1

# 3. Mobile Datenträger

## 3.1. Zweck

Der Zweck dieser Regelung ist die Festlegung von Sicherheitsanforderungen für den Umgang und den Transport von mobilen Datenträgern.

Als mobile Datenträger werden im Rahmen dieser Regelung folgende Geräte definiert:

- Bänder
- Disketten, CDs, DVDs, …
- USB-Sticks
- Externe Festplatten (z. B. USB Festplatte)
- Speicherkarten (z. B. SD, SDHC, …)
- Jedes andere mobile Medium, dass zur Speicherung von Daten geeignet ist

## 3.2. Allgemeine Anforderungen

Die Verwendung und der Transport mobiler Speichermedien müssen geregelt sein.

Ziel: Schutz des Geschäftsbetriebes. Dies beinhaltet unerlaubte Weitergabe, Änderung, Entfernen oder Zerstörung von Inventar oder Informationen.

- Datenträger müssen verwaltet und vor Diebstahl entsprechend physisch geschützt werden.
- Es müssen angemessene Maßnahmen zum Schutz der mobilen Speichermedien (und den darauf gespeicherten Daten) gegen unbefugte Veränderung, Zerstörung, Veröffentlichung oder Diebstahl umgesetzt werden.

### 3.2.1 Umgang mit mobilen Speichermedien

- Wenn Wechselmedien nicht mehr gebraucht werden, dann sollte der Inhalt aller Wechselmedien, die aus einer Organisation entfernt werden, so unbrauchbar gemacht werden, dass keinerlei Informationen wiederherstellbar sind.
- Wo es notwendig und praktisch umsetzbar ist, sollte die Entnahme von Wechselmedien aus einer Organisation (Verlassen des Werksgeländes) eine Genehmigung erfordern. Diese Entnahme sollte zu Nachweiszwecken aufgezeichnet werden.
- Alle Wechselmedien sollten in einer sicheren und geschützten Umgebung, gemäß der Herstellerspezifikation, aufbewahrt werden.
- Auf Wechselmedien gespeicherte Informationen, die über die Lebensdauer eines Mediums (gemäß Herstellerangaben) hinaus verfügbar sein müssen, sollten zusätzlich an anderer Stelle (auf anderem Medium) gespeichert werden, um den Verlust durch Alterung des Mediums zu umgehen.
- Um Datenverlust zu vermeiden dürfen nur freigegebene Medien eingesetzt werden.
- Laufwerke für Wechselmedien sollten nur dann aktiviert werden, wenn es dafür einen geschäftlichen Grund gibt
- Zum Speichern von firmenbezogenen Daten dürfen nur von AUDI BRUSSELS offiziell bereitgestellte Speichermedien verwendet werden

### 3.2.2 Transport/Versand mobiler Datenträger

- Verwendung einer zuverlässigen Beförderung oder eines Kuriers.
- Eine Liste zugelassener Kuriere sollte mit dem Management festgelegt werden.
- Es sollten Verfahren entwickelt werden, um die Identität des Kuriers zu prüfen.
- Die Verpackung sollte vor physischen Beschädigungen, wie sie während des Transports leicht auftreten können, ausreichend schützen und im Einklang mit den Spezifikationen des Herstellers (z. B. für Software) stehen. So sollte z. B. ein ausreichender Schutz vor Umwelteinflüssen bestehen, die einen negativen Einfluss auf die Wiederverwendung haben, z. B. Hitze, Feuchtigkeit oder elektromagnetische Felder.
- wenn nötig sollten Maßnahmen angewandt werden, um sensitive Informationen vor unbefugter Veröffentlichung oder Veränderung zu schützen, zum Beispiel:
  - die Verwendung abschließbarer Behälter;
  - die persönliche Zustellung;
  - die Verpackung, bei der erkennbar ist, ob versucht wurde, diese zu öffnen oder zu manipulieren (Versiegelung);
  - In besonderen Fällen sollte eine Warensendung in mehrere Lieferungen aufgeteilt werden und über unterschiedliche Wege zugestellt werden.
  - Verschlüsselung

## 3.3. Maßnahmen

Alle Prozesse und zugehörige Rollen/Berechtigungen aus Kapitel 3.2 müssen klar dokumentiert sein.

### 3.3.1 Umgang mit mobilen Speichermedien

- Datenträger die nicht mehr benötigt werden müssen sicher durch Überschreiben gelöscht oder physisch zerstört werden.
- Zur Entsorgung sind geeignete Entsorgungscontainer zu verwenden. Der Standort dieser Entsorgungscontainer kann bei der zuständigen Stelle erfragt werden.
- Es müssen Prozesse für das sichere Löschen von Daten oder die physische Zerstörung von Datenträgern definiert werden.
- Die Entfernung mobiler Datenträger vom Betriebsgelände bedarf der Genehmigung durch den Vorgesetzten und ist zu regulieren.
- Werden Speichermedien außerhalb der Werksgrenzen transportiert, so müssen die Vorgaben und Betriebsvereinbarungen[13] eingehalten werden.
- Der Transport mobiler Datenträger außerhalb des Betriebsgeländes ist nur für die in den Transsportpapieren[14] genannten Zwecke erlaubt. Ausnahmen sind von der IT-Sicherheit und dem Werkschutz zu genehmigen.

[13] Siehe A.1.2 - Kapitel 7.4 Austausch von Informationen bzw. Passierschein – Berechtigung zum Mitführen von Audi Unterlagen (interne Mitarbeiter) / Passierschein Mitführen von Audi Unterlagen durch Mitarbeiter einer externen Firma

[14] Siehe Anhang B.3.5

- Mobile Datenträger sollten lediglich zu Datenaustauschzwecken als temporärer Speicher verwendet werden. Der Anwender ist dafür verantwortlich, ein ggf. notwendiges Backup der Daten zu erstellen. Diese Anforderung gilt nicht, wenn mobile Datenträger als Backup-Medien verwendet werden.
- Alternativ zu d1) muss eine Prozedur definiert sein, die das Kopieren von Informationen auf neuere Medien nach einem definierten Zeitraum (der kürzer als die Lebensdauer des Mediums sein muss) regelt. Die Möglichkeit einer Beschädigung des Mediums und damit einhergehender Verlust der Daten muss berücksichtigt werden.
- Mobile Datenträger (z.B. private USB-Sticks, CDs) die nicht durch Audi bereitgestellt wurden dürfen nicht zu geschäftlichen Zwecken verwendet werden und dürfen auch nicht an Audi Systeme angeschlossen oder eingesetzt werden. Dies beinhaltet jegliche Art von USB-Speichermedien die nicht von Audi zur Verfügung gestellt worden sind (z. B. USB Licht, Kaffeewärmer, privates Smartphone und andere technische Geräte). Davon ausgenommen sind vom Hersteller zur Verfügung gestellte Installationsmedien.
- Mobile Datenträger dürfen nicht an Systeme angeschlossen werden, wenn
  - diese zufällig irgendwo gefunden wurden
  - diese von unbekannten Personen übergeben wurden
  - die Herkunft des Mediums unbekannt ist (z. B. unbekannte Person/Firma)
- Die Verwendung von mobilen Datenträgern an Clients oder Servern mit geschäftlichem Hintergrund ist erlaubt. Hier müssen die nachfolgenden Regelungen umgesetzt werden:
  - Datenträger (z.B. USB-Sticks) mit vertraulichen oder geheimen Daten müssen verschlüsselt werden[15]. Details sind in der Datenklassifizierung zu finden[16].
  - Die Anforderungen aus der Datenklassifikation[17] für den Umgang und den Transport von mobilen Datenträgern.

### 3.3.2 Transport/Versand mobile Datenträger

- Nur die von Audi unterstützen Möglichkeiten zum Transport oder Kuriere[18] dürfen verwendet werden.
- Eine Liste[19] zugelassener Kuriere ist im Rahmen der Logistikprozesse definiert.
- Es müssen Verfahren entwickelt werden, um die Identität des Kuriers zu prüfen.
- Die Verpackung muss geeignet sein um den Inhalt vor physischen Beschädigungen, wie sie während des Transports leicht auftreten können, ausreichend zu schützen. Die Verpackung muss im Einklang mit den Spezifikationen des Herstellers stehen.

[15] Siehe Anhang A.1.3, Kapitel 8.1.1

[16] Siehe Anhang A.1.5

[17] Siehe Anhang A.1.5

[18] Siehe Anhang B.3.3

[19] Siehe Anhang B.3.4

- Maßnahmen für den Transport aus den Vorgaben der Informationsklassifikation müssen eingehalten werden.

# II. Verantwortlichkeiten

## II.I Kapitel 1: Multifunktionsgeräte (Drucker, Kopierer, Scanner, Fax, E-Mail)

Diese Regelung ist von allen Betreibern von Multifunktionsgeräten 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: Bildaufzeichnungsgeräte

Diese Regelung ist von allen Betreibern von Bildaufzeichnungsgeräten 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.III Kapitel 3: Mobile Datenträger

Diese Regelung ist von allen Anwendern und Administratoren von mobilen Datenträgern 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 Mitarbeiterinnen und Mitarbeiter

### A.1.3 Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren

### A.1.4 Informationssicherheit Regelung Nr. 03.02.01 Funknetzwerke

### A.1.5 Informationsklassifizierung (siehe A.1.2)

## A.2 Referenzen zu Standards

Die folgende Tabelle zeigt die Referenzen zu den Standards ISO/IEC 27001:2013, ISO/IEC 27001:2005 und VDA.

| Thema | Kapitel | ISO 27001:2013 | ISO 27001:2005 | VDA |
|---|---|---|---|---|
| Umgang mit Informationen | 1.2, 1.2.1 | A.8.2.3 | A.10.7.3 | |
| Verwaltung von Wechselmedien | 3 | A.8.3.1 | A.10.7.1 | |
| Transport physischer Medien | 3 | A.8.3.3 | A.10.8.3 | |
| Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln | 1.2.1 | A.11.2.7 | A.9.2.6 | |

## A.3 Anlagen

### A.3.1 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.4 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[20].

## A.5 Dokumentenhistorie

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

[20] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

# B. Spezifische Ausprägungen

## B.1 Kapitel 1: Multifunktionsgeräte (Drucker, Kopierer, Scanner, Fax, E-Mail)

### B.1.1 IT-Sicherheit

## B.2 Kapitel 2: Bildaufzeichnungsgeräte

### B.2.1 Werkssicherheit / Unternehmenssicherheit

## B.3 Kapitel 3: Mobile Datenträger

### B.3.1 Sekretariat

**B.3.2 Mobile Datenträger können in den Datenschutzcontainern zur Zerstörung mittels eines sicheren Prozesses entsorgt werden, siehe A1.2 - “Vernichtung von schutzbedürftigen Unterlagen”.**

**B.3.3 Über die zentrale Poststelle, “Hauspost” oder Sekretariat. Pakete müssen über die Transportlogistik abgegeben werden.**

**B.3.4 Pakete werden derzeit mit UPS versendet (innerhalb von Deutschland), DHL (in Europa) und FedEx (andere Länder).**

**B.3.5 Es muss mindestens der Passierschein – Berechtigung zum Mitführen von Audi – Unterlagen vorhanden sein.**