Informationssicherheit

Infrastruktur

Regelung Nr. 03.05.01

Physischer Schutz

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

Inhalt

I. Zweck

Diese Regelung legt die Sicherheitsanforderungen für IT-Räume.

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

Bei bereits vorhandenen IT-Räumen kann nach Abstimmung mit den verantwortlichen Stellen von den folgenden Regelungen abgewichen werden. Die Abweichungen müssen bewertet und dokumentiert werden. Neue Räume oder Räume nach ausführlicher Sanierung oder Modernisierung müssen die folgenden Anforderungen erfüllen.

1. IT-Räume

1.1. Ziel

Um die Sicherheit von IT-Komponenten (Vertraulichkeit, Integrität, Verfügbarkeit, Nachweisbarkeit) und Hilfsmitteln zu gewährleisten, sind physische Sicherheitsvorkehrungen erforderlich. Daher müssen sich IT-Komponenten und Hilfsmittel in geschützten Bereichen mit speziellen Sicherheitsmaßnahmen befinden. In diesem Kapitel werden diese Bereiche als „IT-Räume“ bezeichnet. Ziel dieses Kapitels ist die Festlegung der grundlegenden Anforderungen für die Einrichtung und den Betrieb von IT-Räumen.

1.2. Kategorien von IT-Räumen

Der Hausherr hat seine IT-Räume gemäß den hier beschriebenen Kategorien zu kategorisieren. Aus diesen ergeben sich dann die entsprechenden Anforderungen an die IT-Räume.

1.2.1 IT-Räume

IT-Räume können in drei Kategorien eingeteilt werden:

1.2.1.1 Firmenrechenzentren (Corporate Data Centres, CDCs), regionale Rechenzentren (Regional Data Centres, RDCs)

- Rechenzentren verfügen über die höchsten Sicherheitsstandards.
- CDC: Zentralisierung der weltweit verwendeten Anwendungen, Kompetenzen, Dienstleistungen und Management; Hot-Standby – Der Entfernte Standort übernimmt die globalen geschäftskritischen Anwendungen.
- RDC: Zentralisierung der regionalen Anwendungen, Kompetenzen, Dienstleistungen und Management; Hot-Standby (Lastverteilung) – Der entfernte Standort übernimmt die regionalen geschäftskritischen Anwendungen.

1.2.2 Lokale Datenräume (Local Data Rooms, LDRs)

Ein lokaler Datenraum hat reduzierte Sicherheitsstandards für:

- Bereitstellung von lokal genutzten Prozess- und Basisanwendungen, Dienstleistungen und Management; Hot-/Cold-Standby am Standort für lokale Anwendungen.

1.2.3 Verteilerräume (TRs)

Ein Verteilerraum umfasst in der Regel Folgendes:

- Verteilersysteme von Primär-, Sekundär- und Tertiärkabeln
- Dezentral verwendete aktive und passive Netzwerkkomponenten
- Diese Räume sind ausschließlich für Netzwerkelemente vorgesehen, die Endgeräte bereitstellen. In diesen Räumen dürfen sich keine Serversysteme befinden.

1.3. Allgemeine Anforderungen

- Der Verantwortliche für das Betreiben des IT-Raums ist zuständig für die ordnungsgemäße Nutzung der Sicherheitseinrichtungen, Einhaltung der Regelungen und das Sicherheitsbewusstsein der Mitarbeiter.
- Die IT-Räume müssen regelmäßig (Empfohlen: Jährlich) auf die Einhaltung der Sicherheitsmaßnahmen überprüft werden.
- Die Effizienz und Wirksamkeit der Sicherheitsmaßnahmen muss regelmäßig (Empfohlen: Jährlich) überprüft werden.
- Umgesetzte Maßnahmen müssen regelmäßig auf Einhaltung der Sicherheitsanforderungen überprüft werden. Abweichungen müssen dokumentiert und im Sicherheitskonzept begründet werden.
- Es müssen Benutzerregeln für IT-Räume[1] festgelegt und beachtet werden.
- Verkabelungsstandards sind zu beachten.
- Es muss ein Sicherheitskonzept erstellt werden, das mindestens folgende Aspekte abdeckt:

- Status quo-Analyse
- Risikoanalyse und -auswertung einschließlich Restrisiko
- Personelle, organisatorische, technische und strukturelle Maßnahmen
- Unterteilung des IT-Raums in verschiedene Sicherheitszonen[2]. Festlegung von angemessenen Schutzmaßnahmen für jede Zone.

- Alle zuständigen Stellen[3] müssen in die Ausarbeitung des Konzepts miteinbezogen werden.
- Das Sicherheitskonzept muss lokale Gesetze und Regelungen beachten.
- Das Sicherheitskonzept muss durch die zuständige Stelle (B.1.1) abgenommen werden.
- Die Minimum Standards „Zutrittsregelung“ der AUDI BRUSSELS müssen eingehalten werden.
- Die Minimum Standrads „Objektschutz“ der AUDI BRUSSELS müssen eingehalten werden

[1] Hausordnung

[2] Weitere Informationen finden Sie unter A.1.3 und A.1.4

[3] Siehe Anhang B.1.1

1.4. Nicht-IT-Räume

1.4.1 Verteiler-Schränke außerhalb geschlossener IT-Räume

Die folgenden Anforderungen müssen beachtet werden (Anforderungen aus vorangegangen Kapiteln entfallen)

Die Einrichtung von Verteiler-Schränken außerhalb geschlossener Verteilerräume ist von der zuständigen Stelle freizugeben, und wenn aufgrund der baulichen Bedingungen kein separater Verteilerraum möglich ist. Die folgenden Anforderungen müssen erfüllt sein:

- Die Schränke müssen gegen Staub und Spritzwasser geschützt sein
- Ausreichende Lüftung und (wenn erforderlich) Kühlung müssen sichergestellt sein.
- Die Schränke müssen vollständig geschlossen sein. Die Vorder- und Rückseite muss mit Schranktüren verschließbar sein
- Schutzmaßnahmen müssen an die Umgebung und mögliche Risiken angepasst werden (z. B. Zusammenstoß mit Fahrzeugen)
- Verkabelungsstandards müssen eingehalten werden

II. Verantwortlichkeiten

II.I Kapitel 1: IT-Räume

Diese Regelung muss von allen Stellen beachtet werden, die IT-Räume planen und betreiben.

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 Informationssicherheit Regelung Nr. 03.01.14 IT Service Continuity Management

A.1.3 Minimum Standard Objektschutz durch bzw. von Unternehmenssicherheit

A.1.4 Minimum Standard Zutrittsregelung durch bzw. von Unternehmenssicherheit

A.1.5 Sicherheitskonzeption durch bzw. von Unternehmenssicherheit

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.3 Abkürzungen und Definitionen

Begriff	Definition
Corporate Data Center (CDC)	Zentralisierung von weltweit genutzten IT Anwendungen, IT Support und IT Betrieb. Hot Standby unter Verwendung eines entfernten Standorts (Entfernung > 100 km). Der entfernte Standort übernimmt den Betrieb von weltweiten, geschäftskritischen Konzernanwendungen im Falle einer Störung.

Regional Data Center (RDC)	Zentralisierung von regional genutzten IT Anwendungen, IT Support und IT Betrieb. Hot Standby unter Verwendung eines entfernten Standorts. Der entfernte Standort übernimmt den Betrieb von geschäftskritischen regionalen Konzernanwendungen im Falle einer Störung.
Local Data Room (LDR)	Stellt grundlegende IT Dienste und Anwendungen für einen lokalen Standort zur Verfügung. Hot/Cold Standby am Standort für lokale Anwendungen.

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.

A.5 Dokumentenhistorie

Version	**Name**	**Org. Unit**	**Date**	**Comment**
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht

B. Spezifische Ausprägungen

B.1 Kapitel 1: IT Räume

B.1.1 Planung Versorgungstechnik, Hausherr (Betreiber), Gebäudemanagement, Unternehmenssicherheit, IT-Sicherheit