



**Informationssicherheit**

**Anwendungen**

**Regelung Nr. 03.04.01**

**Kommunikation und Kollaboration**

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

## Inhalt

<b>I. Zweck.....</b>	<b>3</b>
<b>1. Synchrone Kollaboration .....</b>	<b>3</b>
1.1. Ziel .....	3
1.2. Definition .....	3
1.3. Anwendungsfälle .....	3
1.4. Anforderungen.....	4
1.4.1 Grundlagen .....	4
1.4.2 Verantwortung von Moderatoren und Präsentatoren .....	4
1.4.3 Sicherheitsanforderungen für alle Kollaborationssysteme .....	4
1.5. Spezifische Anforderungen (Systeme und Teilnehmer) .....	5
1.5.1 Kollaboration unter Verwendung der Konzernsysteme .....	5
1.5.2 Kollaboration innerhalb des Konzerns mit außenstehenden Teilnehmern .....	5
1.5.3 Kollaboration außerhalb des Konzerns (Verwendung einer externen Lösung)...	6
1.6. Spezifische Anforderungen (Funktionalität).....	6
1.6.1 Chat .....	6
1.6.2 Instant Messaging .....	6
1.6.3 Whiteboard.....	7
1.6.4 Desktop-Sharing .....	7
1.6.5 Application-Sharing .....	7
1.6.6 Übergabe der Steuerung.....	7
1.6.7 Webcast.....	7
<b>II. Verantwortlichkeiten.....</b>	<b>8</b>
II.1 Kapitel 1: Synchrone Kollaboration .....	8
<b>Anhang .....</b>	<b>9</b>
<b>A. Allgemeines.....</b>	<b>10</b>
A.1 Mitgeltende Dokumente .....	10
A.2 Anlagen .....	10
A.3 Abkürzungen und Definitionen .....	10
A.4 Gültigkeit .....	11
A.5 Dokumentenhistorie.....	12
<b>B. Spezifische Ausprägungen.....</b>	<b>13</b>
B.1 Kapitel 1: Synchrone Kollaboration .....	13

## **I. Zweck**

Der Zweck dieser Regelung ist die Definition von Sicherheits-Anforderungen, sowie technischen und organisatorischen Anforderungen, für den Gebrauch von Kollaborationssystemen.

Im Sinne dieser Regelung bezeichnet der Begriff Informationssicherheit die IT-Sicherheit als Bestandteil der ganzheitlichen Informationssicherheit.

## **1. Synchrone Kollaboration**

### **1.1. Ziel**

Das Ziel dieser Regelung ist die Definition von Grundlagen und Anforderungen für die Verwendung von Kollaborationssystemen. Systeme für Remote-Support, Remote-Administration und Remote-Assistance sind nicht Bestandteil dieser Regelung.

### **1.2. Definition**

Systeme für die Zusammenarbeit können als virtuelle Teamräume betrachtet werden. In virtuellen Teamräumen kann asynchrone und synchrone Zusammenarbeit bereitgestellt werden.

Asynchrone Kollaboration besteht aus folgenden Funktionen:

- Virtuelle Chatrooms
- Diskussionsforen
- Dateiablage (Dateiverwaltung)

Synchrone Kollaboration besteht aus folgenden Funktionen<sup>1</sup>:

- Instant Messaging
- Webkonferenzen
  - Whiteboard
  - Desktop-Sharing
  - Application-Sharing
  - Webcast

### **1.3. Anwendungsfälle**

Man unterscheidet zwischen zwei Arten der Kollaboration:

- Präsentation
- Bearbeitung/Zusammenarbeit

Im Präsentationsmodus haben alle Teilnehmer (abgesehen vom Moderator/Präsentator) nur Lesezugriff.

---

<sup>1</sup> Siehe Anhang A.3

Im Bearbeitungsmodus haben alle Teilnehmer vollständigen Lese- und Schreibzugriff auf das Gerät des Data Providers.

## **1.4. Anforderungen**

### **1.4.1 Grundlagen**

- Es dürfen nur kollaborative Software und Systeme verwendet werden, die von der verantwortlichen Stelle<sup>2</sup> genehmigt wurde.
- Die genehmigten Lösungen dürfen nur mit den Daten (gemäß der Datenklassifizierung) verwendet werden, für die sie zugelassen wurden.
- Die Datenklassifizierung, die mit einer genehmigten, kollaborativen Software verwendet werden darf, muss dokumentiert und für die Benutzer zugänglich gemacht werden.

### **1.4.2 Verantwortung von Moderatoren und Präsentatoren**

Zur gemeinsamen Bearbeitung von Dokumenten ist immer ein Moderator erforderlich.

- Der Moderator/Präsentator ist für den bereitgestellten Inhalt und dessen Vertraulichkeit verantwortlich.

Kollaborations-Services dürfen nur für geschäftliche Zwecke verwendet werden. Aufgaben des Moderators sind:

- Die Sitzung muss vom Moderator eingeleitet werden.
- Die Teilnehmer müssen vom Moderator eingeladen werden.
- Nur der Moderator darf die Möglichkeit haben, Teilnehmern die Berechtigung für die Teilnahme an einer Sitzung zuzuteilen.
- Die gesamte Gruppe darf nur dann Eigentümer oder Autor eines Dokuments sein, wenn dieses über ein System erstellt wurde, welches integrierte Authentifizierung und Protokollierung in Übereinstimmung mit den Anforderungen zur Nachweisbarkeit<sup>3</sup> bereitstellt. Die Nachvollziehbarkeit der Ersteller muss also gegeben sein.
- Der Moderator trägt die allgemeine Verantwortung für die Sitzung und alle präsentierten oder bearbeiteten Dokumente.

### **1.4.3 Sicherheitsanforderungen für alle Kollaborationssysteme**

- Das System muss eine zentrale, angemessene Authentifizierungsfunktion für alle Teilnehmer aufweisen (z. B. eine Windows-Anmeldung), die der Datenklassifizierung entspricht, für welche die Software entwickelt wurde.
- Das System muss zwischen Lese- und Schreibzugriff unterscheiden können.
- Nur der Moderator darf die Möglichkeit haben anderen Teilnehmern Rollen und Rechte zuzuteilen.
- Alle Teilnehmer müssen vom Moderator autorisiert werden.

---

<sup>2</sup> Siehe Anhang B.1.1

<sup>3</sup> Siehe Anhang A.1.2

- Die Teilnehmer eine Sitzung müssen gemäß den entsprechenden Regelungen protokolliert werden<sup>4</sup>.
- Sitzungen dürfen nicht durch die Teilnehmer aufgezeichnet werden können.
- Der Moderator darf die Sitzung nur mit Einverständnis aller Teilnehmer aufzeichnen. Es müssen zusätzliche rechtliche oder unternehmensspezifische Regelungen beachtet werden<sup>5</sup>.
- Nur der Moderator darf die Möglichkeit haben Dokumente zu speichern.
- Alle bereitgestellten Autorisierungen und Berechtigungen dürfen nur für eine einzelne Sitzung gültig sein.
- Das System muss die ungewollte Freigabe von Informationen (z. B. default-Einstellung zur Freigabe des Desktops oder allen Applikationen) verhindern.
- Die Übertragungsverschlüsselung muss gemäß des Stands der Technik und der Regelung zu Kryptographie<sup>6</sup>, verwendet werden.
- Kollaboration mit Hilfe von Standardanwendungen wie Word, Excel usw. sollte serverbasiert stattfinden. So hängt die Sicherheit der Dokumente nicht vom Client selbst ab und ein hohes Sicherheitsniveau kann zentral durchgesetzt werden.

## **1.5. Spezifische Anforderungen (Systeme und Teilnehmer)**

### **1.5.1 Kollaboration unter Verwendung der Konzernsysteme**

In diesem Fall ist das kollaborative System (z.B. Skype for Business) freigegeben und wurde durch den Konzern bereitgestellt.

Die in Kapitel 1.4.1 und 1.4.3 definierten Anforderungen sind zu beachten.

### **1.5.2 Kollaboration innerhalb des Konzerns mit außenstehenden Teilnehmern**

In diesem Fall ist das kollaborative System (z.B. Skype for Business) freigegeben und wurde durch den Konzern bereitgestellt. Es kann von außenstehenden Teilnehmern über das Internet verwendet werden.

- Zusätzlich zu den in Kapitel 1.4.1 und 1.4.3 definierten Anforderungen müssen rechtliche und unternehmensspezifische Regelungen<sup>7</sup> für die Autorisierung von außenstehenden Teilnehmern sowie die Vorgaben zu Geheimhaltungsvereinbarungen<sup>8</sup> beachtet werden.

die Kommunikation muss über ein Sicherheitsgateway erfolgen.

---

<sup>4</sup> Siehe Anhang A.1.2

<sup>5</sup> Siehe Anhang B.1.2

<sup>6</sup> Informationssicherheit Regelung Nr. 03.01.02 Kryptographie

<sup>7</sup> Siehe Anhang A.1.4

<sup>8</sup> NDA für interne Daten, Audits für vertraulich/geheime Daten

### 1.5.3 Kollaboration außerhalb des Konzerns (Verwendung einer externen Lösung)

In diesem Fall wird das kollaborative System durch einen Partner oder Dritten bereitgestellt und durch Konzern-Mitarbeiter verwendet.

- Sofern das System nicht durch einen freigegebenen Partner<sup>9</sup> bereitgestellt wird, ist diese Art der Kollaboration nur bei öffentlichen Daten oder Daten ohne Verweise auf den Konzern (z. B. Produktpräsentationen eines Herstellers) zulässig.
- Für alle anderen Daten (intern/vertraulich/geheim) muss der Partner, dessen kollaboratives System verwendet wird entsprechend der relevanten Prozesse<sup>10</sup> freigegeben sein.
- Lösungen, die nicht innerhalb des Audi-Netzwerks gehostet werden, dürfen nur verwendet werden, wenn sie zusätzlich die folgenden Bedingungen erfüllen und von der verantwortlichen Stelle<sup>11</sup> freigegeben wurden:
  - Übertragungsverschlüsselung muss gemäß des Stands der Technik und der Regelung zu Kryptographie<sup>12</sup>, verwendet werden
  - Keine externe Speicherung von Informationen (nur Übertragung von Bildschirminhalten)

## 1.6. Spezifische Anforderungen (Funktionalität)

### 1.6.1 Chat

- Es sind nur Textnachrichten zulässig.
- Andere Informationen (z. B. Dateien) dürfen nicht übertragen werden.
- Informationen mit der Klassifizierung „öffentlich“ dürfen über Chat übertragen werden.
- Die Übertragung von Informationen mit der Klassifizierung „intern“ sollte bevorzugt auf anderen Wegen erfolgen.

### 1.6.2 Instant Messaging

- Das System muss Anwesenheitsanzeigen für Teilnehmer bereitstellen.
- Die Benutzer müssen den Status ihrer Anwesenheitsanzeige ändern können.
- Teilnehmer dürfen nicht zur Verwendung des Instant Messaging verpflichtet sein und müssen sich jederzeit abmelden können.
- Die Übertragung muss verschlüsselt werden.
- Es dürfen keine Dateien über Instant Messaging übertragen werden.
- Rechtliche oder unternehmensspezifische Regelungen<sup>13</sup> müssen beachtet werden.

---

<sup>9</sup> NDA für interne Daten, Audits für vertraulich/geheime Daten

<sup>10</sup> NDA für interne Daten, Audits für vertraulich/geheime Daten

<sup>11</sup> Siehe Anhang B.1.1

<sup>12</sup> Informationssicherheit Regelung Nr. 03.01.02 Kryptographie

<sup>13</sup> Siehe Anhang B.1.3

### **1.6.3 Whiteboard**

- Keine zusätzlichen Anforderungen.

### **1.6.4 Desktop-Sharing**

- Sollte vermieden werden, da das Risiko einer unbeabsichtigten Preisgabe von Informationen besteht. Application-Sharing ist zu bevorzugen.

### **1.6.5 Application-Sharing**

- Im Präsentationsmodus und für Standarddokumente ist eine serverbasierte Lösung vorzuziehen.
- Application-Sharing ist zulässig, wenn die Anforderungen in Kapitel 1.4.1 und 1.4.3 erfüllt sind.

### **1.6.6 Übergabe der Steuerung**

- Nur zulässig, wenn der verantwortlichen Benutzer, dessen Account verwendet wird, den freigegebenen Desktop genau und mit Expertise überwacht.
- Es muss für den verantwortlichen Benutzer jederzeit die Möglichkeit bestehen, die Übergabe der Steuerung zu beenden.
- Muss auf die Freigabe von geteilten Applikationen beschränkt sein (und nicht Desktops – mit der Ausnahme von remote support, wie z.B. durch den Helpdesk).

### **1.6.7 Webcast**

- Für Präsentationen zulässig
- Für Zusammenarbeit zulässig, wenn die Anforderungen in Kapitel 1.4.1 und 1.4.3 erfüllt sind.

## **II. Verantwortlichkeiten**

### **II.I Kapitel 1: Synchrone Kollaboration**

Diese Regelung ist von allen Planern, Einkäufern, Implementierern und Anwendern von kollaborativer Software einzuhalten und anzuwenden.

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 Mitarbeiterinnen und Mitarbeiter

#### A.1.3 Informationssicherheitshandlungsleitlinien für Systementwickler

#### A.1.4 Informationssicherheitshandlungsleitlinien für Partnerfirmen

### 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](mailto:it-security.audibx@audi.de)

### A.3 Abkürzungen und Definitionen

Abkürzung/Begriff	Erläuterung
Chat	Echtzeit-Übertragung von Textnachrichten.  Im Rahmen dieser Regelung kann es sich um eine webbasierte Anwendung (virtuellen Chatroom) oder eine Funktion eines Webkonferenz-Diensts vom zentralen Serversystem handeln.  Die ausgetauschten Informationen müssen mit Bedacht eingegeben werden.
Instant Messaging	Echtzeit-Übertragung von Textnachrichten vom Absender an den Adressaten (Peer-to-Peer).

	<p>Im Rahmen dieser Regelung handelt es sich um eine Client-basierte Anwendung.</p> <p>Die ausgetauschten Informationen müssen mit Bedacht eingegeben werden.</p>
Anwesenheitsanzeige	Statusanzeige über die Verfügbarkeit oder Bereitschaft des Benutzers, Kommunikation anzunehmen (z. B. Verfügbar, Beschäftigt, Abwesend und Nicht Stören). Die Anwesenheitsanzeige kann vom Benutzer festgelegt werden.
Webkonferenzen	Webkonferenzen ist der Oberbegriff für verschiedene Funktionen, z. B. Whiteboard, Desktop-Sharing, Application-Sharing und Webcast. Webkonferenzen ermöglichen das Organisieren von Onlinesitzungen mit Teilnehmern an unterschiedlichen Standorten. Die Teilnehmer können einander Dokumente oder Anwendungen präsentieren und gemeinsam an Dokumenten arbeiten.
Whiteboard	Die Funktion „Whiteboard“ ermöglicht es den Teilnehmern, Kommentare zu den übertragenen Inhalten hinzuzufügen, die von allen anderen Teilnehmern gelesen werden können.
Desktop-Sharing	Übertragung einer Ansicht des Desktops oder Zugriff auf den Desktop eines lokalen Clients für andere Teilnehmer. Das Konto des derzeit angemeldeten Benutzers lässt die gleichzeitige Verwendung mit Leserechten oder mit Änderungen zu.
Application-Sharing	Übertragung einer Ansicht der Anwendung oder Zugriff auf die Anwendung auf einem lokalen Client für andere Teilnehmer. Das Konto des derzeit angemeldeten Benutzers lässt die gleichzeitige Verwendung mit Leserechten oder mit Änderungen zu.
Webcast	Hochladen eines Dokuments auf einen Server. Nur eingeladene Personen können an der Präsentation teilnehmen. Die Teilnehmer können die Inhalte nicht ändern.
Moderator	Benutzer/Rolle. Der Moderator leitet eine Sitzung ein und verwaltet sie.
Teilnehmer	Benutzer/Rolle. Teilnehmer werden vom Moderator eingeladen und können über eine Anwendung an der Sitzung teilnehmen.
Präsentator	Benutzer/Rolle (kann Teilnehmer oder Moderator sein). Der Präsentator zeigt den anderen Teilnehmern der Sitzung den eigenen Desktop bzw. die Anwendung (Präsentationsmodus).

## 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<sup>14</sup>.

## A.5 Dokumentenhistorie

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

---

<sup>14</sup> Siehe Anhang A.2.1 Anlage 1 Feedbackformular

## **B. Spezifische Ausprägungen**

### **B.1 Kapitel 1: Synchrone Kollaboration**

**B.1.1 Verantwortlich für die Freigabe von Software: IT-Services -- Freigabe hinsichtlich Sicherheit durch IT-Sicherheit**

**B.1.2 Generell mit Rechtsabteilung, DPO und Personalwesen abzustimmen. Die Speicherung der Daten hat je nach Datenklassifikation ggf. verschlüsselt zu erfolgen.**

**B.1.3 Keine weiteren Angaben**