Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.10

Awareness und Training

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

Inhalt

I. Zweck 3
1. Schulung 3
1.1. Ziel 3
1.2. Allgemeine Anforderungen 3
1.3. Anforderungen für die Einstellung neuer Mitarbeiter (intern und für Dritte) 4
1.4. Anforderungen für den Standortwechsel neuer Mitarbeiter (intern und für Dritte) 5
2. Sensibilisierungskampagnen 6
2.1. Ziel 6
2.2. Allgemeine Anforderungen 6
II. Verantwortlichkeiten 7
II.I Kapitel 1: Schulung 7
II.II Kapitel 2: Awareness Kampagnen 7
Anhang 8
A. Allgemeines 9
A.1 Mitgeltende Dokumente 9
A.2 Referenzen zu Standards 9
A.3 Anlagen 9
A.4 Gültigkeit 10
A.5 Dokumentenhistorie 10
B. Spezifische Ausprägungen 11
B.1 Kapitel 1: Schulung 11
B.2 Kapitel 2: Awareness Kampagnen 11

I. Zweck

Das Informationssicherheitsniveau der AUDI BRUSSELS hängt hauptsächlich ab von dem umsichtigen Verhalten der Arbeitnehmer und der Mitarbeiter von Dritten (z. B. Auftragnehmern), die mit vertraulichen Informationen der AUDI BRUSSELS arbeiten. Die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen kann nur sichergestellt werden, wenn die Mitarbeiter und die betroffenen Parteien die Notwendigkeit der Informationssicherheit verstehen und sie bezüglich der implementierten Sicherheitsmaßnahmen informiert und geschult wurden.

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

Der Zweck dieser Regelung ist die Definition von Anforderungen für folgende Bereiche:

- Erhöhen des Bewusstseins der AUDI BRUSSELS-Mitarbeiter zu Themen der Informationssicherheit
- Definieren der organisatorischen Anforderungen für Schulungen, um dieses Ziel zu erreichen

1. Schulung

1.1. Ziel

Das Ziel dieses Kapitels ist die Definition von Anforderungen für das Unternehmen und die Ausführung der Informationssicherheitsschulungen.

1.2. Allgemeine Anforderungen

- Die Mitarbeiter und relevante Parteien müssen auf die Notwendigkeit der Informationssicherheit hingewiesen werden und zu Sicherheitsmaßnahmen als Teil des Schulungsprogramms zur Informationssicherheit aufgeklärt und geschult werden.
- Das Schulungsprogramm zur Informationssicherheit muss auf die spezifische Zielgruppe zugeschnitten werden. Diese Schulung muss mindestens folgende Themen umfassen:

- Schulungsmaterialien, die bestimmte Themen abdecken, die auf verschiedene Zielgruppen zugeschnitten sind (z. B. Management, Administratoren, Personalabteilung, Entwickler, Standardbenutzer und andere Rollen, die von dem jeweiligen Unternehmen festgelegt wurden).
- Kombination relevanter Themen für jede Zielgruppe.

- Das Schulungsprogramm zur Informationssicherheit muss von der oberen Geschäftsleitung abgesegnet sein. Das Management muss sicherstellen, dass die Schulungen durchgeführt werden.
- Die Mitarbeiter müssen Schulungsgruppen zugewiesen werden und in regelmäßigen Abständen für Schulungen im Schulungsplan eingeteilt werden.

- Themen und Inhalte, die in den Schulungen enthalten sind, müssen, abhängig von den aktuellen IS-Risiken der Organisation (einschließlich Top-Risiken), ihren Auswirkungen und den Maßnahmen zur Abmilderung, regelmäßig aktualisiert werden.[1]
- Das Schulungsprogramm muss regelmäßig geprüft werden, um seine Effektivität (z. B. durch Umfragen vor Ort oder online, Audits), Effizienz und Durchführbarkeit zu bemessen.
- Die zuständige Stelle[2] muss Schulungsmaterialien zur Verfügung stellen (z. B. Präsentationen, webbasierte Schulungen), die vor Ort übernommen werden können.
- Die Schulungen werden von der zuständigen Stelle durchgeführt[3].
- Der Schulungsleiter muss entsprechende Kompetenzen vorweisen können, um die Schulung durchzuführen (z.B. Arbeitserfahrung, Zertifikate oder Schulungen).
- Der Schulungsinhalt muss mindestens einmal pro Jahr auf Aktualität geprüft und ggf. angepasst werden.
- Schulungen müssen Themen enthalten, die bereits durch andere Maßnahmen abgedeckt wurden (z. B. Sensibilisierungskampagnen), um das Gelernte zu festigen.
- Ein jährlicher Schulungsplan muss von der zuständigen Stelle zusammengestellt werden[4], die folgende Verantwortlichkeiten hat:

- Erstellen des Schulungsplans
- Festlegen, welche Zielgruppe zu welchen Themen geschult wird.

- Es muss gemäß rechtlichen Schutzfristen festgehalten werden, wer an geplanten Schulungen teilgenommen hat.
- Der Schulungsplan muss der Situation angepasst werden, z. B. wenn Sicherheitsvorfälle gehäuft auftreten.
- Alle Schulungsthemen, die für eine bestimmte Zielgruppe wichtig sind, müssen einmal pro Jahr wiederholt werden.

1.3. Anforderungen für die Einstellung neuer Mitarbeiter (intern und für Dritte)

- Jeder Mitarbeiter muss zu Beginn der Anstellung über die grundlegenden Informationssicherheitsanforderungen und -verantwortlichkeiten innerhalb seines jeweiligen Verantwortungsbereichs und seiner Funktion informiert werden. Die anfänglich gegebenen Informationen müssen dokumentiert werden (z. B. durch die Unterschrift eines Mitarbeiters).

[1] A.1.2

[2] Siehe B.1.1

[3] Siehe B.1.2

[4] Siehe B.1.1

- Jeder neue Mitarbeiter muss auf die Informationssicherheitsrichtlinien und -regelungen zugreifen können.
- Jeder neue Mitarbeiter muss darauf hingewiesen werden, wo sich die aktuellen Informationssicherheitsrichtlinien und -regelungen befinden (z. B. Intranet).
- Die organisationseinheits- oder funktionsspezifischen Informationssicherheitsanforderungen innerhalb des Aufgabenbereichs des Mitarbeiters müssen verfügbar gemacht oder in Schriftform ausgehändigt werden.

1.4. Anforderungen für den Standortwechsel neuer Mitarbeiter (intern und für Dritte)

- Alle oben genannten Anforderungen gelten auch für die Änderung des Aufgabenbereichs des Mitarbeiters.
- Der (neue) Vorgesetzte ist für die intensive Einführung der Mitarbeiter verantwortlich, die innerhalb des Audi Konzerns ihren Aufgabenbereich wechseln. Neben funktionalen Aspekten gehören dazu auch relevante Informationssicherheitsanforderungen des neuen Aufgabenbereichs.

2. Sensibilisierungskampagnen

2.1. Ziel

Das Ziel dieses Kapitels ist das Definieren von Anforderungen für Sensibilisierungskampagnen zur Informationssicherheit.

Das Ziel einer Sensibilisierungskampagne ist ein grundlegendes Sicherheitsverständnis, um Informationssicherheitsbedrohungen und -vorfälle zu erkennen und angemessen darauf zu reagieren und um die Exposition von Informationswerten durch Achtlosigkeit oder Unwissenheit zu verhindern.

2.2. Allgemeine Anforderungen

- Sensibilisierungskampagnen müssen regelmäßig durchgeführt werden, um die Mitarbeiter für Informationssicherheit zu sensibilisieren.
- In Sensibilisierungskampagnen werden für bestimmte Themen und Zielgruppen über einen festgelegten Zeitraum medienübergreifende Inhalte (Maßnahmen sind z. B. Flyer, Quiz, Zeichen, Poster) verwendet. Pro Jahr sollte mindestens eine Maßnahme ausgeführt werden.
- Die verantwortliche Stelle[5] muss Sensibilisierungsmaterial zur Verfügung stellen, die von Gruppenunternehmen lokal übernommen werden kann.
- Manager müssen an Sensibilisierungskampagnen zur Verstärkung beteiligt werden, um ein nachhaltiges Informationssicherheitsbewusstsein für Mitarbeiter zu erreichen.
- Sensibilisierungskampagnen müssen vom Management und von anderen beteiligten Organisationseinheiten unterstützt werden (d. h. Datensicherheit, GRC, Personalabteilung, Rechtsabteilung).
- Ergebnisse und Umfragen sollten dem Management in regelmäßigen Abständen über offizielle Kommunikationskanäle vorgelegt werden (d. h. IS-Lenkungsausschüsse, jährliche Berichte).

[5] Siehe B.2.1

II. Verantwortlichkeiten

II.I Kapitel 1: Schulung

Diese Regelung ist von allen OEs 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: Awareness Kampagnen

Diese Regelung ist von allen OEs 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 Informationssicherheit Regelung Nr. 03.01.15 Risikomanagement in der Informationssicherheit

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**
Management responsibilities	1.2, 2.2	A.7.2.1	A.8.2.1	7.2
Information security awareness, education and training	1.2, 2.2	A.7.2.2	A.8.2.2	7.2
Disciplinary process		A.7.2.3	A.8.2.3	-

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[6].

A.5 Dokumentenhistorie

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

[6] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Schulung

B.1.1 IT-Sicherheitsschulungen werden von der IT-Sicherheit erstellt.

B.1.2 Die IT-Sicherheitsveranstaltungen werden von den Verantwortlichen für IT-Sicherheit durchgeführt oder veranlasst.

B.2 Kapitel 2: Awareness Kampagnen

B.2.1 Die IT-Sicherheit stellt das Sensibilisierungsmaterial zum Thema IT-Sicherheit zur Verfügung.