Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.13

Asset Management

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 Definition von Sicherheitsanforderungen für die Identifizierung organisationseigener Assets im Zusammenhang mit Informationssicherheit und die Definition angemessener Maßnahmen zu ihrem Schutz.

1 Assets

1.1 Ziel

In diesem Kapitel werden die Sicherheitsanforderungen für Assets im Zusammenhang mit Informationssicherheit definiert.

1.2 Definition

1.2.1 Assets

Der Begriff Assets (bzw. Werte) umfasst alles, was für das Unternehmen von Wert ist [1] (materielle Assets, Informations-Assets).

1.2.2 Materielle Assets

Im Zusammenhang mit Informationssicherheit handelt es sich bei materiellen Assets um Werte, die zur Erfassung, Verarbeitung, Speicherung und Kommunikation von Informationen genutzt werden. Beispiele:

- Alle Komponenten der IT-Infrastruktur (Router, Switch, Firewall etc.)
- Server
- PCs
- Laptops
- Mobile Endgeräte (z. B. HDT, Smartphones, Tablets)
- Multifunktionsgeräte (Drucker, Kopierer, Scanner, Faxe)
- Telefone
- Speichermedien (z. B. Festplatten, USB-Sticks, Speicherkarten, CDs, DVDs)
- Karteikarten und Pläne aus Papier
- IT-Support-Infrastruktur (z. B. Stromleitungen, Brandschutz)
- Gebäude (z. B. Rechenzentren)

1.2.3 Informations-Assets

Informations-Assets sind Prozesse und Verfahren oder Kenntnisse bzw. Daten (einschließlich persönlicher Daten), die für die Organisation unabhängig von deren Form (auf Papier oder digital) von Wert sind. Dies bezieht sich auch auf Informations-Assets, die auf digitalen Medien gespeichert oder von Software verarbeitet werden (z. B. Dateien, Datenbanken) sowie Software selbst. Hierzu gehören auch Lizenzen für Software.

1.3 Inventar

- Für materielle Assets und Informations-Assets[2] ist ein Inventar zu erstellen. Daher ist es notwendig, einen Inventarisierungsprozess zu definieren. Es können verschiedene Inventarisierungen[3]

[1] Definition gemäß ISO/IEC 27000.
[2] Die KSU-Anforderungen müssen erfüllt werden.
[3] Siehe Anhang B.2.1.1

genutzt werden, doch müssen sie einen vollständigen Überblick über das Inventar gewähren. Folgende Informationen müssen zumindest dokumentiert werden:

- Eindeutige ID
- Speicher-/Aufbewahrungsort
- Zuständige Person oder Abteilung
- Klassifikation (Schutzbedarf, Kritikalität)
- Zweck

- Weitere nützliche Informationen:
  - IP-Adressen
  - SLAs
  - Wartungsverträge
  - Lizenzen

1.4 Lebenszyklus der Assets

- Für materielle Assets und Informations-Assets ist die Definition eines Eigentümers erforderlich, der während des Lebenszyklus eines Assets für diesen zuständig ist.
  - Assets sollten gruppiert werden (z. B. hinsichtlich des unterstützten IT-Services)
  - Für jede Gruppe muss ein Asset-Eigentümer benannt werden.
  - Der Asset-Eigentümer muss vom Eigentümer der Information darüber informiert werden, wenn abhängige Assets das Ende ihres Lebenszyklus erreichen und zerstört werden. Alternativ kann der Status des Lebenszyklus ggf. auch der Kennzeichnung des abhängigen Assets entnommen werden.
- Der Lebenszyklus besteht aus folgenden Schritten:
  - Erstellung/Erwerb
  - Betrieb/Änderung
  - Löschung/Zerstörung

1.5 Handhabung der Assets

1.5.1 Klassifikation

- Alle Informations-Assets müssen gemäß den Anforderungen der Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter eingestuft werden[4] um den **Schutzbedarf** zu bestimmen.
- Des Weiteren ist eine Einstufung bzgl. **Kritikalität** im Kontext Business Continuity Management / IT Service Continuity Management durchzuführen. Hierbei ist die Priorität für Problemerhebung im Fehler / Desaster-Fall zu ermitteln, um die Kontinuität von Business-Prozessen zu gewährleisten.
- Materielle Assets, die Informations-Assets enthalten, verarbeiten oder transportieren, erben die Klassifikation der entsprechenden Informations-Assets.
  - Je nach Klassifikation müssen Anforderungen an die Handhabung von Assets[5] definiert und umgesetzt werden.

[4] Siehe Anhang A.1.2
[5] Siehe Anhang A.1.2 und A.1.3

1.5.2 Kennzeichnung

- Informations-Assets müssen mit ihrer Klassifikation gekennzeichnet werden.
  - Für die Kennzeichnung müssen je nach Klassifikationsschema entsprechende Verfahren entwickelt und umgesetzt werden.

1.5.3 Physischer Schutz

- Assets müssen je nach ihrer Klassifikation geschützt werden.
  - Für jede Asset-Klasse müssen geeignete Schutzmaßnahmen definiert und dokumentiert werden[6].

[6] Z. B. in einer CMDB

II Verantwortlichkeiten

II.I Kapitel 1: Assets

Diese Regelung ist von allen Betreibern von IT-Systemen und allen Asset-Eigentümern 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. 03.01.09 Ausnahmeprozess

A.1.2 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

A.1.3 Information-Security-Wiki

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 (2014)
Inventory of assets	1.3	A.8.1.1	A.7.1.1	8.1
Ownership of assets	1.4	A.8.1.2	A.7.1.2	8.1
Acceptable use of assets	1.5	A.8.1.3	A.7.1.3	8.1
Classification of information	1.5.1	A.8.2.1	A.7.2.1	8.2
Labelling of information	1.5.2	A.8.2.2	A.7.2.2	8.2
Handling of assets	1.5	A.8.2.3	A.10.7.3	8.2

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: 01.10.2023

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[7].

A.5 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	01.10.2020	Veröffentlicht

[7] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B Spezifische Ausprägungen

B.1 Konzernweit

Dieses Kapitel beinhaltet spezifische Ausprägungen die innerhalb des gesamten Konzerns gelten. Diese Ausprägungen dürfen durch die Gesellschaften nicht geändert werden.

B.1.1 Kapitel 1: Assets

-

B.2 Gesellschaftsweit

Dieses Kapitel beinhaltet spezifische Ausprägungen die innerhalb der Gesellschaft gültig sind. Diese Ausprägungen müssen durch die Gesellschaften auf die jeweiligen Gegebenheiten angepasst werden. Bei manchen Ausprägungen ist zur Information in kursiver Schrift angegeben welche Vorgaben für Volkswagen Marke gelten.

B.2.1 Kapitel 1: Assets

B.2.1.1 z.B. *planningIT*, IT-Landscape, Command, Excel-Tabelle. Der jeweilige Asset-Eigentümer bzw. Verantwortliche für das Asset-Management muss sicherstellten, dass ein geeignetes System verwendet wird.