Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.06

Backup und Archivierung

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 an die Datensicherung und Archivierung für alle IT-Systeme. Es besteht keine Definition für die Anforderungen an die Client-Rechner, da auf Clients die Benutzer für die Datensicherung und Archivierung verantwortlich sind[1].

1. Datensicherung und Archivierung

1.1. Ziel

Das Ziel dieses Kapitels besteht in der Definition der erforderlichen Anforderungen an den Betrieb von IT-Systemen (Anlagen, die der Informationsverarbeitung dienen, z.B. Server, Clients, Switches oder Sicherheitsgateways) bezüglich Datensicherung und Archivierung. Dadurch soll es bei einem Ausfall möglich sein, relevante Daten auf einem reparierten oder ausgetauschten System wiederherzustellen.

1.2. Allgemeine Anforderungen

- Die für ein IT-System zuständige Einheit ist für die Festlegung und Dokumentation eines Datensicherungs- und Archivierungskonzepts verantwortlich. Dies geschieht unter Berücksichtigung der Verfügbarkeitsklasse sowie der rechtlichen und unternehmensspezifischen Anforderungen. Das Konzept muss zumindest folgende Aspekte umfassen:
  - Häufigkeit der Datensicherung (Echtzeit, täglich, wöchentlich usw.)
  - Art der Datensicherung (vollständig, inkrementell, differenziell usw.)
  - Aufbewahrungsfrist[2]
  - Schutzbedarf gemäß der Systemeinstufung der gespeicherten Informationen (z. B. Verschlüsselung)
  - Definition des Speicherortes für die Sicherungsdateien
  - Beschreibung des Importprozesses für eine Sicherungsdatei
  - Bestimmung der zum Beantragen eines Imports einer Sicherungsdatei autorisierten Personen
  - Bestimmung der für den Import einer Sicherungsdatei autorisierten/zuständigen Personen
  - Definition der zum Sicherstellen der erfolgreichen Datensicherung erforderlichen Prüfungen
  - Häufigkeit und Art der Tests für die Wiederherstellung von Datensicherungen
  - Bestimmung der für die Erstellung von Datensicherungen und Durchführung von Sicherungstests zuständigen Einheit
  - Definition der Protokollierungsanforderungen

[1] Siehe Anhang A.1.2

[2] Siehe Anhang A.1.4

- Datensicherungen und archivierte Dateien/Medien müssen vor unautorisiertem Zugriff geschützt werden.
  - Es muss sichergestellt werden, dass ausschließlich die zuständigen Administratoren Zugriff auf die Datensicherungen erhalten.
  - Es dürfen nur personalisierte Benutzerkonten verwendet werden.
  - Datensicherungen und archivierte Medien müssen vor physischen Schäden oder Umwelteinflüssen geschützt werden.
  - Datensicherungen und archivierte Medien müssen gemäß den Anforderungen der Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren[3] aufbewahrt werden.
- Enthält eine Datensicherung Daten mit verschiedenen Verfügbarkeitsklassen, müssen die Anforderungen an die Verfügbarkeitsklasse der jeweils kritischsten Daten erfüllt werden.
  - Die Definition angemessener Mechanismen zur Datensicherung und Archivierung erfolgt auf der Grundlage der Definition der Verfügbarkeitsklasse der Systeme seitens der Eigentümer. Wird die Verfügbarkeitsklasse des Systems nicht definiert, ist der Eigentümer für deren Definition zuständig. Der Eigentümer kann dabei ggf. vom Systembetreiber unterstützt werden.
  - Für die Systemeinstufung sind die durch die Fachabteilung definierten Verfügbarkeitsklassen[4] [5] zu verwenden.
  - Die Einstufung der Datensicherungen erfolgt auf der Grundlage der Verfügbarkeitsklasse der enthaltenen Daten.
- Es muss eine Kapazitätsplanung durchgeführt werden, um zu gewährleisten, dass auf den Sicherungsmedien stets ausreichend Speicherplatz vorhanden ist.
- Es muss während der gesamten Aufbewahrungsfrist sichergestellt sein, dass die gesicherten oder archivierten Daten jederzeit les- und nutzbar sind (z. B. muss die Sicherungstechnologie unterstützt werden und eine Entschlüsselung möglich sein).
  - Die relevanten rechtlichen und unternehmensspezifischen Anforderungen (z. B. rechtliche Aufbewahrungsfristen) müssen identifiziert, dokumentiert und erfüllt werden.
  - Zum Testen der Datensicherungen hinsichtlich Les- und Nutzbarkeit müssen Zeitplanungen erstellt werden.
- Datensicherungs- und Archivierungsmedien müssen so ausgewählt werden, dass sie die maximal benötigte Laufzeit überdauern.

[3] Siehe Anhang A.1.3

[4] Siehe Anhang A.1.2

[5] Siehe Anhang A.1.5

  - Es müssen Richtlinien zur Auswahl geeigneter Datensicherungs- und Archivierungsmedien definiert und befolgt werden.[6]
  - Wenn die gesamte Aufbewahrungsfrist nicht von derselben Technologie abgedeckt werden kann, muss eine Migration zu alternativen Sicherungsmedien gewährleistet werden.

- Datensicherungen und archivierte Medien müssen gemäß den Anforderungen der Datenklasse auf den Medien gelöscht bzw. zerstört werden, wenn die Medien nicht länger genutzt oder anderweitig eingesetzt werden.

[6] Bitte beachten Sie die unter A.1.6 Book of Standards beschriebenen Methoden und Medien.

II. Verantwortlichkeiten

II.I Kapitel 1: Backup und Archivierung

Diese Regelung ist von allen Betreibern von IT-Systemen 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 für Mitarbeiterinnen und Mitarbeiter

A.1.3 Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren

A.1.4 URLB_014 Aufbewahrung von Unterlagen

A.1.5 Informationssicherheit Regelung Nr. 03.01.14 IT Service Continuity Management

A.1.6 Book of Standards

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)
Information backup	1	A.12.3.1	A.10.5.1	12.4

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[7].

A.5 Dokumentenhistorie

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

[7] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Backup und Archivierung

-