Dokument	501
Autor:	Cornelia Vogt
Freigegeben von:	Hans-Werner Rückwardt
Freigabedatum:	28.04.2023
Vertraulichkeitsstufe:	intern

BJA automotive GmbH

Informationssicherheits-Leitlinie

Inhaltsverzeichnis

1. Zweck, Anwendungsbereich und Anwender

Ziel dieser übergeordneten Leitlinie ist es, den Zweck, die Ausrichtung, die Grundsätze und die Grundregeln für das Informationssicherheitsmanagement zu definieren.

Diese Richtlinie gilt für das gesamte Informationssicherheits-Managementsystem (ISMS), wie es im ISMS-Anwendungsbereich-Dokument, definiert ist.

Nutzer dieses Dokuments sind alle Mitarbeiter des Unternehmens BJ Automotive GmbH sowie relevante externe Parteien.

2. Referenzdokumente

- ISO/IEC 27001-Norm, Abschnitte 5.2 und 5.3 sowie VDA ISA v. 5.1
- ISMS-Anwendungsbereich: Dokument 603 Risikomatrix.xlsx Tabelle 4.3 ISMS Scope
- Siehe hierzu Dokument 505 – Liste der relevanten Dokumente

3. Verweis auf ISMS-Richtlinien -und Verfahren

- Siehe hierzu Dokument 505 – Liste der relevanten Dokumente

4. Grundlegende Terminologie der Informationssicherheit

Vertraulichkeit – Eigenschaft der Information, durch die sie nur für autorisierte Personen oder Systeme verfügbar ist.

Integrität – Eigenschaft der Information, durch die sie nur von autorisierten Personen oder Systemen in zulässiger Weise verändert wird.

Verfügbarkeit – Eigenschaft der Information, durch die sie von autorisierten Personen abgerufen werden kann, wenn sie benötigt wird.

Informationssicherheit - Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

ISMS (Information Security Management System) – Teil des gesamten Managementprozesses, der sich um die Planung, Implementierung, Aufrechterhaltung, Überprüfung und Verbesserung der Informationssicherheit kümmert.

5. Management des ISMS

5.1. Zielsetzung und Bewertung

Anhand der Geschäftsziele hat sich die Organisation strategische Maßnahmen einzusteuern, um Kundengruppen im Automotiv-Bereich halten oder ggf. dieses Marktsegment aufbauen zu können.

Dazu ist es wichtig, ein TISAX-Label zu erhalten, welches der Organisation ein relevantes Maß an Informationssicherheit bestätigt. Wir wollen alles Erforderliche für dieses Label tun.

Daraus leiten sich weitere Informationssicherheitsziele ab, welche die Organisation verfolgt und alle Beschäftigten auffordert, an der Zielerreichung mitzuwirken. Die Ziele stehen im Einklang mit den Geschäftszielen, der Strategie und den Geschäftsplänen der Organisation.

- Verbesserung des Ansehens auf dem Markt sowie Verringerung der durch potenzielle Zwischenfälle verursachten Schäden.
- 100%iger Einhaltung von für Informationssicherheit relevanten Vorschriften/Gesetzen zur Erfüllung der Kunden-Compliance
- Nachverfolgen und Verringern der Anzahl der informationssicherheitsrelevanten Vorfälle
- Erhöhung der Nutzerzufriedenheit.

Schließlich ergeben sich aus diesen Informationssicherheitszielen weitere Ziele an ein Informationssicherheitsmanagementsystem (ISMS-Ziele), wie im Dokument 403 beschrieben.

Der Informationssicherheitsbeauftragte (ISB) ist für die Überprüfung der Informationssicherheitsziele und der ISMS-Ziele und für die Festlegung neuer Ziele verantwortlich.

Ziele für einzelne Sicherheitskontrollen oder Gruppen von Kontrollen werden vom DSB vorgeschlagen und vom Management in der Erklärung zur Anwendbarkeit genehmigt.

Alle Ziele werden mindestens einmal im Jahr überprüft werden.

BJ Automotive GmbH wird die Erreichung aller Ziele messen. Der ISB ist für die Festlegung der Methode zur Messung der Zielerreichung verantwortlich - die Messung wird mindestens einmal jährlich durchgeführt und ISB analysiert und bewertet die Messergebnisse und berichtet sie an die Geschäftsleitung als Input-Material für die Managementbewertung.

5.2. ISMS Anforderungen

Diese Leitlinie und das gesamte ISMS werden mit den für die Organisation relevanten gesetzlichen und behördlichen Anforderungen im Bereich Informationssicherheit, Datenvertraulichkeit, Geschäftskontinuität, Schutz personenbezogener Daten sowie mit den vertraglichen Verpflichtungen in Einklang stehen.

Eine detaillierte Auflistung aller gesetzlichen Anforderungen findet sich in Dokument 504 - Liste der relevanten Gesetze.

5.3. Informations-Sicherheitsmaßnahmen

Das Verfahren zur Auswahl der Maßnahmen (Sicherheitsvorkehrungen) ist in Dokument 602 – Risiko Assessment & Risiko Behandlungsmethodik festgelegt. Die ausgewählten Kontrollen und ihr Umsetzungsstatus sind im Dokument 601-Statement of Applicability aufgeführt.

5.4. Geschäftskontinuität

Das Management der Geschäftskontinuität ist in Dokument A 1701 – Business Continuity Management - Richtlinie festgelegt.

5.5. Verantwortlichkeiten

Die Zuständigkeiten für das ISMS sind in Dokument 502 ISMS-Rollen- und Verantwortlichkeiten festgelegt.

5.6. Kommunikation der Leitlinie

Der ISB muss sicherstellen, dass alle Mitarbeiter der BJ Automotive GmbH sowie die entsprechenden externen Parteien mit dieser Richtlinie vertraut sind.

6. Verbesserungen und Korrekturmaßnahmen

6.1. Abweichungen und Korrekturen

Eine Abweichung ist jeder Verstoß gegen die Anforderungen der Normen, der internen Dokumentation, der Vorschriften, der vertraglichen und sonstigen Verpflichtungen im Rahmen des ISMS. Abweichungen können, während eines internen oder externen Audits, aufgrund der Ergebnisse der Managementbewertung, nach Vorfällen, während des normalen Geschäftsbetriebs oder bei jeder anderen Gelegenheit festgestellt werden.

Ein Mitarbeiter, der eine Abweichung feststellt, muss sofort Maßnahmen ergreifen, um sie zu kontrollieren, einzudämmen, zu korrigieren und ihre Folgen zu bewältigen; ist ein Mitarbeiter nicht für eine solche Abweichung verantwortlich, muss er die Informationen über diese Abweichung an eine verantwortliche Person weiterleiten, die eine Korrektur vornehmen muss.

7. Maßregelungspozess

Der Maßregelungsprozess ist in Dokument A0701 – Richtlinie zur Personalsicherheit unter 5.2.3 beschrieben.

8. Korrekturmaßnahmen

8.1. Korrekturmaßnahmen

Die Unternehmensleitung muss beurteilen, ob die Ursache der Abweichung beseitigt werden muss. Außerdem muss die oberste Leitung durch die Veranlassung von Korrekturmaßnahmen ein erneutes Auftreten des Missstandes verhindern (Der Hauptunterschied besteht darin, dass Korrekturmaßnahmen die Ursache einer Abweichung beseitigen, während sich die Korrektur nur auf die Beherrschung der Abweichung und den Umgang mit den direkten Folgen konzentriert).

8.2. Umsetzung von Korrekturmaßnahmen

Die Korrekturmaßnahmen werden auf folgende Weise durchgeführt:

Korrekturreihenfolge	Verantwortlicher
1. Überprüfung der Abweichung	Jeder, der eine Rolle im ISMS spielt
2. Ermittlung der Ursache der Abweichung	Verantwortliche Person für den Bereich, in dem die Abweichung festgestellt wurde
3. Feststellung, ob eine ähnliche Abweichung bereits besteht oder bestand	Verantwortliche Person für den Bereich, in dem die Abweichung festgestellt wurde
4. Bewertung des Handlungsbedarfs zur Beseitigung der Abweichung	Verantwortliche Person für den Bereich, in dem die Abweichung festgestellt wurde
5. Bestimmung der Maßnahmen, die zur Beseitigung der Ursachen der Abweichungen erforderlich sind, um sicherzustellen, dass die Abweichungen nicht wieder auftreten	Verantwortliche Person für den Bereich, in dem die Abweichung festgestellt wurde
6. Durchführung der geplanten Maßnahmen	Mit der Durchführung beauftragte Person, die von der verantwortlichen Person ernannt wird
7. Überprüfung, ob die ergriffenen Maßnahmen zur Beseitigung der Ursachen der Abweichungen geführt haben	Person, die für den Bereich verantwortlich ist, in dem die Abweichung festgestellt wurde; oder interner Auditor, falls ernannt
8. Unterrichtung aller betroffenen Personen über die Durchführung von Korrekturmaßnahmen	Mit der Durchführung beauftragte Person, die von der verantwortlichen Person ernannt wird
9. Änderungen am ISMS vornehmen, falls erforderlich	Verantwortliche Person für das ISMS

9. Unterstützung bei der Umsetzung des ISMS

Hiermit erklärt die Geschäftsleitung der BJ Automotive GmbH, dass die Umsetzung des ISMS und die kontinuierliche Verbesserung mit angemessenen Ressourcen unterstützt werden, um alle in dieser Strategie festgelegten Ziele zu erreichen und alle ermittelten Anforderungen zu erfüllen.

10. Gültigkeit und Dokumentenverwaltung

Dieses Dokument ist ab dem Datum 05.05.2023 gültig.

Der Eigentümer dieses Dokuments ist der Informationssicherheitsbeauftragte, der das Dokument mindestens einmal jährlich überprüfen und gegebenenfalls aktualisieren muss.