Leitlinie zur Informationssicherheit

Jendamark GmbH & Co. KG

Graf Zeppelin Str. 4

86929 Penzing

Inhalt

In diesem Dokument wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist und Personenbezeichnungen gelten gleichwohl für alle Geschlechter.

1 Einleitung

1.1 Motivation

Hiermit wird folgende Leitlinie zur Informationssicherheit, durch die Geschäftsführung der Jendamark GmbH & Co. KG (nachfolgend Organisation genannt), als Bestandteil der Unternehmensstrategie verabschiedet

Aufgrund der permanenten Weiterentwicklung in der Informationstechnologie unterliegt diese Informationssicherheitsleitlinie und alle darauf aufbauenden Richtlinien und Konzepte der fortlaufenden Anpassung und Weiterentwicklung.

Die Informationssicherheitsleitlinie ist für alle Beschäftigten der Jendamark GmbH & Co. KG im Intranet einsehbar und ist im Internet veröffentlicht.

1.2 Geltungsbereich

Diese Leitlinie zur Informationssicherheit ist im gesamten Tätigkeitsbereich der Organisation gültig und verbindlich. Das umfasst insbesondere den Standort Penzing und alle zukünftigen Standorte, vollkonsolidierte Unternehmen als auch Joint-Ventures und Minderheitsbeteiligungen.

Werden Dritte mit der Erbringung von Leistungen beauftragt, ist durch vertragliche Vereinbarungen sicher zu stellen, dass die Leitlinie zur Informationssicherheit in den Leistungsbeziehungen berücksichtigt wird.

Darüber hinaus können weitere Richtlinien und Regelungen gelten, die den Anwendungsbereich betreffen.

1.3 Ansprechpartner

Ansprechpartner zu allen Fragen dieser Leitlinie ist der ISB. Der ISB berät und informiert die Organisation, insbesondere die oberen Leitungsebenen, in Fragen der Informationssicherheit. Er berichtet der Geschäftsführung regelmäßig über Lage und Entwicklung der Informationssicherheit in der Organisation, über die Entwicklung der Bedrohungslage und über kritische Abweichungen und Störungen der Informationssicherheit.

1.4 Verantwortlichkeiten

Die Geschäftsführung definiert, die in dieser Leitlinie dokumentierten, organisationsweiten Sicherheitsziele sowie die Sicherheitsstrategie und überwacht deren Umsetzung.

In Zusammenarbeit mit dem ISB werden die Schwerpunkte der Informationssicherheit in Übereinstimmung mit Geschäftsentwicklung und Geschäftsstrategie definiert und verbindlich vorgegeben. Der ISB implementiert ein ISMS, welches die Einhaltung der Sicherheitsanforderungen garantiert.

2 Unternehmens- und Sicherheitsziele

2.1 Grundsätze der Informationssicherheit

Verspätete oder fehlerhafte Entscheidungen des Managements können weitreichende Folgen nach sich ziehen. Daher ist für das Management bei wichtigen Entscheidungen ein Zugriff auf einen aktuellen Stand an Informationen wichtig. Für diese Informationen ist ein hohes Schutzniveau, in

Bezug auf Verfügbarkeit und Integrität, sichergestellt.
Die historisch bedingte Trennung der Steuerung von IT-Netzen und Bürokommunikation wird durch den Einsatz heutiger Informations- und Kommunikationstechnik zunehmend aufgeweicht. Hieraus ergibt sich die Wichtigkeit einer engen Abstimmung bzgl. der Ziele, Herausforderungen, Bedrohungen und Maßnahmen.
Für die Jendamark GmbH & Co. KG ist die Aufrechterhaltung der Kommunikation nach außen, zu unseren Kunden und Geschäftspartnern, von elementarer Bedeutung. Es darf zu keiner Verzögerung oder Gefährdung der Abwicklung von Aufträgen kommen. Wenn vertraglich festgelegte Leistung nicht erbracht oder gar Liefertermine nicht eingehalten werden können, kann dies erhebliche negative Folgen haben. Für uns ist daher die ständige Verfügbarkeit unserer Informations- und Kommunikationstechnik sowie die durchgängige Gewährleistung des Zugriffs auf korrekte Daten für unsere Beschäftigten von höchster Bedeutung, woraus wir einen hohen Schutzbedarf für diese Unternehmenswerte ableiten.
Durch die Jendamark GmbH & Co. KG werden innerhalb einiger Prozesse und Bereiche Informationen verarbeitet, welche sehr hohe Anforderungen an die Vertraulichkeit stellen.
Durch entsprechende technische und organisatorische Maßnahmen, sowie die hohe Aufmerksamkeit der Mitarbeiter wird die Vertraulichkeit gewährleistet und der Datenmanipulation vorgebeugt.
Die Nutzung von Internet und E-Mail zur Beschaffung von Informationen und zur Kommunikation ist für uns selbstverständlich. Durch entsprechende Maßnahmen wird sichergestellt, dass mit der Nutzung dieser Technologien verbundene Risiken möglichst gering bleiben.
Bei der Verarbeitung personenbezogener Daten unserer Kunden und Beschäftigten legen wir größten Wert auf die Einhaltung gesetzlicher Vorschriften und Regelungen. Die mit der Verarbeitung beauftragten Beschäftigten gehen vertraulich mit diesen Daten um.
In der Jendamark GmbH & Co. KG finden Maßnahmen zur Sensibilisierung im Bereich der Informationssicherheit Anwendung.

2.2 Ziele der Informationssicherheit

Nachfolgende Grundsätze bilden die Basis dieser Leitlinie, an denen sich alle Sicherheitsmaßnahmen und -vorgaben ausrichten und die für alle im Geltungsbereich tätigen Personen verbindlich ist.

1. Für Unternehmenswerte wie Informationen und IT-Systeme sind Eigentümer benannt, welche für die Sicherung der jeweiligen Unternehmenswerte (Assets) verantwortlich sind.
2. Mögliche Risiken, welche sich aus der Nutzung der Informationen und Informationssysteme ergeben, sind identifiziert und auf ein akzeptierbares Restrisiko minimiert.
3. Kosten für Maßnahmen zur Informationssicherheit stehen in einem angemessenen Verhältnis zur Größe und Wirtschaftlichkeit des Unternehmens.
4. Vorgaben und Maßnahmen orientieren sich an anerkannten Standards und Best Practices zur Informationssicherheit.
5. Gesetzliche, vertragliche und sonstige Vorgaben für die Informationssicherheit sind identifiziert und durch angemessene Maßnahmen umgesetzt.

6. Zugang/Zutritt und Zugriff zu den Informationswerten des Unternehmens sind auf das notwendige Maß beschränkt.
7. Alle wesentlichen Aktivitäten im Bereich der Informationssicherheit sind transparent und in erforderlichem Umfang nachvollziehbar.
8. Für die Wiederherstellung des Betriebes der wesentlichen Informationssysteme ist ein Notfallkonzept erstellt.
9. Für Beschäftigte, welche mit der Verarbeitung von Informationen betraut sind, sind angemessene Vorkehrungen zur Gewährleistung der Vertrauenswürdigkeit getroffen.
10. Die Beschäftigten werden hinsichtlich des sicheren Umgangs mit Informationswerten geschult und sensibilisiert und sind angehalten, die entsprechenden Vorgaben umzusetzen.

3 Anforderungen an die Informationssicherheit

Zur Erreichung der oben festgelegten Unternehmens- und Sicherheitsziele führt die Organisation ein einheitliches Informationssicherheitsmanagementsystem (ISMS) ein. Dieses besteht aus den zur Umsetzung der Sicherheitsziele festgelegten Richtlinien, Verfahren, Standards, Best Practices und Informationsmaterialien.

Bei Planung, Aufbau und Pflege des ISMS orientiert sich die Organisation an anerkannten Standards, insbesondere an der internationalen Normenreihe ISO/IEC 27001. Sie berücksichtigt außerdem die organisationsweit geltenden gesetzlichen und behördlichen Vorgaben.

Das ISMS unterliegt regelmäßiger Fortschreibung seiner Inhalte zur Anpassung an den fortschreitenden Stand der Technik, an veränderte Vorgaben und Strategien und an die sich verändernde Geschäftslandschaft.

Bestandteil des ISMS ist zudem die kontinuierliche Überprüfung der Umsetzung der Informationssicherheit im Unternehmen, mit dem Ziel erkannte Abweichungen und Schwächen zu beseitigen und das Gesamtschutzniveau der Organisation sicherzustellen.

3.1 Einhaltung von Gesetzen oder Vorschriften

Die regelmäßige Ermittlung von gesetzlichen, regulatorischen und vertraglichen Bestimmungen mit Relevanz zur Informationssicherheit ist ein wichtiger Schritt, um sicherzustellen, dass die erforderlichen Maßnahmen ergriffen werden, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten.

Spezielle Gesetze und Anforderungen sind im Rechtskataster geregelt.

Besonders hervorzuhebende sind folgende:

- Datenschutzgesetze, wie DSGVO, BDSG, TMG, TTDSG
- Branchenspezifische Vorschriften, wie z.B. TISAX®, Lieferantenkettensorgfaltsgesetz
- Normen und Standards: VDA-ISA Katalog
- Verträge und Vereinbarungen mit Kunden, Lieferanten oder Partnern, die spezifische Anforderungen an die Informationssicherheit enthalten. Diese Verträge umfassen beispielsweise Vertraulichkeitsvereinbarungen inklusive Geheimhaltungsvorschriften in Geschäftsbeziehungen mit Kunden und externen Stellen.
- Geschäftsgeheimnisgesetz: Im Rahmen von Geheimhaltungsvereinbarungen und entsprechenden Klauseln in den Verträgen schützt es vor unerlaubter Erlangung, Nutzung und Offenlegung von Geschäftsgeheimnissen.

- Vertraglich vereinbarte Bestimmungen, wie Allgemeine Einkaufsbedingungen, Rahmenverträge
- Stakeholder Anforderungen, z. B: Gesetzgeber, OEMs, Lieferanten, Kunden, Versicherungen stellen Anforderungen z.B. im Rahmen des Datenschutzes zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten oder zur Durchführung von Datenschutz-Folgenabschätzungen

Die regelmäßige Ermittlung, mindestens jährlich der gesetzlichen Bestimmungen ist wichtig, da sich Gesetze und Vorschriften ändern können und neue Anforderungen entstehen können. Durch die regelmäßige Überprüfung und Aktualisierung der relevanten Bestimmungen wird sichergestellt, dass die erforderlichen Maßnahmen ergriffen werden, um die Informationssicherheit zu gewährleisten und rechtliche oder vertragliche Verpflichtungen zu erfüllen.

3.2 Mitarbeiter-Bewusstsein für Informationssicherheit

Um Informationssicherheit gewährleisten zu können, sind angemessene technische und organisatorische Maßnahmen erforderlich. Diese können nur dann hinreichend wirksam sein, wenn alle Mitarbeiter die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln. Regelmäßige Fortbildungen zur Informationssicherheit unterstützen die Effektivität des Informationssicherheitsmanagements. Die Schulungen und Informationen erfolgen digital über eLearnings oder klassisch in Vor-Ort Schulungen. Die regelnden und informierenden Dokumente werden digital vollständig oder in adäquat zusammengefasster Form im Intranet zur Verfügung gestellt.

3.3 Kontinuierliche Verbesserung

Die Leitlinie zur Informationssicherheit und alle weiteren Richtlinien werden regelmäßig, hinsichtlich Aktualität und Wirksamkeit, geprüft.

Werden Schwachstellen in der Informationssicherheit identifiziert, so werden neue geeignete Maßnahmen entwickelt, auf ihre Integrationsfähigkeit in die Geschäftsabläufe untersucht und nach erfolgter Verifizierung in die Prozesse integriert.

Die Geschäftsführung unterstützt die ständige Verbesserung des Sicherheitsniveaus.

Alle Beschäftigten sind angehalten, an der kontinuierlichen Verbesserung des Sicherheitsniveaus mitzuwirken und mögliche Schwachstellen oder Verbesserungen, z.B. durch Hinweise oder Verbesserungsvorschläge, an die entsprechenden Stellen weiterzuleiten.

3.4 Aktualisierung und Information

Diese Leitlinie ist mindestens jährlich auf Aktualität zu überprüfen. Die Überprüfung ist in Form einer neuen Revision zu belegen. Die Änderungen werden von der Geschäftsführung freigegeben. Der Datenschutz wird stetig mitberücksichtigt. Unterjährige Vorfälle zur Informationssicherheit, welche eine Anpassung des ISMS erforderlich machen, sind unmittelbar mit dem ISB abzustimmen.

Jährlich wird ein Management-Report zur Wirksamkeit des ISMS erstellt und entsprechende Handlungsempfehlungen daraus abgeleitet.

4 Konsequenzen bei Nichtbeachtung des ISMS

Vorsätzliche oder grob fahrlässige Handlungen, die die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Mitarbeiter, Geschäftspartner und Kunden schädigen oder den Ruf des Unternehmens gefährden. Die Folgen von Zuwiderhandlungen erstrecken sich auf alle Bereiche des Informationssicherheitsmanagements. Bewusste Verstöße gegen verpflichtende Sicherheitsregeln

können arbeitsrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.

5 Rahmenwerk des ISMS

Das Rahmenwerk eines Informationssicherheitsmanagementsystems (ISMS) gemäß TISAX® bildet einen entscheidenden Leitfaden für Unternehmen, die in der Automobilindustrie tätig sind. TISAX® definiert einen standardisierten Ansatz zur Bewertung und Zertifizierung der Informationssicherheit.

ID	Aufbau des ISMS	
1	Richtlinien und Organisation des IS	
2	Human Resources	
3	Physical Security and Business Continuity	
4	Identity and Access Management	
5	IT Security / Cyber Security	
6	Supplier Relationships	
7	Compliance	

6 Regelmäßige Überprüfung dieser Leitlinie

Diese Leitlinie wird mindestens einmal im Jahr auf Aktualität überprüft.

7 Bereitstellung dieser Leitlinie

Diese Leitlinie ist öffentlich und wird im Internet zur Verfügung gestellt.

Penzing, 12.02.2026

Rudi Weber
Geschäftsführer