Leitlinie zur Informationssicherheit

CWS Workwear Deutschland GmbH & Co.KG

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

Die CWS Workwear Deutschland GmbH & Co.KG (im Folgenden die „Organisation“ genannt) vertreiben als Grundlage ihrer Geschäftsziele europaweit Dienstleistungen und Produkte.

Dabei spielt die Sicherheit der Informationen zu Kunden-, Lieferanten-, Mitarbeitenden- und Geschäftsdaten sowie der datenspeichernden und verarbeitenden Anwendungen und Systeme eine wichtige Rolle. Wir nutzen Informationssysteme in nahezu allen Kern- und unterstützenden Prozessen im Zuge der Automation, Digitalisierung und der Verarbeitung von Daten. Die Vertraulichkeit, die Integrität sowie die Verfügbarkeit und Belastbarkeit dieser Daten und Systeme sind zum Erreichen der Geschäftsziele unumgänglich. Dies muss mittels angemessener Informationssicherheitsmaßnahmen sichergestellt werden.

Unsere Daten und Systeme sind vielfältigen Gefährdungen von internen und externen Quellen durch Vorsatz, Fahrlässigkeit, Unfälle oder Katastrophen ausgesetzt. Diesen Gefährdungen ist durch geeignete Maßnahmen und Kontrollen zu begegnen. Die Informationssicherheitsmaßnahmen der Organisation sind die Voraussetzung dafür, dass unsere Kunden auch in Zukunft vertrauensvoll eine wachsende Anzahl von Diensten, Services und Produkten in Anspruch nehmen. Sie bilden damit auch eine wichtige Grundlage für die nachhaltige Geschäftsentwicklung der CWS Workwear Deutschland GmbH & Co.KG.

Diese Leitlinie zur Informationssicherheit legt die Grundsätze zur Informationssicherheit fest, die in der Organisation gelten. Sie bildet die Grundlage für die abgeleiteten Sicherheitsrichtlinien und -konzepte, die als Umsetzung bzw. Präzisierung formuliert werden.

Die Leitlinie und die darauf aufbauenden Richtlinien bilden zusammen das Regelwerk für die Informationssicherheit der Organisation.

1.2 Geltungsbereich

Diese Leitlinie zur Informationssicherheit ist im gesamten Tätigkeitsbereich der Organisation gültig und verbindlich. Das umfasst insbesondere alle 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 Chief Information Security Officer (CISO). Der CISO berät und informiert die Organisation, insbesondere die oberen Leitungsebenen, in Fragen der Informationssicherheit. Er berichtet dem Lenkungsausschuss Informationssicherheit 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

Der Lenkungsausschuss für Informationssicherheit definiert, die in dieser Leitlinie dokumentierten organisationsweiten Sicherheitsziele und die Sicherheitsstrategie und überwacht deren Umsetzung. Teilnehmer sind die Mitglieder des Executive Leadership Teams der CWS-Gruppe sowie der Chief Information Security Officer. Der Lenkungsausschuss tritt mindestens einmal jährlich zusammen. Er entscheidet über die Schwerpunkte der Informationssicherheit in Übereinstimmung mit Geschäftsentwicklung und Geschäftsstrategie der CWS-Gruppe und über besonders weitreichende Fragen von strategischer Bedeutung für das Gesamtunternehmen.

2 Unternehmens- und Sicherheitsziele

Die Gewährleistung der Informationssicherheit ist essenzielle Voraussetzung für die Aufrechterhaltung des Geschäftsbetriebs und muss daher angemessen in unserem täglichen Arbeitsleben berücksichtigt werden. Die Organisation verfolgt daher in Bezug auf Informationssicherheit die folgenden allgemeinen Ziele:

- Die Organisation schützt die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit ihrer Informationen, ihrer Geschäftsprozesse und ihrer Infrastruktur, indem sie risikoangemessene Sicherheitsmaßnahmen festlegt, umsetzt und kontinuierlich fortschreibt. Diese können sowohl organisatorischer als auch technischer Natur sein.
- Sie orientiert sich dabei an rechtlichen Vorgaben, allgemein anerkannten Standards, dem anerkannten Stand der Technik sowie der aktuellen Gefährdungslage.
- Die Einhaltung der festgelegten Sicherheitsmaßnahmen wird regelmäßig überprüft. Abweichungen werden ohne unnötige Verzögerungen abgestellt. Wesentliche Abweichungen sowie die zur Abstellung zu ergreifenden Maßnahmen werden den zuständigen Führungskräften und Leitungsgremien berichtet.
- Der Aufwand für die Planung, Umsetzung, Pflege und Kontrolle der Sicherheitsmaßnahmen hat dabei in wirtschaftlich sinnvollem Verhältnis zum erwarteten Nutzen bzw. zu Wahrscheinlichkeit und Höhe des abzuwendenden Schadens zu stehen.
- Alle Mitarbeiter in allen Bereichen und auf allen Hierarchieebenen tragen bei ihrer gesamten Tätigkeit Verantwortung für die Informationssicherheit der Organisation und haben die Aufgabe, ihre Tätigkeit im Bewusstsein dieser Verantwortung zu gestalten.

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, sowie die Vorgaben der Franz Haniel & Cie. GmbH in Bezug auf Informationssicherheit und die organisationsweite Geschäfts- und IT-Strategie.

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.

Der Lenkungsausschuss 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 CISO 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.

Dreieich, 30.04.2024

Carsten Best, Regional Managing Director D/A/CH Healthcare & Workwear

Vor- Nachname

Position