P U E H L

PÜHL GMBH & CO KG

501-Informationssicherheits-Leitlinie

Version dieses Dokuments:	1.1
Datum der letzten Änderung:	11.12.2023
Autor:	Anselm Hugle
Vertraulichkeitsstufe:	intern

Änderungshistorie:

Datum	Version	Erstellt durch	Beschreibung der Änderung
01.01.2022	0.1	DataGuard	Grundstruktur des Dokuments
11.10.2023	1.0	Anselm Hugle	Anpassung an Anforderungen Fa. Pühl
11.12.2023	1.1	Anselm Hugle	Verweise auf Verzeichnisse, Ziele

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 PÜHL GMBH & CO KG sowie relevante externe Parteien.

2. Referenzdokumente

- ISO/IEC 27001-Norm, Abschnitte 5.2 und 5.3

3. Verweis auf ISMS-Richtlinien -und Verfahren

- G:\44_Informationssicherheit\ISMS Pühl_ISO27001_2013

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

Die allgemeinen, strategische Informationssicherheitsziele für das ISMS sind wie folgt:

1 Schutz vertraulicher Daten sowohl von PUEHL und seinen Mitarbeiter als auch von seinen Kunden und Lieferanten.
2 Verfügbarkeit sämtlicher PUEHL Produkte und Leistungen sowie der involvierten Daten.
3 Integrität sämtlicher PUEHL Produkte und Leistungen sowie der involvierten Daten.
4 Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte.
5 Einhaltung der aus gesetzlichen, vertraglichen und aufsichtsrechtlichen Verpflichtungen resultierenden Anforderungen.
6 Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb von PUEHL.
7 Etablierung und Erhaltung eines guten Rufs von PUEHL bzgl. Informationssicherheit im Kundenbewußtseins.
8 Reduzierung der im Schadensfall entstehenden Kosten für PUEHL.
9 Need-to-know-Prinzip: Der Zugriff auf sicherheitskritische Systeme, Applikationen und Informationen bei PUEHL ist auf einen minimalen Personenkreis einzuschränken. Prinzipiell ist verboten, was nicht explizit erlaubt ist.
10 Einführung und fortlaufender Erhalt des ISMS bei PUEHL in Anlehnung an den kontinuierlichen Verbesserungsgedanken im Sinne des PDCA-Modells (Plan-Do-Check-Act).

Die Ziele stehen im Einklang mit den Geschäftszielen, der Strategie und den Geschäftsplänen der Organisation. Der interne Informationssicherheits-Beauftragte ist für die Überprüfung dieser allgemeinen ISMS-Ziele und die Festlegung neuer Ziele verantwortlich.

Ziele für einzelne Sicherheitskontrollen oder Gruppen von Kontrollen werden von externen DSB & ISB vorgeschlagen und von der Pühl Geschäftsführung in der Erklärung zur Anwendbarkeit genehmigt.
(*DSB=Datenschutzbeauftragter; ISB=Informationssicherheitsbeauftragter*)

Alle Ziele müssen mindestens einmal im Jahr überprüft werden.

PÜHL GMBH & CO KG wird die Erreichung aller Ziele messen. Der interne Informationssicherheits-Beauftragte ist für die Festlegung der Methode zur Messung der Zielerreichung verantwortlich - die Messung wird mindestens einmal jährlich durchgeführt und der interne Informationssicherheits-Beauftragte analysiert und bewertet die Messergebnisse und berichtet sie an die Geschäftsführung als Input-Material für die Managementbewertung.

5.2. ISMS-Anforderungen

Diese Leitlinie und das gesamte ISMS müssen mit den für die Organisation relevanten gesetzlichen und behördlichen Anforderungen im Bereich der Informationssicherheit, des Datenschutzes und Pühl-internen Richtlinien und Regeln sowie mit den vertraglichen Verpflichtungen in Einklang stehen.

Eine detaillierte Auflistung aller vertraglichen und gesetzlichen Anforderungen findet sich in der Liste der gesetzlichen, regulatorischen und vertraglichen Verpflichtungen.

5.3. Informations-Sicherheitsmaßnahmen

Das Verfahren zur Auswahl der Maßnahmen (Sicherheitsvorkehrungen) ist in der Methodik zur Risikobewertung und Risikobehandlung festgelegt.

Die ausgewählten Kontrollen und ihr Umsetzungsstatus sind im „Statement of Applicability" aufgeführt.

5.4. Geschäftskontinuität

Das Management der Geschäftskontinuität ist in der Richtlinie zum Management der Geschäftskontinuität festgelegt.

5.5. Verantwortlichkeiten

Die Zuständigkeiten für das ISMS sind in der ISMS-Rollen- und Verantwortungsmatrix zu finden.

5.6. Kommunikation der Leitlinie

Der interne Informationssicherheits-Beauftragte muss sicherstellen, dass alle Mitarbeiter der Pühl GmbH & CO KG, Plettenberg 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.

6.2.Korrekturmaßnahmen

Die Unternehmensleitung muss beurteilen, ob die Ursache der Abweichung beseitigt werden muss. Außerdem muss die Geschäftsleitung durch Korrekturmaßnahmen ein erneutes Auftreten des Missstandes verhindern.

Anmerkung: *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.*

6.3.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

7. Unterstützung bei der Umsetzung des ISMS

Hiermit erklärt die Geschäftsführung der Firma Pühl, 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.

8. Gültigkeit und Dokumentenverwaltung

Dieses Dokument ist ab dem Datum 11.12.2023 gültig.

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

Pühl Geschäftsführung
Dr. Götz Kaltheuner

11.12.2023