[Name der Organisation & formaler Firmenbriefkopf]

Leitlinie zur Informationssicherheit

Zweck und Anwendungsbereich

Diese oberste Informationssicherheitsleitlinie definiert den Rahmen für die Verwaltung der Informationssicherheit innerhalb von [Name der Organisation], in Übereinstimmung mit der strategischen Ausrichtung der Organisation und in Übereinstimmung mit den Informationssicherheitsstandards nach [bitte fügen Sie Ihre anwendbare Norm wie ISO 27001:2022 oder ISA-TISAX 6.0 oder beides hinzu]. Zweck dieser Informationssicherheitspolitik ist es, einen umfassenden Rahmen für den Schutz der sensiblen Informationen, der Infrastruktur und des Rufs unserer Organisation zu definieren.

Diese Leitlinie gilt für das gesamte Informationssicherheits-Managementsystem (ISMS) und ist im ISMS-Anwendungsbereich-Dokument [bitte den Namen des Anwendungsbereich-Dokuments wie "ISMS-Handbuch" hinzufügen] definiert.

Anwendbarkeit

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, Drittdienstleister und Interessenvertreter, die Zugang zu den Informationswerten im Anwendungsbereich des ISMS haben oder an der Verwaltung und dem Schutz dieser Werte beteiligt sind. Sie umfasst alle Systeme, Netzwerke und Daten, die unter der Kontrolle des ISMS-Anwendungsbereichs stehen, unabhängig von deren Standort oder Form [Bitte passen Sie diese Aussage an Ihren Geltungsbereich an].

Grundsatzerklärung

[Name der Organisation] hat sich verpflichtet, seine Informationswerte vor allen Bedrohungen zu schützen, seien sie intern oder extern, absichtlich oder versehentlich. Unsere Informationssicherheitsleitlinie beruht auf den folgenden Grundsätzen:

- **Zweckausrichtung**: Die Leitlinie dient der Unterstützung des Geschäftszweck und der strategischen Ziele unserer Organisation.
- **Ziele für die Informationssicherheit**: Die Leitlinie bietet einen Rahmen für die Festlegung, Überprüfung und Erreichung von Informationssicherheitszielen, die mit den allgemeinen Geschäftszielen der Organisation in Einklang stehen.
    - Die allgemeinen Ziele des Informationssicherheitsmanagementsystems bestehen darin, die Vertraulichkeit, Integrität und Verfügbarkeit (VVI) von Informationswerten zu gewährleisten und so den Ruf, die rechtliche Konformität und die betriebliche Effizienz der Organisation zu schützen.
    - Die oberste Leitung der Organisation ist für die Überprüfung dieser allgemeinen ISMS-Ziele und für die Festlegung neuer Ziele verantwortlich.
    - Ziele für einzelne Sicherheitsmaßnahmen oder Gruppen von Sicherheitsmaßnahmen sind definiert ir [bitte Dokument hinzufügen, in dem ISMS-Ziele und -Maßnahmen definiert sind, z. B. "ISMS-Handbuch"]. Alle diese Zielvorgaben müssen mindestens einmal im Jahr überprüft werden.
    - Die Organisation evaluiert und misst die Erreichung dieser Ziele.
- **Informationssicherheitsmaßnahmen**: Das Verfahren für die Anwendung von Sicherheitsmaßnahmen ist in der Methodik für die Risikobewertung und Risikobehandlung festgelegt. Die ausgewählten Maßnahmen und ihr Umsetzungsstatus sind im [bitte auswählen: ISO27001: Erklärung zur Anwendbarkeit / TISAX: TISAX-ISA-Katalog] dokumentiert.
- **Einhaltung gesetzlicher und behördlicher Vorschriften**: Unsere Organisation hat sich verpflichtet, alle geltenden gesetzlichen, behördlichen und vertraglichen Anforderungen in Bezug auf die Informationssicherheit einzuhalten. Eine detaillierte Auflistung aller vertraglichen und gesetzlichen Anforderungen ist der Liste der gesetzlichen, behördlichen, vertraglichen und sonstigen Anforderungen beigefügt.
- **Konsequenzen bei Nichteinhaltung:**
  Alle Mitarbeitenden sind verpflichtet, diese Informationssicherheitsleitlinie sowie die dazugehörigen Richtlinien und Verfahren vollständig einzuhalten. Zuwiderhandlungen – ob vorsätzlich oder fahrlässig – werden untersucht und

können je nach Schweregrad disziplinarische Maßnahmen (z. B. Ermahnung, Abmahnung bis hin zur Kündigung) sowie ggf. weitere arbeits-, zivil- oder strafrechtliche Konsequenzen nach sich ziehen.

- **Kontinuierliche Verbesserung**: Wir sind bestrebt, unser ISMS ständig zu verbessern, um sicherzustellen, dass es angesichts der sich entwickelnden Bedrohungen und geschäftlichen Veränderungen wirksam bleibt.

Führung und Verpflichtung

Die oberste Leitung der Organisation verpflichtet sich, das Informationssicherheits-Managementsystem (ISMS) einzurichten, umzusetzen, aufrechtzuerhalten und kontinuierlich zu verbessern. Dieses Engagement zeigt sich durch:

- **Strategische Ausrichtung**: Sicherstellung, dass die Informationssicherheitspolitik und -ziele mit den allgemeinen strategischen Zielen der Organisation übereinstimmen.
- **Integration**: Einbettung der Anforderungen an die Informationssicherheit in alle organisatorischen Prozesse, um einen ganzheitlichen Ansatz für das Risikomanagement zu gewährleisten.
- **Zuweisung von Ressourcen**: Bereitstellung der notwendigen Ressourcen, einschließlich finanzieller, technischer und personeller Ressourcen, um das ISMS zu unterstützen und die angestrebten Ergebnisse zu erreichen.
- **Kommunikation**: Aktive Förderung der Bedeutung eines wirksamen Informationssicherheitsmanagements und Gewährleistung, dass alle Mitarbeiter die Anforderungen des ISMS verstehen und einhalten.
- **Überprüfung der Wirksamkeit**: Regelmäßige Überprüfung des ISMS, um sicherzustellen, dass es seine Ziele erreicht und zur allgemeinen Sicherheitslage der Organisation beiträgt.
- **Unterstützung und Führung**: Ermutigung und Schulung aller Mitarbeiter und relevanten Interessengruppen, zur Wirksamkeit des ISMS beizutragen und eine Kultur des Sicherheitsbewusstseins zu fördern.
- **Kontinuierliche Verbesserung**: Förderung von Initiativen zur kontinuierlichen Verbesserung der Informationssicherheitspraktiken des Unternehmens.
- **Führung in Rollen**: Befähigung anderer Managementfunktionen innerhalb der Organisation zur Führung und zum Engagement für die Informationssicherheit in ihrem jeweiligen Verantwortungsbereich. Rollen und Verantwortlichkeiten innerhalb des ISMS sind definiert in [bitte Dokument hinzufügen, in dem die ISMS-Rollen und Verantwortlichkeiten definiert sind, z. B. "ISMS-Handbuch"]
    - Um sicherzustellen, dass das ISMS die Anforderungen dieses Dokuments erfüllt, um den Betrieb des ISMS zu koordinieren und um regelmäßig über die Wirksamkeit des ISMS zu berichten, ernennt die oberste Leitung einen Informationssicherheitsbeauftragten (ISO).

Dokumentation und Kommunikation

Um sicherzustellen, dass diese Politik wirksam umgesetzt wird, wird unsere Organisation:

- **Dokumentation und Kommunikation**: Diese Leitlinie und weitere themenspezifischen Richtlinien werden als dokumentierte Information regelmäßig überprüft und aktualisiert, um etwaige Änderungen in der Organisation oder im externen Umfeld zu berücksichtigen.
- **Externe Verfügbarkeit**: Diese Leitlinie und weitere themenspezifischen Richtlinien werden an relevante interne Personengruppen und externe Parteien veröffentlicht.

Überprüfung und Verbesserung

Diese Informationssicherheitsleitlinie wird jährlich oder bei Bedarf überprüft, um ihre kontinuierliche Relevanz und Wirksamkeit zu gewährleisten. Rückmeldungen aus internen Audits, Risikobewertungen und Vorfällen werden genutzt, um Verbesserungen des ISMS und der allgemeinen Sicherheitslage der Organisation voranzutreiben.

Dieses Dokument in seiner Version [Bitte fügen Sie die aktuelle Versionsnummer ein]ist gültig ab [Datum]

[Signatur] _____

[Name], [Berufsbezeichnung]

Version	*1.0*

Besitzer der Police	Name *des Top-Managements eingeben*
Genehmigt durch	Ausschuss *zur Genehmigung der Politik*
Datum der Genehmigung	Datum *eingeben*
Datum des Inkrafttretens	Datum *eingeben*
Nächster Überprüfungstermin	Datum *eingeben*
Vertraulichkeitsstufe	INTERN

Versionsverlauf

Datum	Version	Erstellt von	Beschreibung der Änderung
08.09.25	0.92	DataGuard	Grundstruktur des Dokuments
XX.XX.24	1.00	XX	Genehmigte Version und minimale Änderungen