Informationssicherheitsleitlinie

1. Zweck, Anwendungsbereich und Anwender

Dieses Dokument definiert die Informationssicherheitsleitlinie der Organisation und somit das übergeordnete Ziel des Informationssicherheitsmanagementssystems (ISMS). In diesem Dokument wird der Zweck, die Ausrichtung, die Grundlagen sowie die allgemeinen Regelungen für das ISMS festgelegt.

Die in diesem Dokument festgelegte Informationssicherheitsleitlinie bezieht sich auf das gesamte ISMS gemäß dem definierten Anwendungsbereich.

Die in diesem Dokument verwendeten männlichen Formen knüpfen nicht an ein Geschlecht an, sondern sind vereinfachend verwendet und genderneutral zu verstehen.

Anwender des Dokuments sind alle Mitarbeitenden der Organisation und alle interessierten Parteien.

2. Begriffe der Informationssicherheit

Begriff	**Bedeutung**
Vertraulichkeit	die Eigenschaft, dass Informationen nicht unbefugten Personen, Einrichtungen oder Prozessen zugänglich gemacht oder offengelegt werden
Integrität	die Eigenschaft der Richtigkeit und Vollständigkeit der Informationen
Verfügbarkeit	die Eigenschaft, dass Informationen bei Bedarf von einer autorisierten Stelle zugänglich und nutzbar sind
Informationssicherheit	Erhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen
Informationssicherheitsmanagementsystem (ISMS)	Managementprozess, der sich mit Planung, Implementierung, Instandhaltung, Überprüfung und Verbesserung der Informationssicherheit befasst

3. Stellenwert der Informationssicherheit

3.1. Geschäftsziele

Geschäftsziel ist der weltweite Verkauf von selbst entwickelten solarbetriebenen Pumpen und deren Zubehör.

- Produkte entwerfen, die unsere Hauptkriterien – effizient, robust und langlebig – erfüllen und gleichzeitig für ein möglichst breites Publikum zugänglich sind
- Unser Partnernetzwerk unterstützen, um die Geschäftsabwicklung zu vereinfachen und sicherzustellen, dass Endkunden gut bedient werden

3.2. Relevante Anforderungen und interessierte Parteien

Alle relevanten rechtlichen, amtlichen, vertraglichen und sonstigen Anforderungen sind in der "Relevante Anforderungen Interessierte Parteien" dokumentiert und werden regelmäßig überprüft.

Insbesondere ist für uns wichtig, dass wir folgende Anforderungen erfüllen:

Kundenanforderungen

Die Erfordernisse und Erwartungen folgender interessierter Parteien möchten wir primär mit dem ISMS erfüllen:

- Kunden
- Gesetzgeber
- Geschäftsführung

3.3. Informationssicherheit

Das Thema Informationssicherheit hat entsprechend unserer Geschäftsziele einen hohen Stellenwert. Die Ziele für das ISMS leiten sich aus der gemäß „Informationssicherheitsleitlinie | 3.1 Geschäftsziele“ beschriebenen Geschäftsstrategie der Organisation sowie gemäß „Informationssicherheitsleitlinie | 3.2 Relevante Anforderungen und interessierte Parteien“ beschriebenen relevanten Anforderungen und interessierten Parteien ab.

3.4. ISMS Ziele

Das Ziel des Informationssicherheitsmanagementsystems ist insbesondere die Erfüllung aller Anforderungen der ISO/IEC 27001, insbesondere einer erfolgreichen (Re)-Zertifizierung. Das Gesamtrisiko der Organisation im Sinne der Informationssicherheit soll maximal "Mittel" sein.

Die Ziele des ISMS werden dokumentiert und deren Erfüllung gemäß „Informationssicherheitsleitlinie | 3.5. Planung und Überprüfung der Ziele der ISMS uns ihrer Erfüllung“ überprüft.

3.5. Planung und Überprüfung der Ziele der ISMS und ihrer Erfüllung

Bei der Planung, wie die Ziele des ISMS erreicht werden sollen, müssen die geplanten Maßnahmen, die Ressourcen, Verantwortlichkeiten, zeitlichen Ziele sowie die Bewertungsmethode für die Überprüfung festgelegt werden. Die Punkte sind zu dokumentieren. Die Ziele des ISMS und deren Erfüllung sind jährlich zu überprüfen. Verantwortlich für die Durchführung der Überprüfung, die Analyse der Ergebnisse der Überprüfung und die Erstellung eines Prüfberichts für das Management ist der Informationssicherheitsbeauftragte.

3.6. Informationssicherheitsmaßnahmen

Die Organisation verpflichtet sich, die geltenden Anforderungen an die Informationssicherheit zu erfüllen, wie sie in den themenspezifischen Informationssicherheitsrichtlinien des

ISMS und ISO/IEC 27001 definiert sind. Geeignete Informationssicherheitsmaßnahmen (sogenannte Controls) werden innerhalb des Risikomanagementrahmens in der Methodik zur Risikobewertung und Risikobehandlung identifiziert, definiert und überprüft.

Die anwendbaren Informationssicherheitsmaßnahmen, ihr Umsetzungsstatus und etwaige Ausnahmen werden in der Erklärung zur Anwendbarkeit (sogenannte Statement of Applicability (SOA)) dokumentiert. Verantwortlich für die SOA ist der Informationssicherheitsbeauftragte. Die SOA ist gemäß dem Kapitel "Informationssicherheitsleitlinie | 8. Verwaltung von Aufzeichnungen zu diesem Dokument" abzulegen.

4. Verantwortlichkeiten

Im Rahmen des ISMS gibt es folgende Verantwortlichkeiten:

Stellenbezeichnung	**Verantwortlich für**
Geschäftsführung	die korrekte Umsetzung und Instandhaltung des ISMS gemäß der Informationssicherheitsleitlinie sowie die Sicherstellung, dass ausreichend Ressourcen dafür verfügbar sind.
Informationssicherheitsbeauftragter	die Koordination des Betriebs des ISMS und die Berichterstattung über dessen Leistungsfähigkeit.
Informationssicherheitsbeauftragter	die Sicherstellung, dass jährliche Überprüfungen des ISMS bzw. bei entscheidenden Änderungen durchgeführt und protokolliert werden.
Informationssicherheitsbeauftragter	das Informationssicherheitsbewusstsein aller Mitarbeiter sowie deren Ausbildung und Schulung zum Thema Informationssicherheit.
Asset-Owner	die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit der Assets bzw. Informationen, für die die Person zuständig ist.
Alle Mitarbeiter	die Meldung von Informationssicherheitsvorfällen oder Schwachstellen.
Informationssicherheitsbeauftragter	die Behandlung von Informationssicherheitsvorfällen und Schwachstellen.
Geschäftsführung	die Definition der Informationen, die im Rahmen der Informationssicherheit an interessierte Parteien kommuniziert werden.

Alle wesentlichen Verantwortlichkeiten und wiederkehrenden Aufgaben im ISMS werden über den Task Manager im Digital Compliance Office (DCO) oder auf Confluence über den Bereich ISO 27001 ISMS gesteuert und dokumentiert.

5. Policy

Die Informationssicherheit ist auf der obersten Führungsebene der Organisation verankert. Die Geschäftsleitung der Organisation hat sich dem ISMS gemäß den Anforderungen von ISO/IEC 27001 und den Anforderungen des Risikomanagements verpflichtet, um das System an die sich ständig ändernden Geschäftsbedingungen anzupassen und sicherzustellen, dass die erforderlichen Ressourcen bereitgestellt werden. Dies soll alle relevanten Beteiligten des ISMS in die Lage versetzen, die Ziele der Informationssicherheit zu erreichen und das ISMS kontinuierlich zu verbessern. Das Management ist auch für die Umsetzung der Unternehmenspolitik verantwortlich.

6. Verpflichtungen und Zuständigkeiten im Bereich der Informationssicherheit

Alle Mitarbeitende und relevante Dritte müssen mit der Informationssicherheitsleitlinie der Organisation und dem ISMS vertraut sein. Alle Mitarbeitende müssen in Übereinstimmung mit der Informationssicherheitsleitlinie, den themenspezifischen Informationssicherheitsrichtlinien und allen von der Geschäftsführung festgelegten Vorgaben handeln. Sofern gegen Unternehmensrichtlinien verstoßen wird, können disziplinarische Maßnahmen eingeleitet werden. Die Geschäftsführung ist dafür verantwortlich, die Informationssicherheitsleitlinie zu kommunizieren und die Bedeutung des ISMS und der unternehmensweiten Verpflichtung zur Informationssicherheit zu verdeutlichen.

7. Referenzdokumente

Die folgenden Dokumente werden referenziert:

- Anwendungsbereich des Informationssicherheitsmanagementsystems
- Verfahren zur Identifikation von relevanten Erfordernissen
- Verfahren zu Informationssicherheitszielen & KPIs
- Verfahren zu Korrekturmaßnahmen und kontinuierlichen Verbesserungen

8. Verwaltung von Aufzeichnungen zu diesem Dokument

Folgende Aufzeichnungen werden zu diesem Dokument geführt:

- Übersicht - ISMS Ziele KPIs
- Berichte – ISMS – KPI - Zielreichungen
- Übersicht rechtlicher, amtlicher, vertraglicher und anderer Erfordernisse
- Statement of Applicability (SoA) - Maßnahmenbehandlung

Die Aufzeichnungen sind gemäß dem Verfahren zur Lenkung von Dokumenten und Aufzeichnungen aufzubewahren.

9. Gültigkeit und Dokumentenhandhabung

Dieses Dokument ist gültig ab 22 Jan 2026 .

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

Für die Auswertung des Dokuments auf Wirksamkeit und Angemessenheit sowie möglichen Anpassungsbedarf müssen mindestens folgende Kriterien berücksichtigt werden:

- Ergebnisse von internen und externen Audits
- Ergebnisse der KPI-Auswertung
- Ergebnisse der Managementreviews
- Anpassungen, die sich aus dem Risikomanagement oder Korrekturmaßnahmen ergeben