

Information Security Policy One-Pager

SATECO AG
Sonnenbergstrasse 72
8603 Schwerzenbach

Dokumentenhistorie

Datum	Name	Neu	Ver.
07.04.2026	Tim Becker	Anpassungen des Drafts für die SATECO AG	0.1
22.06.2026	Kevin Struwe	Finalisierung	1.0
10.07.2026	Dr. Daniel Häfliger	Freigabe	1.0

Inhaltsverzeichnis

Dokumentenhistorie	2
1. Zweck und Zielsetzung	4
2. Geltungsbereich	4
3. Definition	4
4. Sicherheitsziele	4
5. Grundsätze	5
6. Verantwortung der Geschäftsführung	5
7. Überprüfung und Freigabe.....	5
Anhang A Handlungsübersicht für Mitarbeiter.....	6

1. Zweck und Zielsetzung

Die Sateco AG verarbeitet sensible Informationen, eigene sowie solche unserer Kunden, Partner und Lieferanten, insbesondere im Kontext der Automobilindustrie (OEM-Assets). Ziel dieser Information Security Policy ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen.

Die Policy bildet die Grundlage für unser Information Security Management System (ISMS) gemäß TISAX (Scope ID SW45T8, Assessment Level 2) und orientiert sich an ISO/IEC 27001.

2. Geltungsbereich

Die Policy gilt für die gesamte SATECO AG am Standort Schwerzenbach, TISAX Scope ID S67H1C – AL2 (Information High) mit allen Inhalten und Dokumenten, und umfasst:

- alle Mitarbeitenden, Führungskräfte, freien Mitarbeiter, Lieferanten, Dienstleister und Geschäftspartner mit Zugang zu Informationen oder Systemen der Sateco AG,
- alle Arten von Informationen, unabhängig von Medium und Form (digital, physisch, mündlich).

3. Definition

Informationssicherheit bedeutet den Schutz von Informationen vor unbefugtem Zugriff, Missbrauch, Offenlegung, Zerstörung, Veränderung oder Störung. Die zentralen Schutzziele sind:

- Vertraulichkeit (C): Schutz vor unbefugter Preisgabe.
- Integrität (I): Vollständigkeit und Unverändertheit der Daten.
- Verfügbarkeit (A): Zugriff auf Informationen und Systeme zum benötigten Zeitpunkt.

4. Sicherheitsziele

Die Sicherheitsziele der Sateco AG sind:

- Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit der Unternehmens- und Kundendaten.
- Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderungen.
- Identifikation und Bewertung von Informationssicherheitsrisiken sowie Begrenzung auf ein akzeptables Maß.
- Schutz der OEM-Assets und Wahrung von Geschäftsgeheimnissen unserer Kunden und Partner.
- Vermeidung von Reputations- und finanziellen Schäden.
- Transparenz in allen relevanten Geschäfts- und Serviceprozessen.

5. Grundsätze

- Schutz von Kunden- und Unternehmensdaten durch wirksame technische und organisatorische Maßnahmen.
- Regelmäßige Schulung und Sensibilisierung aller Mitarbeitenden zu Informationssicherheit und Datenschutz.
- Klassifizierung von Informationen entsprechend ihrem Schutzbedarf.
- Etabliertes Risikomanagement mit Fokus auf kontinuierlicher Verbesserung.
- Berücksichtigung von Informationssicherheit und Datenschutz in allen Change-Management-Prozessen.
- Berechtigungskonzept nach dem Prinzip der minimalen Rechtevergabe (Need-to-know).
- Regelmäßige interne Audits zur Überprüfung der Wirksamkeit und Identifikation von Verbesserungspotenzial.

6. Verantwortung der Geschäftsführung

Die Geschäftsführung der Sateco AG betrachtet Informationssicherheit als unverzichtbares Qualitätsmerkmal. Sie stellt die erforderlichen Ressourcen bereit (Personal, Budget, Technologie), benennt verantwortliche Personen (insbesondere den Informationssicherheitsbeauftragten), unterstützt die notwendigen Strukturen und Prozesse, überprüft regelmäßig die Wirksamkeit des ISMS und verpflichtet sich zur kontinuierlichen Verbesserung.

Alle Mitarbeitenden, Lieferanten und Geschäftspartner sind verpflichtet, diese Policy einzuhalten, Risiken und Vorfälle zu melden und aktiv zum Schutz von Informationen beizutragen.

Sicherheitsvorfälle sind unverzüglich zu melden an: **incidents@satecogroup.com**

7. Überprüfung und Freigabe

Diese Information Security Policy wird mindestens einmal jährlich sowie bei wesentlichen Änderungen überprüft und durch die Geschäftsführung freigegeben.

Anhang A Handlungsübersicht für Mitarbeiter

Thema	Anweisung
Passwörter	- Verwenden Sie in der Firma andere Passwörter als privat - Nutzen Sie keine Trivialpasswörter
Fremdsoftware	- Installieren Sie keine Fremdsoftware, sprechen Sie mit der IT vor der Installation
Arbeitsplatz	- Sperren Sie Ihren PC bei Verlassen des Platzes mit Windows-L - Lassen Sie keine Informationen auf ihrem Arbeitsplatz liegen
Online Services im Internet	- Nutzen Sie nur Services im Internet, bei denen Sie keine Dokumente oder Daten hochladen müssen - Fragen Sie ihren ITSB vor der Nutzung von Online-Services, ob diese freigegeben wurden bzw. welche freigegeben sind
Nutzung von Mobiles	- Aktivieren Sie den Zugangsschutz mit Passwort oder Fingerprint - Melden Sie einen Verlust umgehend an den Informationssicherheitsbeauftragten
Nutzung eigener Geräte	- Prüfen Sie gemeinsam mit dem ITSB die Einstellungen ihres Gerätes vor der geschäftlichen Nutzung - Nutzen Sie keine eigenen USB-Sticks ohne vorherige Prüfung durch den ITSB
Projekt-Sicherheitsprüfung	- Kontaktieren Sie bei neuen Projekten ihren Informations-sicherheitsbeauftragten und beziehen Sie diesen ein - Klassifizieren Sie das Projekt gemeinsam mit Ihrem Kunden und dokumentieren dies
Kunden-klassifizierung	- Fragen Sie ihren Kunden, wie das Projekt bei Ihm intern klassifiziert ist und welche Vorgaben dafür vorliegen - Lassen Sie sich die Sicherheitsrichtlinie ihres Kunden geben
Streng Vertrauliche Projekte/Inhalte	- Nutzen Sie nur explizit freigegebene Systeme - Achten Sie darauf für den Transport nur verschlüsselte Datenträger zu verwenden
Klassifizierung von Dokumenten und Informationen	- Klassifizieren Sie jede Information. - Achten Sie darauf, wer diese Information wirklich sehen muss - Nutzen Sie das Dokument "Hilfsmittel zur Klassifizierung"

Öffentlich - Klassifizierte Dokumente

- Keine besonderen Vorgaben. Achten Sie bitte im Sinne des Datenschutzes auf personenbezogene Daten
- Mailversand kann inhouse auch unverschlüsselt erfolgen

Intern - Klassifizierte Dokumente

- Speicherung auf verschlüsselter Festplatte
- Mailversand kann inhouse auch unverschlüsselt erfolgen
- Vermerk "intern" auf den Dokumenten reicht aus

Vertraulich - Klassifizierte Dokumente

- Speicherung auf verschlüsselter Festplatte
- Transport nur auf verschlüsselten Datenträgern
- Vermerk "vertraulich" mit Autor und Datum
- Mailversand nur verschlüsselt als Anhang
- Vernichtung Shredder Klasse 4

Streng Vertraulich - Klassifizierte Dokumente

- Speicherung auf verschlüsselter Festplatte
- Transport nur auf verschlüsselten Datenträgern
- Vermerk "streng vertraulich" mit Autor und Datum
- Mailversand nur verschlüsselt als Anhang an eindeutigen Empfänger
- Drucken nur wenn Sie selbst am Drucker stehen
- Vernichtung Schredder Klasse 5

Email Eingang

- Öffnen Sie nur Mails, deren Ursprung Sie kennen
- Öffnen Sie keine Mail Anhänge, die mit .exe enden oder unbekannte Dateiendungen haben
- Sollten Sie sich unsicher sein, kontaktieren Sie den ITSB

Email Versand

- Versenden Sie keine als vertraulich oder streng vertraulich eingestuften Information ohne diese vorher zu verschlüsseln
- Versenden Sie Mails immer nur über ihren internen Rechner

Dienstreisen

- Achten Sie darauf, dass niemand auf ihrem Rechner mitlesen kann, z.B. Sitznachbar im Zug oder Flugzeug
- Besprechen Sie vertrauliche und streng vertrauliche Angelegenheiten nur wenn niemand mithört
- Informieren Sie sich bei Auslandsreisen über den dortigen Sicherheitsstatus bei Ihrem ISB
- Synchronisieren Sie Ihr Mobile nicht mit Leihwagen