Saarotec

Richtlinie Informationssicherheit für Partnerfirmen

Informationssicherheit ist ein wesentliches Element des Saarotec-Leitbilds und integraler Bestandteil unserer Geschäftsstrategie.

Herausgeber:
Saarotec GmbH, In den Schankgärten 1, 66386 St. Ingbert
Leitung Materialwirtschaft, Martin Anstadt
Rev.01_20.10.2023

Inhalt

0. Ziel

Diese Richtlinie zur Informationssicherheit von Saarotec soll die getroffenen Maßnahmen zum Schutz der Informationen vor unbefugter Kenntnisnahme durch Dritte oder nichtberechtigte Mitarbeitende erläutern und darüber hinaus eine verbindliche Leitlinie für alle Partnerfirmen von Saarotec im Hinblick auf den Umgang mit Informationen sein.

Durch die verstärkte Abhängigkeit von moderner IT hat sich das Risiko der Beeinträchtigung von Informationsinfrastrukturen und deren Komponenten durch vorsätzliche Angriffe von innen und außen, durch fahrlässiges Handeln, Unkenntnis oder potenzielles Versagen der Technik sowohl qualitativ als auch quantitativ deutlich erhöht.

Mangelnde Informationssicherheit kann zu Störungen bei den betrieblichen Prozessen führen, die die Leistungsfähigkeit von Saarotec mindern und zu großen materiellen und immateriellen Schäden führen.

Vor diesem Hintergrund ist ein angemessenes Niveau der Informationssicherheit in den Geschäftsprozessen der Firma Saarotec zu organisieren.

1. Geltungsbereich

Diese Richtlinie zur Informationssicherheit gilt für alle Partnerfirmen der Saarotec. Dazu gehören alle Dienstleister und Lieferanten, die Zugriff auf Informationen erhalten.

2. Einhaltung von Rechtsvorschriften

Es ist stets darauf zu achten, dass geltender Datenschutz und Datensicherheit sowie die Unternehmensregelungen einzuhalten sind. Mitarbeiter der Partnerfirmen sind dahingehend zu schulen.

3. Allgemeine Regelungen

3.1 Klassifikation

Die Klassifizierung von Dokumenten erfolgt durch Saarotec. Anforderungen hierzu sind in der nachstehenden Tabelle zusammengefasst.

Einstufung (Klassifikation)	Anforderung
Vertraulich	**Kennzeichnung:** „vertraulich“ (personenbezogene Daten sind generell auch ohne Kennzeichnung vertraulich) **Speicherung:** unverschlüsselt **Transport:** Verschlüsselt **Entsorgung und Löschung:** Sichere Löschverfahren und Entsorgung nach DIN 66399 Stufe 4
Streng vertraulich	**Kennzeichnung:** „streng vertraulich“ **Speicherung:** Verschlüsselt **Transport:** Verschlüsselt **Entsorgung und Löschung:** Sichere Löschverfahren und Entsorgung nach DIN 66399 mind. Stufe 5

3.2 Arbeitsplatz (Clean Desk)

Der Arbeitsplatz ist so einzurichten, dass unbefugte Dritte keinen Einblick auf Informationen erhalten können. Nach Beendigung der Arbeit muss der Arbeitsplatz stets sauber hinterlassen werden. Dokumente, insbesondere vertrauliche und streng vertrauliche Dokumente, sind so aufzubewahren, dass Unbefugte keinen Zugriff darauf erlangen.

3.3 Überprüfung auf Schadsoftware

Die Partnerfirma ist dazu verpflichtet die zu transportierenden Daten auf Schadsoftware zu überprüfen. Bei Erkennung ist umgehend Saarotec zu informieren.

3.4 Backup

Sofern möglich, sind Daten so zu speichern, dass diese einer zentralen Datensicherung zugeführt werden. Die Datensicherungen sind zu schützen.

3.5 Zugriffsrechte

Hier wird das „Need-to-Know“ Prinzip angewandt. D.h. dem jeweiligen Mitarbeiter oder Partnerfirmenmitarbeiter werden nur die Informationen zur Verfügung gestellt, die er für seine Arbeiten benötigt. Zugriffe sind in angemessener Form abzusichern (z.B. Benutzername mit ausreichendem und komplexem Passwort oder starke Authentifizierung).
Eine Liste alle Partnerfirmenmitarbeiter, die Zugriff auf Saarotec-Systeme haben, ist auf Anfrage zu Verfügung zu stellen.

3.6 Zugangsdaten und Passwörter

Standardpasswörter müssen abgeändert werden.
Passwörter müssen dem aktuellen Stand der Technik entsprechen, z.B. BSI.
Zugangsdaten dürfen nicht weitergegeben werden.

3.7 Austausch von Daten

Die gesamte Kommunikation vertraulicher Informationen zwischen Saarotec und externen Partnern darf ausschließlich über kontrollierte Kanäle erfolgen, die durch ein spezielles Schutzsystem geführt werden. So ist der Austausch von schützenswerten Daten nur über den Saarotec-Filetransfer (Zugriff wird protokolliert) oder geeignete Kunden- und Lieferanten Plattformen gestattet. „Öffentliche“ Cloud-Dienste sind grundsätzlich nicht gestattet.

3.8 Umgang mit Informationssicherheitsvorfällen

Ereignisse Informationssicherheit betreffend (sofern Saarotec betroffen) sind umgehend der Kontaktperson von Saarotec als auch dem Informationssicherheitsbeauftragen (Informationssicherheit@Saarotec.de) mitzuteilen.

4. Zutritts- und Zugangsregelungen (vor Ort Termine)

4.1 Allgemein

Besucher müssen sich in der zentralen Besucherliste eintragen und wieder bei Verlassen austragen.

Der Zutritt zu kritischen Räumlichkeiten bzw. der Zugang zu den IT-Diensten ist gegen Unbefugte geschützt. Partnerfirmenmitarbeiter dürfen sich hier nicht frei und unkontrolliert bewegen, sondern ausschließlich mit Begleitung eines Mitarbeiters der Saarotec. Ein Fotografier-Verbot ist auf dem gesamten Gelände der Saarotec.

5. Remotezugänge

Saarotec sichert die Zugänge so ab, dass Partnerfirmen nur auf die notwendigen Ressourcen Zugriff haben. Die Verbindung darf nur so lange bestehen, bis die Arbeiten abgeschlossen sind.