KAISER GmbH
OBERFLÄCHENTECHNIK

# Lieferantenselbstauskunft

## Informationssicherheit

| | | | |
|---|---|---|---|
| Firmenname: | | Ansprechpartner: | |
| Straße / Nr.: | | Telefon: | |
| PLZ / Ort: | | Fax: | |
| Land: | | E-Mail: | |

**Sehr geehrte Damen und Herren,**

da Sie in die Auswahl der Zulieferer unseres Hauses gekommen sind, möchten wir Sie bitten, den Fragenkatalog verbindlich zu beantworten und uns diesen schnellstmöglich per E-Mail zurückzusenden.

Sofern Sie nach TISAX (min. AL 2), DIN EN ISO 27001 oder BSI Grundschutz zertifiziert sind oder ein Audit nach KRITIS durchführen mussten, bitten wir Sie, uns den Nachweis zukommen zu lassen bzw. über das ENX-Portal freizuschalten. Der Fragebogen muss dann nicht ausgefüllt werden.

Wir verpflichten uns, Ihre Angaben vertraulich und nur für den internen, eigenen Gebrauch zu behandeln.

| Frage | Ja | Nein | Trifft nicht zu |
|---|---|---|---|
| **Wir haben eine allgemeine Richtlinie für unsere Mitarbeiter, die Regelungen zur Informationssicherheit definiert.** | ◯ | ◯ | ◯ |
| **Wir haben eine klare Verantwortlichkeit für unsere Informationssicherheit definiert.** | ◯ | ◯ | ◯ |
| Die private Nutzung unserer Unternehmens-IT ist in einer Richtlinie geregelt. | ◯ | ◯ | ◯ |
| **Wir prüfen unsere Lieferanten auf die Umsetzung von Informationssicherheitsmaßnahmen.** | ◯ | ◯ | ◯ |
| **Alle Mitarbeiter haben eine schriftliche Vertraulichkeitserklärung abgegeben.** | ◯ | ◯ | ◯ |
| Zugänge für unsere IT-Infrastruktur werden konsequent nur gewährt, wenn sie für die Aufgabenerfüllung notwendig sind. | ◯ | ◯ | ◯ |
| **Normale User erhalten keine administrativen Zugänge.** | ◯ | ◯ | ◯ |
| Administrative Zugänge werden von uns regelmäßig auf deren Notwendigkeit überprüft. | ◯ | ◯ | ◯ |
| **Wir schulen regelmäßig unsere Mitarbeiter zu Informationssicherheitsthemen.** | ◯ | ◯ | ◯ |
| Wir haben schriftlich festgelegt, wie mit vertraulichen Informationen im Unternehmen umgegangen werden muss. | ◯ | ◯ | ◯ |
| Unsere Nutzer werden über die spezifischen Risiken mobiler Datenträger (z. B. durch Verlust oder Diebstahl oder durch das Einschleppen von Schadsoftware) informiert und sensibilisiert. | ◯ | ◯ | ◯ |
| Wir haben ein Schutzkonzept, wie unsere IT-Systeme abgesichert werden. | ◯ | ◯ | ◯ |
| **Wir haben ein geregeltes Verfahren, wie Zutritte zu unserem Unternehmen freigegeben werden.** | ◯ | ◯ | ◯ |

KAISER GmbH
OBERFLÄCHENTECHNIK

| Frage | Ja | Nein | Trifft nicht zu |
|---|---|---|---|
| **Wir haben ein geregeltes Besuchermanagement und stellen so sicher, dass unbefugte Personen keinen Zugriff auf Daten haben.** | ◯ | ◯ | ◯ |
| **Wir schützen uns vor dem Verlust der wichtigsten Unternehmensdaten durch eine Datensicherung.** | ◯ | ◯ | ◯ |
| **Wir setzen auf unseren Clients und Servern einen aktuellen Virenschutz ein.** | ◯ | ◯ | ◯ |
| Wir haben eine Richtlinie, in welcher der Umgang mit Sicherheitsvorfällen festgelegt ist. | ◯ | ◯ | ◯ |
| **Wir halten unsere Betriebssysteme aktuell (Sicherheits-Updates etc.).** | ◯ | ◯ | ◯ |

## Reaktionsplan

Fett markierte Fragen haben eine erhöhte Priorität. Wenn eine solche Frage oder vier Fragen der normalen Priorität mit „Nein“ beantwortet werden, ist ein Maßnahmenplan erforderlich, damit die Kaiser GmbH Oberflächentechnik mit Ihnen Daten austauschen kann.

**Bemerkungen (Lieferant):**

Datum

Unterschrift Lieferant

## Von der Kaiser GmbH Oberflächentechnik auszufüllen

Datenaustausch mit Lieferanten möglich: ◯ Ja ◯ Nein

Maßnahmenplan zum Austausch von Daten notwendig: ◯ Ja ◯ Nein

Maßnahmenplan erforderlich bis:

**Bemerkungen:**

Datum

Unterschrift