**PROBENFORMULAR FÜR DEN FRAGEBOGEN ZUR RISIKOBEWERTUNG VON LIEFERANTEN**

|  |  |
| --- | --- |
| NAME DES HERSTELLERS | HERSTELLERADRESSE |
|   |   |
| ANSPRECHPARTNER | KONTAKTINFORMATIONEN |
|   |   |

ANLEITUNG: Bitte füllen Sie diesen Fragebogen vollständig aus, hinterlassen Sie Notizen und fügen Sie gegebenenfalls unterstützende Unterlagen bei.

**Art des Datenanbieters hat Zugriff, um** *alle zutreffenden Punkte zu überprüfen*

|  |  |  |
| --- | --- | --- |
| **X** | **DATENTYP** | **NOTIZEN** |
|  | Kein Datenaustausch |  |
|  | Demografische Daten |  |
|  | Finanzdaten |  |
|  | Personenbezogene Daten (z.B. Name, Adresse, Telefonnummer) |  |
|  | Nicht öffentliche personenbezogene Daten (z. B. SSN, medizinische, proprietäre) |  |
|  | Andere:  |  |  |

**RICHTLINIEN UND PROZESSE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ja** | **Nein** | **N/A** | **FRAGE** | **NOTIZEN** |
|  |  |  | Dokumentiert, veröffentlicht und erzwingt Ihre Organisation Sicherheitsrichtlinien? |  |
|  |  |  | Dokumentiert und erzwingt Ihr Unternehmen HR-Richtlinien? |  |
|  |  |  | Dokumentiert und erzwingt Ihre Organisation Richtlinien für die autorisierte Nutzung von Netzwerkdiensten? |  |

**RICHTLINIEN UND PROZESSE Fortsetzung**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ja** | **Nein** | **N/A** | **FRAGE** | **NOTIZEN** |
|  |  |  | Dokumentiert und erzwingt Ihre Organisation Richtlinien für die autorisierte Verwendung von Unternehmens-E-Mail, Internet und Intranet? |  |
|  |  |  | Dokumentiert und erzwingt Ihre Organisation Verschlüsselungsrichtlinien und -standards? |  |
|  |  |  | Dokumentiert und durchsetzt Ihre Organisation Richtlinien in Bezug auf die Speicherung, Verwendung und Entsorgung sensibler Daten? |  |
|  |  |  | Dokumentiert und durchsetzt Ihre Organisation Richtlinien in Bezug auf die Speicherung, Verwendung und Entsorgung sensibler Daten durch Dritte? |  |
|  |  |  | Lagert Ihr Unternehmen Funktionalitäten im Zusammenhang mit dem Sicherheitsmanagement aus? |  |
|  |  |  | Halten Richtlinien und Verfahren die Datenschutzgesetze und -vorschriften in Bezug auf die Sicherheit, das Verschweigen und den Schutz von Kundendaten ein und halten sie ein? |  |
|  |  |  | Sind die Strafen, die mit der Nichteinhaltung der Richtlinien Ihrer Organisation verbunden sind, gut dokumentiert? |  |
|  |  |  | [Frage zu Richtlinien und Prozessen hier einfügen] |  |
|  |  |  | [Frage zu Richtlinien und Prozessen hier einfügen] |  |
|  |  |  | [Frage zu Richtlinien und Prozessen hier einfügen] |  |

**PHYSISCHE UND RECHENZENTRUMSSICHERHEITSMASSNAHMEN**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ja** | **Nein** | **N/A** | **FRAGE** | **NOTIZEN** |
|  |  |  | Überprüft und bewertet Ihr Unternehmen regelmäßig physische und ökologische Risiken? |  |
|  |  |  | Beinhalten die Perimeterkontrollen des Rechenzentrums die Verwendung von Zugangskarten? |  |
|  |  |  | Beinhalten Rechenzentrumsumkreiskontrollen die Verwendung von Tastatursteuerungen? |  |
|  |  |  | Beinhalten die Perimeterkontrollen des Rechenzentrums den Einsatz von Sicherheitspersonal? |  |
|  |  |  | Beinhalten die Perimeterkontrollen des Rechenzentrums die Verwendung von \_\_[hier eine Kennzahl hinzufügen]\_\_? |  |
|  |  |  | Verfügen Sie über Business Continuity-Verfahren, wenn das Büro aus irgendeinem Grund nicht zugänglich ist? |  |
|  |  |  | Sind alle Netzwerkgeräte physisch gesichert? |  |
|  |  |  | Verwendet Ihre Organisation Rechenzentrumsanbieter? |  |
|  |  |  | Verwendet Ihre Organisation Besucherprotokolle? Wenn ja, werden sie länger als 30 Tage aufbewahrt? |  |
|  |  |  | Unterhält Ihre Organisation eine schriftliche Richtlinie in Bezug auf physische Sicherheitsanforderungen für das Büro? |  |
|  |  |  | [Fügen Sie hier eine Frage zur physischen und Rechenzentrumssicherheit ein] |  |
|  |  |  | [Fügen Sie hier eine Frage zur physischen und Rechenzentrumssicherheit ein] |  |

**SICHERHEITSMASSNAHMEN FÜR MALWARE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ja** | **Nein** | **N/A** | **FRAGE** | **NOTIZEN** |
|  |  |  | Werden alle E-Mails auf Viren überprüft? |  |
|  |  |  | Ist Antivirensoftware erforderlich und auf allen Netzwerkcomputern aktiviert? |  |
|  |  |  | Hat Antivirensoftware eine festgelegte Häufigkeit von Scans auf Netzwerkcomputern? |  |
|  |  |  | Lässt Ihre Organisation die Installation nicht genehmigter Software auf Netzwerkcomputern zu? |  |
|  |  |  | [Frage zur Malware-Sicherheit hier einfügen] |  |
|  |  |  | [Frage zur Malware-Sicherheit hier einfügen] |  |
|  |  |  | [Frage zur Malware-Sicherheit hier einfügen] |  |

**INFORMATIONSSICHERHEITSMASSNAHMEN**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ja** | **Nein** | **N/A** | **FRAGE** | **NOTIZEN** |
|  |  |  | Verfügt Ihre Organisation über ein Informationssicherheitsprogramm? (Bitte geben Sie in der Spalte "Hinweise" einen Link zu allen relevanten öffentlich zugänglichen Sicherheits- und Datenschutzrichtlinien an.) |  |
|  |  |  | Wenn Ihre Organisation über ein Informationssicherheitsprogramm verfügt, gilt es dann für alle Vorgänge und Systeme, die sensible Daten verarbeiten? |  |
|  |  |  | Sind relevante Mitarbeiter und Führungskräfte professionell in der Informationssicherheit zertifiziert? |  |
|  |  |  | Ist der Zugriff auf Administratorebene auf die Netzwerkinfrastruktur beschränkt? |  |
|  |  |  | Gibt es strenge Kontrollen, um auf Sicherheitsprotokolle zuzugreifen? |  |
|  |  |  | [Frage zur Informationssicherheit hier einfügen] |  |
|  |  |  | [Frage zur Informationssicherheit hier einfügen] |  |
|  |  |  | [Frage zur Informationssicherheit hier einfügen] |  |

**SICHERHEIT DER NETZWERKINFRASTRUKTUR**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ja** | **Nein** | **N/A** | **FRAGE** | **NOTIZEN** |
|  |  |  | Unterhält Ihre Organisation eine Netzwerksicherheitsrichtlinie? |  |
|  |  |  | Sind alle Router mit Zugriffskontrolllisten systematisiert, um unbefugten Datenverkehr zu unterdrücken? |  |
|  |  |  | Sind Server-Betriebssysteme auf dem neuesten Stand gepatcht? |  |
|  |  |  | Verfügt Ihre Organisation über einen Prozess zum Nachverfolgen und Kommunizieren von Schwachstellen-Patches? |  |
|  |  |  | Sichert Ihre Organisation Ihre Daten? |  |
|  |  |  | Werden Backups gespeichert und getestet? |  |
|  |  |  | Sind Mitarbeitergeräte verschlüsselt? |  |
|  |  |  | Wird ein Drittanbieter verwendet, um die Sicherheit der Netzwerkinfrastruktur zu testen? |  |
|  |  |  | Setzen Sie Einbruchmeldesysteme ein? |  |
|  |  |  | [Frage zur Sicherheit der Netzwerkinfrastruktur hier einfügen] |  |
|  |  |  | [Frage zur Sicherheit der Netzwerkinfrastruktur hier einfügen] |  |
|  |  |  | [Frage zur Sicherheit der Netzwerkinfrastruktur hier einfügen] |  |

|  |
| --- |
| **ZUSATZINFORMATION** |
|  |

|  |  |  |
| --- | --- | --- |
| NAME UND TITEL DES RISIKOBEWERTERS | UNTERSCHRIFT | DATUM |
|  |  |  |

|  |
| --- |
| **VERZICHTSERKLÄRUNG**Alle Artikel, Vorlagen oder Informationen, die von Smartsheet auf der Website bereitgestellt werden, dienen nur als Referenz. Obwohl wir uns bemühen, die Informationen auf dem neuesten Stand und korrekt zu halten, geben wir keine Zusicherungen oder Gewährleistungen jeglicher Art, weder ausdrücklich noch stillschweigend, über die Vollständigkeit, Genauigkeit, Zuverlässigkeit, Eignung oder Verfügbarkeit in Bezug auf die Website oder die auf der Website enthaltenen Informationen, Artikel, Vorlagen oder zugehörigen Grafiken. Jegliches Vertrauen, das Sie auf solche Informationen setzen, erfolgt daher ausschließlich auf Ihr eigenes Risiko. |