**Smartsheet KOSTENLOS testen**

**VORLAGE FÜR DATENSICHERHEITSPLAN**

| VERSIONSVERLAUF |
| --- |
| VERSION | GENEHMIGT VON | ÜBERARBEITUNGSDATUM | BESCHREIBUNG DER ÄNDERUNG | AUTOR |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

DATENSICHERHEITSPLAN

NAME DES UNTERNEHMENS

Adresse

Ort, Bundesland und Postleitzahl

webaddress.com

Version 0.0.0

00/00/0000

1. **SYSTEMIDENTIFIZIERUNG**

Details zu System, Systeminhaber, Anzahl der Benutzer

1. **SYSTEMUMGEBUNG**

Details zu Systemverbindungen, Schlüsselgeräten, Hardware- und Softwarekomponenten

1. **ANFORDERUNGEN**

Details zu den geltenden Datensicherheitsanforderungen

* 1. **Zugriffssteuerung**

Stellen Sie sicher, dass das System den Zugriff auf autorisierte Benutzer begrenzt, die Art der zulässigen Transaktionen festlegt, bestimmte Funktionen auf "privilegierte" Benutzer begrenzt, den Fernzugriff überwacht, die Verbindung von Mobilgeräten steuert

* 1. **Bewusstsein und Training**

Stellen Sie sicher, dass sich alle in der Organisation der Sicherheitsrisiken des Systems bewusst sind und angemessen geschult sind, um Aktivitäten auf eine Weise durchzuführen, die Daten schützt, und Indikatoren für Bedrohungen oder Infiltrationen kennen

* 1. **Prüfung und Rechenschaftspflicht**

Stellen Sie sicher, dass das Unternehmen über ein fortlaufendes System verfügt, das ungewöhnliche oder nicht autorisierte Aktivitäten im System überwacht.

* 1. **Konfigurationsmanagement**

Basiskonfigurationen im gesamten System einrichten und pflegen, einschließlich der Steuerung und Überwachung von benutzerinstallierter Software

* 1. **Identifizierung und Authentifizierung**

Stellen Sie sicher, dass das System Systembenutzer und -geräte identifizieren und eine minimale Kennwortkomplexität durchsetzen kann

* 1. **Reaktion auf Vorfälle**

Ein System einrichten, das Vorfälle verfolgt, dokumentiert und meldet, die möglicherweise die Sicherheit beeinträchtigt haben, und testet die Reaktionsfähigkeit des Unternehmens auf einen Vorfall.

* 1. **Wartung**

Kontinuierliche Wartungsarbeiten am System durchführen

* 1. **Medienschutz**

Beschränken Sie den Zugriff auf die digitalen Medien des Systems auf autorisierte Benutzer und stellen Sie sicher, dass die digitalen Medien auf andere Weise geschützt sind

* 1. **Personalsicherheit**

Überprüfen Sie Personen, bevor Sie den Zugriff auf das System zulassen, und stellen Sie sicher, dass das System geschützt ist, nachdem Personen das Unternehmen verlassen haben

* 1. **Physischer Schutz**

Beschränken Sie den Zugriff auf physische Systeme und Ausrüstung auf autorisierte Personen

* 1. **Risikobewertung**

Bewerten Sie in regelmäßigen Abständen die Sicherheitsrisiken im normalen Betrieb des Systems und scannen Sie nach Schwachstellen und nehmen Sie Korrekturen vor, wenn Schwachstellen gefunden werden.

* 1. **Sicherheitsbewertung**

Bewerten Sie die Sicherheitskontrollen in regelmäßigen Abständen, um sicherzustellen, dass sie effektiv sind, und nehmen Sie bei Bedarf Korrekturen vor

* 1. **System- und Kommunikationsschutz**

Überwachen und schützen Sie die Kommunikation, die das System von außen erhält

* 1. **System- und Informationsintegrität**

Systemfehler rechtzeitig identifizieren, melden und korrigieren, Schutz vor bösartigem Code bieten und Sicherheitsalarme und -ratschläge überwachen

|  |
| --- |
| **HAFTUNGSAUSSCHLUSS**Alle von Smartsheet auf der Website aufgeführten Artikel, Vorlagen oder Informationen dienen lediglich als Referenz. Wir versuchen, die Informationen stets zu aktualisieren und zu korrigieren. Wir geben jedoch, weder ausdrücklich noch stillschweigend, keine Zusicherungen oder Garantien jeglicher Art 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 in solche Informationen setzen, ist aus eigener Verantwortung. |