**Smartsheet 無料お試し**

**データ セキュリティ計画テンプレート**

| バージョン履歴 |
| --- |
| バージョン | 承認者 | 改訂日 | 変更の説明 | 著者 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

データ セキュリティ計画

組織/団体名

番地

市区町村、都道府県、郵便番号

webaddress.com

バージョン 0.0.0

00/00/0000

1. **システム識別**

システム、システム所有者、ユーザー数の詳細

1. **システム環境**

システム相互接続、主要デバイス、ハードウェアおよびソフトウェアコンポーネントの詳細

1. **要件**

該当するデータ セキュリティ要件の詳細

* 1. **アクセス制御**

システムが許可されたユーザーへのアクセスを制限し、許可されたトランザクションの種類を設定し、特定の機能を「特権」ユーザーに制限し、リモート アクセスを監視し、モバイル デバイスの接続を制御するようにする

* 1. **意識向上とトレーニング**

組織内の全員がシステム セキュリティリスクを認識し、データを保護したり、脅威の指標を理解したり、侵入の指標を理解したりする方法で活動を実行するための十分なトレーニングを受けている

* 1. **監査と説明責任**

システム内の異常または不正なアクティビティを監視する継続的なシステムが組織に搭載されていることを確認する

* 1. **構成管理**

ユーザーがインストールしたソフトウェアの制御と監視など、システム全体でベースライン構成を確立および維持する

* 1. **識別と認証**

システムがシステムのユーザーとデバイスを特定し、パスワードの最小の複雑さを強制できるようにします

* 1. **インシデント対応**

セキュリティを損なう可能性のあるインシデントを追跡、文書化、報告し、組織がインシデントに対応する能力をテストするシステムを確立する

* 1. **メンテナンス**

システムの継続的なメンテナンスを実行する

* 1. **メディア保護**

システムのデジタル メディアへのアクセスを許可されたユーザーに制限し、デジタル メディアが他の方法で安全に保たれるようにする

* 1. **社員のセキュリティ**

システムへのアクセスを許可する前にユーザーをスクリーニングし、ユーザーが組織を離れた後にシステムが保護されていることを確認する

* 1. **物理的保護**

物理的なシステムや機器へのアクセスを許可された人に制限する

* 1. **リスク評価**

システムの通常の運用におけるセキュリティ リスクを定期的に評価し、脆弱性が見つかった場合に脆弱性をスキャンし、修正を行う

* 1. **セキュリティ評価**

セキュリティ制御を定期的に評価して、セキュリティ制御が効果的であることを確認し、必要に応じて修正を行う

* 1. **システムとコミュニケーションの保護**

システムが受信したシステム外からの通信を監視および保護する

* 1. **システムと情報の整合性**

システムの欠陥をタイムリーに特定、報告、修正し、悪意のあるコードや監視セキュリティアラートとアドバイザリからの保護を提供する

|  |
| --- |
| **– 免責条項 –**Smartsheet がこの Web サイトに掲載している記事、テンプレート、または情報などは、あくまで参考としてご利用ください。Smartsheet は、情報の最新性および正確性の確保に努めますが、本 Web サイトまたは本 Web サイトに含まれる情報、記事、テンプレート、あるいは関連グラフィックに関する完全性、正確性、信頼性、適合性、または利用可能性について、明示または黙示のいかなる表明または保証も行いません。かかる情報に依拠して生じたいかなる結果についても Smartsheet は一切責任を負いませんので、各自の責任と判断のもとにご利用ください。 |