**ベンダーリスク評価アンケートサンプルフォーム**

|  |  |
| --- | --- |
| ベンダー名 | ベンダー住所 |
|   |   |
| 連絡先 | 連絡先 |
|   |   |

指示:このアンケートに全文を記入し、メモを残し、必要に応じて補足文書を添付してください。

**データベンダーの性質は、***適用されるすべてをチェックするためのアクセス権を持つことになります*

|  |  |  |
| --- | --- | --- |
| **X** | **データ型** | **筆記** |
|  | データの交換なし |  |
|  | 人口統計データ |  |
|  | 財務データ |  |
|  | 個人データ(氏名、住所、電話番号など) |  |
|  | 非公開の個人データ(SSN、医療、専有など) |  |
|  | 他：  |  |  |

**ポリシーとプロセス**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **はい** | **いいえ** | **該当なし** | **質問** | **筆記** |
|  |  |  | 組織は、セキュリティ ポリシーを文書化、公開、および適用していますか。 |  |
|  |  |  | 組織では、人事ポリシーを文書化して適用していますか? |  |
|  |  |  | 組織では、ネットワーク サービスを承認済みで使用するためのポリシーを文書化して適用していますか。 |  |

**ポリシーとプロセスの** *続き*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **はい** | **いいえ** | **該当なし** | **質問** | **筆記** |
|  |  |  | 組織では、会社の電子メール、インターネット、およびイントラネットの承認された使用に関するポリシーを文書化して適用していますか。 |  |
|  |  |  | 組織では、暗号化ポリシーと標準を文書化して適用していますか。 |  |
|  |  |  | 組織は、機密データの保存、使用、廃棄に関するポリシーを文書化し、適用していますか。 |  |
|  |  |  | 組織は、第三者による機密データの保存、使用、廃棄に関するポリシーを文書化し、実施していますか。 |  |
|  |  |  | 組織は、セキュリティ管理に関連する機能を外部委託していますか。 |  |
|  |  |  | ポリシーと手順は、顧客データのセキュリティ、隠蔽、および保護に関連するプライバシーに関する法律および規制を遵守していますか? |  |
|  |  |  | 組織のポリシーへの違反に関連する罰則は、十分に文書化されていますか? |  |
|  |  |  | [ポリシーとプロセスの質問をここに挿入] |  |
|  |  |  | [ポリシーとプロセスの質問をここに挿入] |  |
|  |  |  | [ポリシーとプロセスの質問をここに挿入] |  |

**物理的およびデータ・センターのセキュリティ対策**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **はい** | **いいえ** | **該当なし** | **質問** | **筆記** |
|  |  |  | 組織は、物理的および環境的リスクを定期的に確認および評価していますか? |  |
|  |  |  | データ センターの境界制御にはアクセス カードの使用が含まれますか。 |  |
|  |  |  | データ センターの境界コントロールには、キーパッド コントロールの使用が含まれますか。 |  |
|  |  |  | データセンターの境界制御には警備員の使用が含まれますか? |  |
|  |  |  | データ センターの境界制御には、\_\_[メジャーをここに追加]\_\_ の使用が含まれますか。 |  |
|  |  |  | 何らかの理由でオフィスにアクセスできない場合のビジネス継続性手順はありますか。 |  |
|  |  |  | すべてのネットワーク機器は物理的に保護されていますか? |  |
|  |  |  | 組織ではデータセンタープロバイダーを使用していますか? |  |
|  |  |  | あなたの組織は訪問者ログを利用していますか?もしそうなら、それらは30日以上維持されていますか? |  |
|  |  |  | 組織では、オフィスの物理的なセキュリティ要件に関する書面によるポリシーを維持していますか。 |  |
|  |  |  | [物理およびデータセンターのセキュリティの質問をここに挿入] |  |
|  |  |  | [物理およびデータセンターのセキュリティの質問をここに挿入] |  |

**マルウェアのセキュリティ対策**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **はい** | **いいえ** | **該当なし** | **質問** | **筆記** |
|  |  |  | すべてのメールのウイルスがスキャンされていますか? |  |
|  |  |  | ウイルス対策ソフトウェアは、すべてのネットワーク コンピューターで必要で有効になっていますか。 |  |
|  |  |  | ウイルス対策ソフトウェアには、ネットワーク コンピューターでのスキャンの頻度が確立されていますか。 |  |
|  |  |  | 組織では、ネットワーク コンピューターへの承認されていないソフトウェアのインストールを許可していますか。 |  |
|  |  |  | [ここにマルウェアのセキュリティの質問を挿入] |  |
|  |  |  | [ここにマルウェアのセキュリティの質問を挿入] |  |
|  |  |  | [ここにマルウェアのセキュリティの質問を挿入] |  |

**情報セキュリティ対策**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **はい** | **いいえ** | **該当なし** | **質問** | **筆記** |
|  |  |  | 組織では、情報セキュリティ プログラムを実施していますか。(メモ欄には、関連するすべての一般向けセキュリティおよびプライバシーポリシーへのリンクを提供してください。 |  |
|  |  |  | 組織に情報セキュリティ プログラムがある場合、機密データを処理するすべての運用とシステムに適用されますか。 |  |
|  |  |  | 関連するスタッフとマネージャーは、情報セキュリティの専門的認定を受けていますか? |  |
|  |  |  | 管理者レベルのアクセスはネットワーク インフラストラクチャに制限されていますか。 |  |
|  |  |  | セキュリティログにアクセスするために厳格な管理が行われていますか? |  |
|  |  |  | [ここに情報セキュリティの質問を挿入] |  |
|  |  |  | [ここに情報セキュリティの質問を挿入] |  |
|  |  |  | [ここに情報セキュリティの質問を挿入] |  |

**ネットワークインフラのセキュリティ対策**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **はい** | **いいえ** | **該当なし** | **質問** | **筆記** |
|  |  |  | 組織ではネットワーク セキュリティ ポリシーを維持していますか。 |  |
|  |  |  | すべてのルータは、不正なトラフィックを抑制するためにアクセス制御リストで体系化されていますか? |  |
|  |  |  | サーバーオペレーティングシステムは最新レベルでパッチが適用されていますか? |  |
|  |  |  | 組織には、脆弱性パッチを追跡および伝達するためのプロセスがありますか? |  |
|  |  |  | 組織はデータをバックアップしていますか? |  |
|  |  |  | バックアップは保存され、テストされていますか。 |  |
|  |  |  | 従業員のデバイスは暗号化されていますか? |  |
|  |  |  | ネットワーク インフラストラクチャのセキュリティをテストするためにサード パーティが使用されていますか。 |  |
|  |  |  | 侵入検知システムを採用していますか? |  |
|  |  |  | [ここにネットワークインフラストラクチャのセキュリティの質問を挿入] |  |
|  |  |  | [ここにネットワークインフラストラクチャのセキュリティの質問を挿入] |  |
|  |  |  | [ここにネットワークインフラストラクチャのセキュリティの質問を挿入] |  |

|  |
| --- |
| **追加情報** |
|  |

|  |  |  |
| --- | --- | --- |
| リスク評価者の名前と役職 | 署名 | 日付 |
|  |  |  |

|  |
| --- |
| **免責事項**Web サイトで Smartsheet が提供する記事、テンプレート、または情報は、参照のみを目的としています。当社は、情報を最新かつ正確に保つよう努めていますが、本ウェブサイトまたは本ウェブサイトに含まれる情報、記事、テンプレート、また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、または可用性について、明示的または黙示的を問わず、いかなる種類の表明または保証も行いません。したがって、お客様がそのような情報に依拠する行為は、お客様ご自身の責任において厳格に行われるものとします。 |