**ISO 27001 管理チェックリスト テンプレート**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **セクション/****カテゴリ** | **要件/タスク** | **割り当て先** | **遵守していますか？** | **最終更新日** |
| ***5. 情報セキュリティに関するポリシー*** |
| 5.1 | セキュリティに関するポリシーがあること。 |   |   |   |
| 5.2 | すべてのポリシーが経営陣によって承認済みであること。 |   |   |   |
| 5.3 | コンプライアンスの証拠があること。 |   |   |   |
| ***6. 情報セキュリティの組織化*** |
| 6.1 | 役割と責任を明確にしていること。 |   |  |  |
| 6.2 | 職務分掌を明確にしていること。 |   |  |  |
| 6.3 | 認証機関/当局よりコンプライアンス認証に関する連絡があること。 |   |  |  |
| 6.4 | コンプライアンスに関して専門組織へ連絡を取ること。 |   |  |  |
| 6.5 | プロジェクト管理における情報セキュリティの証拠があること。 |   |  |  |
| 6.6 | モバイル デバイスに関する明確なポリシーがあること。 |   |  |  |
| 6.7 | リモート ワークに関する明確なポリシーがあること。 |   |  |  |
| ***7. 人的情報セキュリティ*** |
| 7.1 | 雇用前の従業員選考に関する明確なポリシーがあること。 |   |  |  |
| 7.2 | 人事の雇用条件に関する明確なポリシーがあること。 |   |  |  |
| 7.3 | 経営陣の責任に関する明確なポリシーがあること。  |   |  |  |
| 7.4 | 情報セキュリティの意識向上、教育および訓練に関する明確なポリシーがあること。 |   |  |  |
| 7.5 | 情報セキュリティ関連の懲戒手続に関する明確なポリシーがあること。 |   |  |  |
| 7.6 | 情報セキュリティ関連の人事の雇用の終了および変更に関する明確なポリシーがあること。 |   |  |  |
| ***8. 資産管理*** |
| 8.1 | 完全な資産目録リストがあること。 |   |  |  |
| 8.2 | 完全な資産の管理責任リストがあること。 |   |  |  |
| 8.3 | 資産利用の「許容範囲」に関する明確なポリシーがあること。 |   |  |  |
| 8.4 | 資産の返却に関する明確なポリシーがあること。 |   |  |  |
| 8.5 | 情報分類に関する明確なポリシーがあること。  |   |  |  |
| 8.6 | 情報のラベル付けに関する明確なポリシーがあること。 |   |  |  |
| 8.7 | 資産の取り扱いに関する明確なポリシーがあること。 |   |  |  |
| 8.8 | 利用者の秘密認証情報の管理にポリシーがあること。 |   |  |  |
| 8.9 | 媒体の処分に関する明確なポリシーがあること。 |   |  |  |
| 8.10 | 物理的媒体の輸送に関する明確なポリシーがあること。 |   |  |  |
| ***9. アクセス制御*** |
| 9.1 | 利用者の資産登録と登録解除に関する明確なポリシーがあること。 |   |  |  |
| 9.2 | 利用者アクセスの提供に関する明確なポリシーがあること。 |   |  |  |
| 9.3 | 特権アクセス権の管理に関する明確なポリシーがあること。 |   |  |  |
| 9.4 | 利用者の秘密認証情報の管理に関する明確なポリシーがあること。 |   |  |  |
| 9.5 | 利用者アクセス権のレビューに関する明確なポリシーがあること。 |   |  |  |
| 9.6 | アクセス権の削除または修正に関する明確なポリシーがあること。 |   |  |  |
| 9.7 | 秘密認証情報の利用に関する明確なポリシーがあること。 |   |  |  |
| 9.8 | 情報へのアクセス制限に関する明確なポリシーがあること。 |   |  |  |
| 9.9 | セキュリティに配慮したログイン手順に関する明確なポリシーがあること。 |   |  |  |
| 9.10 | パスワード管理システムに関する明確なポリシーがあること。 |   |  |  |
| 9.11 | 特権的なユーティリティ プログラムの使用に関する明確なポリシーがあること。 |   |  |  |
| 9.12 | プログラム ソース コードへのアクセス制御に関する明確なポリシーがあること。 |   |  |  |
| ***10. 暗号化*** |
| 10.1 | 暗号による管理策の利用に関する明確なポリシーがあること。 |   |  |  |
| 10.2 | 鍵管理に関する明確なポリシーがあること。 |   |  |  |
| ***11. 物理的および環境的セキュリティ*** |
| 11.1 | 物理的セキュリティ境界に関する明確なポリシーがあること。 |   |  |  |
| 11.2. | 物理的入退管理策に関する明確なポリシーがあること。 |   |  |  |
| 11.3 | オフィス、部屋、施設のセキュリティに関する明確なポリシーがあること。 |   |  |  |
| 11.4 | 外部および環境の脅威からの保護に関する明確なポリシーがあること。 |   |  |  |
| 11.5 | セキュリティを保つべき領域での作業に関する明確なポリシーがあること。 |   |  |  |
| 11.6 | 受渡場所に関する明確なポリシーがあること。 |   |  |  |
| 11.7 | 機器の設置および保護に関する明確なポリシーがあること。 |   |  |  |
| 11.8 | サポート ユーティリティに関する明確なポリシーがあること。 |   |  |  |
| 11.9 | ケーブル配線のセキュリティに関する明確なポリシーがあること。 |   |  |  |
| 11.10 | 装置の保守に関する明確なポリシーがあること。 |   |  |  |
| 11.11 | 資産の移動に関する明確なポリシーがあること。 |   |  |  |
| 11.12 | 構外にある機器および資産のセキュリティに関する明確なポリシーがあること。 |   |  |  |
| 11.13 | 装置のセキュリティを保った処分または再利用に関するポリシーがあること。 |   |  |  |
| 11.14 | 無人状態にある利用者装置に関する明確なポリシーがあること。 |   |  |  |
| 11.15 | クリア デスク クリア スクリーン ポリシーに関する明確なポリシーがあること。 |   |  |  |
| ***12. 運用セキュリティ*** |
| 12.1 | 操作手順書に関する明確なポリシーがあること。 |   |  |  |
| 12.2 | 変更管理に関する明確なポリシーがあること。 |   |  |  |
| 12.3 | 容量・能力の管理に関する明確なポリシーがあること。 |   |  |  |
| 12.4 | 開発環境、試験環境および運用環境の分離に関する明確なポリシーがあること。 |   |  |  |
| 12.5 | マルウェアに対する管理策に関する明確なポリシーがあること。 |   |  |  |
| 12.6 | システムのバックアップに関する明確なポリシーがあること。 |   |  |  |
| 12.7 | 情報のバックアップに関する明確なポリシーがあること。 |   |  |  |
| 12.8 | イベント ログ取得に関する明確なポリシーがあること。 |   |  |  |
| 12.9 | ログ情報の保護に関する明確なポリシーがあること。 |   |  |  |
| 12.10 | 実務管理者および運用担当者の作業ログに関する明確なポリシーがあること。 |   |  |  |
| 12.11 | クロックの同期に関する明確なポリシーがあること。 |   |  |  |
| 12.12 | 運用システムに関わるソフトウェアの導入に関する明確なポリシーがあること。 |   |  |  |
| 12.13 | 技術的ぜい弱性の管理に関する明確なポリシーがあること。 |   |  |  |
| 12.14 | ソフトウェアのインストールの制限に関する明確なポリシーがあること。 |   |  |  |
| 12.15 | 情報システムの監査に対する管理策に関する明確なポリシーがあること。 |   |  |  |
| ***13. コミュニケーション セキュリティ*** |
| 13.1 | ネットワーク管理策に関する明確なポリシーがあること。 |   |  |  |
| 13.2 | ネットワーク サービスのセキュリティに関する明確なポリシーがあること。 |   |  |  |
| 13.3 | ネットワークの分離に関する明確なポリシーがあること。 |   |  |  |
| 13.4 | 情報転送に関するポリシーと手順に関する明確なポリシーがあること。 |   |  |  |
| 13.5 | 情報転送に関する合意に関する明確なポリシーがあること。 |   |  |  |
| 13.6 | 電子的メッセージ通信に関する明確なポリシーがあること。 |   |  |  |
| 13.7 | 秘密保持契約または守秘義務契約に関する明確なポリシーがあること。 |   |  |  |
| 13.8 | システムの取得、開発、メンテナンスに関する明確なポリシーがあること。 |   |  |  |
| ***14. システムの取得、開発、保守*** |
| 14.1 | 情報セキュリティ要求事項の分析および仕様化に関する明確なポリシーがあること。 |   |  |  |
| 14.2 | 公衆ネットワーク上のアプリケーション サービスのセキュリティの考慮に関する明確なポリシーがあること。 |   |  |  |
| 14.3 | アプリケーション サービスのトランザクションの保護に関する明確なポリシーがあること。 |   |  |  |
| ***15. 供給者関係*** |
| 15.1 | 供給者関係に関する明確なポリシーがあること。 |   |  |  |
| ***16. 情報セキュリティ インシデント管理*** |
| 16.1 | 情報セキュリティ管理に関する明確なポリシーがあること。 |   |  |  |
| ***17. 事業継続管理の情報セキュリティの側面*** |
| 17.1 | 冗長性に関する明確なポリシーがあること。 |   |  |  |
| ***18. 遵守*** |
| 18.1 | 適用法令および契約上の要求事項の特定に関する明確なポリシーがあること。 |   |  |  |
| 18.2 | 知的財産権に関する明確なポリシーがあること。 |   |  |  |
| 18.3 | 記録の保護に関する明確なポリシーがあること。 |   |  |  |
| 18.4 | プライバシーおよび個人を特定できる情報の保護に関する明確なポリシーがあること。 |   |  |  |
| 18.5 | 暗号化機能に対する規制に関する明確なポリシーがあること。 |   |  |  |
| 18.6 | 情報セキュリティのための方針群および標準の順守に関する明確なポリシーがあること。 |   |  |  |
| 18.7 | 技術的順守のレビューに関する明確なポリシーがあること。 |   |  |  |

**– 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。

このテンプレートはサンプルとしてのみ提供されています。このテンプレートは、決して法的またはコンプライアンス上のアドバイスを意味するものではありません。このテンプレートのユーザーは、必須の情報および目的を達成するために必要な情報を見極める必要があります。