ISMS-B-02

ISO27001:2022　適用宣言書　抜粋サンプル

採否-〇採用×採用せず　採用/除外理由-リ：リスクアセスメントの結果　法：法令規制要求　契：契約上の義務　事：事業上の要求

ISO27001:2022 附属書A 管理策	採否	採否の根拠	選択及び適用除外の理由	実行の有無
5　組織的管理策				
5.1 情報セキュリティのための方針群	〇	事	各方針を従業員並びに利害関係者へ確実に伝え、理解させ、方針に沿ったセキュリティ体制が正しく実施され、方針の内容が適切であることを確実にするため	有
5.2 情報セキュリティの役割及び責任	〇	事	情報セキュリティに関する役割及び責任を明確にするため	有
5.3 職務の分離	〇	リ	業務上及び故意の不正やオペレーションミスを防ぐため	有
5.4 管理層の責任	〇	事	経営陣が、情報セキュリティにおける自らの役割を理解し、全ての要員が自らの情報セキュリティの責任を認識し、果たすことを確実にするため	有
5.5 関係当局との連絡	〇	事	情報セキュリティ上の事件・事故へ迅速な対応を行い、行政等との適切な連絡体制を維持するため	有
5.6 専門組織との連絡	〇	事	組織内で対応できないことを組織外の情報セキュリティ専門家より助言を受けるため	有
5.7 脅威インテリジェンス	〇	リ	組織の脅威環境を認識し、適切な低減処置を講じることができるようにするため	有
5.8 プロジェクトマネジメントにおける情報セキュリティ	〇	リ	プロジェクトマネジメントにおいても情報セキュリティの取り組みを行うため	有
5.9 情報及びその他の関連資産の目録	〇	事	情報資産の明確な識別を行い、管理責任者を明確にし、適切に保護するため	有
5.10 情報及びその他の関連資産の許容される利用	〇	事	全ての情報資産利用者に対して、その利用範囲を明確にし、情報資産に応じた取り扱いを適切に行うため	有
5.11 資産の返却	〇	事、契	情報資産の返却を確実に行うため	有
5.12 情報の分類	〇	事	情報資産の重要度を認識・分類し、適切な管理策を実施するため	有
5.13 情報のラベル付け	〇	事	情報資産を分類し、適切なラベル表示を行い、そのラベル区分に応じた取り扱いを行うため	有
5.14 情報の転送	〇	リ、事	情報転送において、情報の紛失、変更、誤用及び漏洩を防止するため	有
5.15 アクセス制御	〇	リ、事	アクセスの必要のある者にだけアクセス権限を与え、適切にアクセス制御を行うため	有
5.16 識別情報の管理	〇	リ、事	識別情報のライフサイクル全体（登録、変更、抹消、休止・有効化）を適切に管理するため	有
5.17 認証情報	〇	リ、事	認証情報の割り当て及びその管理を適切に行い、利用者の責任を理解させるため	有
5.18 アクセス権	〇	リ、事	アクセス権の提供と無効化及びアクセス権のレビューを適切に行うため	有
5.19 供給者関係における情報セキュリティ	〇	リ、事	供給者の製品又はサービスに関する情報セキュリティリスクを軽減するため	有
5.20 供給者との合意における情報セキュリティの取扱い	〇	リ、契	供給者と合意したレベルの情報セキュリティを契約によって、確実に維持するため	有
5.21 情報通信技術(ICT)サプライチェーンにおける情報セキュリティの管理	〇	リ、事	ICT製品又はサービスのサプライチェーンにおいても情報セキュリティを確実に管理するため	有
5.22 供給者のサービス提供の監視、レビュー及び変更管理	〇	リ、事	供給者と合意したレベルの情報セキュリティやサービス提供を確実に維持するため	有
5.23 クラウドサービス利用における情報セキュリティ	〇	リ、事	クラウドサービスの利用における情報セキュリティを確実に規定及び管理するため	有
5.24 情報セキュリティインシデント管理の計画策定及び準備	〇	リ、事	情報セキュリティ事象に関する伝達を含む、情報セキュリティインシデントへの迅速で、効果的で、一貫性があり、かつ秩序のある対応を確実にするため	有
5.25 情報セキュリティ事象の評価及び決定	〇	リ	情報セキュリティ事象の効果的な分類及び優先順位付けを確実にするため	有
5.36 情報セキュリティのための方針、規則及び標準の順守	〇	事	情報セキュリティが情報セキュリティ方針、トピック固有の方針、規則及び標準に従い、実施及び運用されていることを確実にするため	有
5.37 操作手順書	〇	事	情報処理設備の正確かつセキュリティに配慮した操作を確実にするため	有
6　人的管理策				
6.1 選考	〇	事	採用する従業員が、予定する役割に対して適格かつ適切であることを確実にするため	有
6.2 雇用条件	〇	事	採用する従業員が、予定する役割における自らの情報セキュリティの責任を理解することを確実にするため	有
6.7 リモートワーク	〇	リ、事	従業員がリモートで作業する場合に情報セキュリティを確実にするため	有
6.8 情報セキュリティ事象の報告	〇	事	従業員が情報セキュリティ事象において、時機を失せず、一貫性をもって効果的に報告することを確実にするため	有

ISO27001:2022 附属書A 管理策	採否	採否の根拠	選択及び適用除外の理由	実行の有無
7 物理的管理策				
7.1 物理的セキュリティ境界	○	リ	組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷及び干渉を防ぐため	有
7.2 物理的入退	○	リ	組織の情報及びその他の関連資産に、認可された物理的なアクセスだけがなされることを確実にするため	有
7.3 オフィス、部屋及び施設のセキュリティ	○	リ	事務所、部屋、関連施設において、組織の情報及びその他の関連資産に対する認可されていない物理的アクセス、損傷並びに干渉を防ぐため	有
7.14 装置のセキュリティを保った処分又は再利用	○	リ	処分または再利用する装置からの情報漏えいを防止するため	有
8 技術的管理策				
8.1 利用者エンドポイント機器	○	リ	スマートフォン、ノートPC等のユーザーエンドポイントデバイスを使用することでもたらされるリスクから情報を保護するため	有
8.2 特権的アクセス権	○	リ	認可されたユーザーだけに特権アクセス権が与えられることを確実にするため	有
8.3 情報へのアクセス制限	○	リ	情報及び関連するその他の資産への認可されたアクセスのみを確実にし、認可されていないアクセスを防止するため	有
8.29 開発及び受入れにおけるセキュリティテスト	○	リ	アプリケーションやコードを運用環境に導入するときに、情報セキュリティ要求事項が満たされているか、妥当性を確認するため	有
8.30 外部委託による開発	○	リ	自社が要求する情報セキュリティ対策が、外部委託したシステム開発で実施されることを確実にするため	有
8.31 開発環境、テスト環境及び本番環境の分離	○	リ	開発やテストの活動による影響から本番環境とデータを保護するため	有
8.32 変更管理	○	リ	変更を実行するときに情報セキュリティを維持するため	有
8.33 テスト用情報	○	リ	テストの適切な実施、及びテストに使用された本番環境での情報の保護を確実にするため	有
8.34 監査におけるテスト中の情報システムの保護	○	リ	監査やその他の保証活動が運用システムや業務プロセスに与える影響を最小限に抑えるため	有