HP セキュリティ対策の概要

お客様のデータを保護するために、HP は、ポリシー、プラクティス、手順、組織構造などの強固な情報セキュリティ制御を遵守し、自身および顧客の情報 (HP のカスタマおよびデータ処理アデンダで定義されている個人データを含む) の機密性、整合性、および可用性を保護します。以下に、HP の全社における技術的/組織的セキュリティ対策の概要を示します。

1. セキュリティ ポリシー

   HP では、HP およびカスタマ データの保護を目的とした、グローバルに適用されるポリシー、規格、および手順を維持しています。HP のセキュリティ ポリシーの詳細は、HP のデータおよびシステムの整合性を保護するために、機密として扱われます。ただし、以下に、当社の主要なポリシーの概要を示します。

2. 情報セキュリティ機構

   HP の情報セキュリティ プログラムは、組織の情報セキュリティ戦略と管理を指示し、維持するよう設計されています。このシステムは、HP のセキュリティ ポリシーおよび制御に全社的に準拠するとともに、お客様のセキュリティ要件を遵守することを保証します。業界標準のサイバーセキュリティ フレームワーク、法律、および規制に合わせて構成されたフレームワークは、HP の、進化する脅威状況に対処するために、毎年見直されます。

3. サイバーセキュリティ リスク管理

   HP のサイバーセキュリティ リスク管理プログラムは、情報資産の機密性、完全性、および可用性を維持することを目的として設計されています。このプログラムは、サイバーセキュリティ リスクを特定、評価、優先順位付け、治療、解決、追跡、および報告するための一貫したアプローチを提供します。HP は、リスク アペタイトを、許容される損失の露出レベルとリスク許容度をこのアペタイトからの分散の程度として定義します。リスクは、定義された手法を使用して評価されるため、HP は許容できるレベルまで情報セキュリティ リスクを軽減できます。このプログラムは、HP のエンタープライズ リスク管理プロセスに合わせて調整されます。

取終更新日: 2024 年 9 月

4. HR セキュリティ

HP 人事セキュリティ ポリシーは、施設、情報システム、およびその他の資産へのアクセス プロセスを確立することで、従業員のライフサイクル全体を通じて情報セキュリティを確保します。これには、秘密保持契約および秘密保持契約の書面による承認書の取得、バックグラウンド スクリーニング手続きの実施が含まれます。HP の採用応募者は、関連する法律、規則、倫理に従ってバックグラウンド検証を行う必要があります。

5. 資産管理

HP には、技術情報資産を識別し、重要な資産を分類して、個人データを含む各情報分類タイプの、文書化された処理手順を管理するプロセスがあります。これらの手順は、保管、送信、通信、アクセス、ログ、保持、破棄、廃棄、インシデント管理、および違反通知を対象としています。HP のセキュリティ ポリシーおよび規格では、メディアの安全な廃棄も義務付けられています。

6. データ セキュリティ

HP のデータ セキュリティ プログラムでは、データの機密性、信頼性、および整合性を保護するために実装する必要があるセキュリティ プラクティスと技術管理に関する概要を説明します。法的要件、価値、重要度、および不正な開示や変更に対する機密性は、HP のデータ セキュリティ ポリシーに基づいて情報がどのように分類されるかを決定する要因の一部です。このポリシーでは、データの処理手順に加え、データの暗号化、削除、収集と処理、保持、バックアップ、およびデータ損失の防止について説明しています。

7. アクセス制御

HP では、論理アクセス制御の最小権限の原則を採用し、一意のユーザー ID とパスワードによってユーザー アクセスを提供します。パスワード ポリシーは、複雑さ、強度、有効性、およびパスワード履歴の制御を定義します。アクセス権は定期的に確認され、人員の退職時に取り消されます。クライアント システムへのアクセスを、契約に応じて許可または取り消すために、ユーザー アカウントの作成と削除に関する同意済みの手順が実装されています。

8. 暗号化技術

HP では、情報資産の機密性、完全性、および可用性を確保するために、暗号化に関する一連の堅牢なプロセスを定義しました。承認されたプロトコルでは、個人データを含む特定の資産の暗号化が必要です。当社の暗号プログラムは、情報と通信を確保するために数学的技術を使用し、正規の関係者のみがデータにアクセスできるようにしています。HP の情報セキュリティ プログラムの重要なコンポーネントは、不正アクセスや改ざんからデータを保護しています。

9. 物理的および環境的セキュリティ

HP の施設は、セキュリティ ガード、電子アクセス制御、閉回路テレビ (CCTV) など、物理的および電子的なアクセス制御を使用してセキュリティ保護されています。また、UPS やディーゼル発電機を使用して重要なサービスをサポートし、温度制御や電源バックアップなど、必要なインフラ サポートも備えています。すべての HP 担当者が登録されており、適切な識別バッジを身につける必要があります。

10. オペレーション管理

HP では、ワークステーション、サーバー、ネットワーク機器など、テクノロジ インフラストラクチャの最小限の強化要件を確立しています。これらのデバイスは、事前に強化されたオペレーティング システム イメージを使用します。要件はオペレーティング システムや実装されているコントロールによって異なります。さらに、HP では、24 時間 365 日監視および管理されるネットワーク侵入検出/防止システム (NIDS/NIPS) を導入しました。

11. 通信セキュリティ

通信セキュリティは、企業ネットワーク内の情報を保護します。これには、ネットワーク セキュリティ コンポーネント (ファイアウォールなど) のインストールと管理、ネットワークの分離、Web フィルタリングおよび電子メール処理制御が含まれます。さらに、通信チャネルの監視と管理を行い、不正アクセスやデータ違反を検出および防止します。

最終更新日: 2024 年 9 月

12. システム セキュリティ

HP のポリシーでは、システムとソフトウェアのライフサイクル全体にわたる安全な開発方法を義務付けています。ソフトウェア開発ライフサイクルには、開始、開発/取得、実装、運用、および廃棄が含まれます。すべてのシステム コンポーネントは、全体的なセキュリティへの影響について評価されます。HP は、ユーザー資格情報の検証、デジタル署名、暗号化、安全な通信プロトコル、適切なネットワーク セキュリティ ゾーン内でのトランザクション詳細の保存など、アプリケーション サービス トランザクションの制御を確立しています。定期的な内部脆弱性スキャンも実行されます。

13. 第三者および請負業者

HP には、包括的な契約上のセキュリティ要件を満たす請負業者を選択するプロセスがあります。HP またはお客様のデータを処理したり、HP ネットワークにアクセスしたりするサプライヤについては、HP サイバーセキュリティがリスク評価を実施し、物理的、技術的、管理上の保護手段を備えた情報セキュリティ プログラムを検証します。この評価を実施しないと、サプライヤは HP の情報にアクセスできません。

14. 情報セキュリティ インシデント管理

HP には、目的、スコープ、役割、責任、管理に関するコミットメント、組織の調整、実施手順、およびコンプライアンス チェックをまとめた包括的なサイバー インシデント管理プロセスがあります。このプロセスは毎年見直され、更新されます。インシデント対応と危機管理のトレーニングを受けた HP サイバーセキュリティ担当者を含むサイバー インシデント対応チームは、プロセスやインシデント、イベントについて定期的に会議を開いてレビューを行います。

15. 事業継続性管理

HP のグローバルな継続性プログラムは、コラボレーション、標準化、および文書化された計画プロセスを通じて、エンドツーエンドの継続性を保証します。同社は、少なくとも毎年、すべての計画の有効性、テスト、および更新を確保するために、定期的に事業継続性計画を実行しています。また、事業継続性計画に関わるすべての担当者は、適切な研修を受けます。

取終更新日: 2024 年 9 月

16. 遵守

遵守は、効果的な情報セキュリティ プログラムに対する法的、契約的、および内部的な期待を満たす HP のアプローチを形作ります。定期的な情報セキュリティ レビューにより、各事業グループの業務に、プロトコルが統合されます。また、レビュー プロセスでは、要件の進化に伴う現在の法的義務を反映するよう文書を更新します。

17. ペイメント カード業界

ペイメント カード 業界 (PCI) フレームワークは、PCI コンプライアンスの達成に向けた HP のアプローチをガイドし、PCI DSS に沿ったビジネス責任とセキュリティ管理を概説します。ファイアウォールなどのネットワーク セキュリティ制御をインストールして保守することにより、HP は PCI コンプライアンス要件を満たすことができます。

18. HP 製品セキュリティ

HP 製品セキュリティには、コード署名、製品のセキュリティ脆弱性の管理、セキュリティ情報の発行、製品のセキュリティに関する問題の報告など、HP 製品を保護するための基本的なプラクティスが含まれています。これらの措置により、ユーザーにとっての HP 製品の安全性と信頼性が維持されます。製品のセキュリティは HP では最も重要です。お客様の信頼の維持と、潜在的な脅威の排除に役立ちます。

19. HP サービス セキュリティ

HP サービス セキュリティには、HP のお客様に提供されるサービスを保護するための基本的なプラクティスが含まれています。このポリシーは、HP インフラストラクチャのホスト、サードパーティのホスト環境、パートナーホスト環境、カスタマホスト環境など、サービス セキュリティのさまざまな分野に対応します。これらの措置により、HP サービスは、ユーザーにとって安全で信頼性の高い状態を維持できます。強固なセキュリティ プラクティスを実装することにより、HP は、製品およびサービスの安全性と完全性を確保し、すべてのユーザーにとって安全で信頼できる環境を構築します。

取終更新日: 2024 年 9 月