HP 보안 조치 요약

HP 는 고객 데이터를 보호하기 위해 HP 정보 및 고객 정보(HP 고객 및 데이터 처리 부록에서 정의한 개인 데이터 포함)의 기밀성, 무결성, 가용성을 보호하기 위해 정책, 관행, 절차 및 조직 구조를 포함하는 강력한 정보 보안 제어 기능을 준수합니다. 아래의 내용은 HP 전체에서 시행되는 HP 의 기술/조직 보안 조치의 개요입니다.

1. 보안 정책

   HP 는 HP 및 고객 데이터를 보호하기 위해 전 세계적으로 적용되는 정책, 표준 및 절차를 유지합니다. HP 의 보안 정책에 관한 세부 사항은 HP 데이터 및 시스템의 무결성을 보호하기 위해 기밀로 유지됩니다. 하지만 아래에서 핵심 정책의 요약을 확인할 수 있습니다.

2. 정보 보안 조직

   HP 의 정보 보안 프로그램은 조직의 정보 보안 전략 및 제어를 관리 및 유지하도록 설계되었습니다. 이 시스템을 사용하면 HP 의 보안 정책과 제어를 전사적으로 준수하고 고객의 보안 요구 사항을 충족할 수 있습니다. 업계 표준 사이버 보안 프레임워크, 법률 및 규정과 일치하도록 구성된 이 시스템은 HP 의 진화하는 위협 환경에 적응하기 위해 매년 검토됩니다.

3. 사이버 보안 위험 관리

   HP 의 사이버 보안 위험 관리 프로그램은 기밀성, 무결성 및 정보 자산의 가용성을 보존하도록 설계되었습니다. 이 프로그램은 사이버 보안 위험 식별, 평가, 우선순위 지정, 처리, 구제, 추적 및 보고를 위한 일관된 접근 방식을 제공합니다. HP 는 위험 성향을 허용 가능한 손실 노출 수준으로 정의하고, 위험 허용 범위는 허용되는 위험 성향과의 편차로 정의합니다. 위험은 정의된 방법론을 사용하여 평가되므로 HP 는 정보 보안 위험을 허용 가능한 수준으로 완화할 수 있습니다. 이 프로그램은 HP 의 기업 위험 관리 프로세스에 부합합니다.

마지막 업데이트: 2024 년 9 월

4. HR 보안

   HP 인적 자원 보안 정책은 시설, 정보 시스템 및 기타 자산에 대한 액세스 프로세스를 설정하여 직원 수명 주기 전반에 걸쳐 정보 보안을 보장합니다. 여기에는 기밀 유지 및 비공개 동의서를 통해 서면 확인을 받는 것뿐만 아니라 신원 조회 절차를 진행하는 것이 포함됩니다. HP 에 입사하고자 하는 모든 지원자는 관련 법, 규정 및 윤리에 따라 신원 확인 확인을 완료해야 합니다.

5. 자산 관리

   HP 는 기술 정보 자산을 식별, 중요 자산을 분류하고, 개인 데이터를 포함하여 각 정보 분류 유형에 대한 문서 처리 절차를 유지 및 관리하는 프로세스를 제공합니다. 이 프로세스는 저장, 전송, 통신, 액세스, 기록, 보관, 폐기, 처분, 사고 관리, 위반 통지를 다룹니다. HP 보안 정책과 표준에는 또한 용지의 안전한 폐기가 의무화되어 있습니다.

6. 데이터 보안

   HP 의 데이터 보안 프로그램에는 데이터의 기밀성, 인증, 무결성을 보호하기 위해 구현해야 하는 보안 관행과 기술 통제가 개략적으로 설명되어 있습니다. HP 데이터 보안 정책에 따라 정보가 분류되는 방식을 결정하는 몇 가지 요소는 법적 요구 사항, 가치, 중요도 및 무단 공개 또는 수정에 대한 민감도입니다. 이 정책은 데이터 처리 절차 외에도 데이터 암호화, 삭제, 수집 및 처리, 보존, 백업 및 데이터 손실 방지를 개괄합니다.

7. 액세스 제어

   HP 는 고유의 사용자 ID 와 암호를 통해 사용자 액세스를 제공하는 논리적 액세스 제어에 대해 최소 권한의 원칙을 사용합니다. 암호 정책은 복잡성, 강도, 유효성 및 암호 내역 제어를 정의합니다. 액세스 권한은 주기적으로 검토되며 직원 퇴사 시 취소됩니다. 계약 기간 동안에는 사용자 계정 생성 및 삭제에 대해 합의된 절차를 통해 클라이언트 시스템에 대한 액세스 권한을 부여하고 취소할 수 있습니다.

8. 암호화

   HP 는 기밀성, 무결성 및 정보 자산의 가용성을 보장하기 위해 암호화에 대한 강력한 프로세스를 정의했습니다. 승인된 프로토콜에는 개인 데이터가 포함된 특정 자산에 대한 암호화가 필요합니다. HP 의 암호화 프로그램에는 정보 및 통신을 보호하기 위해 수학적 기술을 사용하여 권한이 있는 당사자만 데이터에 액세스할 수 있도록 보장합니다. HP 정보 보안 프로그램의 핵심 요소는 무단 액세스 및 조작으로부터 데이터를 보호하는 것입니다.

마지막 업데이트: 2024 년 9 월

9. 물리적 및 환경적 안전

HP 시설은 경비원, 전자 액세스 제어 및 폐쇄 회로 텔레비전(CCTV)을 포함한 다양한 물리 및 전자 액세스 제어를 사용하여 보호됩니다. 시설에는 중요 서비스를 지원하기 위해 UPS 및/또는 디젤 발전기를 사용하는 온도 제어 및 전원 백업을 포함한 필수 인프라 지원 또한 제공됩니다. 모든 HP 직원은 등록되어 있으며 적절한 식별 배지를 소지해야 합니다.

10. 작업 관리

HP 는 워크스테이션, 서버 및 네트워크 장비를 비롯한 기술 인프라에 대해 최소 강화 요건을 마련했습니다. 이러한 장치는 사전 강화된 운영 체제 이미지를 사용하며 요구 사항은 운영 체제 및 구현되는 제어에 따라 다릅니다. 또한 HP 는 연중무휴 24 시간 모니터링 및 관리되는 네트워크 침입 감지/방지 시스템(NIDS/NIPS)를 배포했습니다.

11. 통신 보안

통신 보안은 기업 네트워크 내에서 정보를 보호합니다. 여기에는 네트워크 보안 구성 요소(예: 방화벽), 네트워크 분리, 웹 필터링 및 전자 메일 처리 제어의 설치 및 관리가 포함됩니다. 또한 권한 없는 액세스 또는 데이터 유출을 감지하고 방지하기 위해 통신 채널을 모니터링 및 관리하는 것이 포함됩니다.

12. 시스템 보안

HP 의 정책은 수명 주기 내내 시스템 및 소프트웨어를 위한 안전한 방법 개발을 의무화합니다. 소프트웨어 개발 수명 주기는 초기화, 개발/획득, 구현, 운영 및 폐기를 포함합니다. 모든 시스템 구성 요소는 보안 전체에 미치는 영향을 평가합니다. HP 는 사용자 자격 증명 확인, 디지털 서명, 암호화, 보안 통신 프로토콜, 해당 네트워크 보안 영역 내 트랜잭션 세부 사항 저장 등 응용 프로그램 서비스 트랜잭션에 대한 제어를 설정했습니다. 또한 일반적인 내부 취약점 스캔도 수행됩니다.

13. 타사 및 하도급업체

HP 는 종합적인 계약 보안 요구 사항을 준수하는 하도급업체를 선택할 수 있는 프로세스를 제공합니다. HP 또는 고객 데이터를 처리하거나 HP 네트워크에 액세스하는 해당 공급업체의 경우 HP 사이버 보안을 통해 위험 평가를 수행하여 물리, 기술 및 관리적 보호 장치를 사용하여 정보 보안 프로그램을 확인합니다. 공급업체가 HP 정보에 액세스하려면 이러한 평가가 필요합니다.

마지막 업데이트: 2024 년 9 월

14. 정보 보안 사고 관리

    HP 는 목적, 범위, 역할, 책임, 관리 약속, 조직 조정, 구현 절차 및 규정 준수 확인을 개괄하는 포괄적인 사이버 사고 관리 프로세스를 제공합니다. 이 프로세스는 매년 검토 및 업데이트됩니다. 사고 대응 및 위기 관리에 교육을 받은 HP 사이버 보안 담당자를 포함한 사이버 사고 대응 팀은 프로세스 및 사건 또는 이벤트에 대한 정기적인 모의 검토를 수행합니다.

15. 비즈니스 연속성 관리

    HP 의 글로벌 운영 연속성 프로그램은 협력, 표준화 및 문서화된 계획 프로세스를 통해 엔드 투 엔드 연속성을 보장합니다. HP 는 비즈니스 연속성 계획의 효과를 보장하기 위해 모든 계획을 최소 1 년에 한 번씩 테스트 및 업데이트합니다. 또한 비즈니스 연속성 계획에 참여하는 모든 직원은 관련 교육을 받습니다.

16. 규정 준수

    규정 준수는 효과적인 정보 보안 프로그램에 대한 법적, 계약적, 내부적 기대를 충족하는 HP 의 접근 방식을 형성합니다. 정기적인 정보 보안 검토는 프로토콜이 각 비즈니스 그룹의 운영에 통합되도록 보장합니다. 또한 검토 프로세스는 요건 변화에 따라 현행 법적 의무를 반영하기 위해 문서의 최신 상태를 유지합니다.

17. 결제 카드 산업

    결제 카드 산업(PCI) 프레임워크는 PCI DSS 에 부합하는 비즈니스 책임 및 보안 제어를 요약하여 PCI 준수를 달성하기 위한 HP 의 접근 방식을 안내합니다. HP 는 방화벽과 같은 네트워크 보안 제어를 설치하고 유지 및 관리함으로써 PCI 규정 준수 요구 사항을 충족합니다.

18. HP 제품 보안

    HP 제품 보안은 코드 서명, 제품 보안 취약점 관리, 보안 공지 발표 및 제품 보안 문제 보고 등 HP 제품 보안에 필수인 관행을 포괄합니다. 이러한 조치는 HP 제품이 사용자 안전성 및 신뢰성을 확보하는 데 도움이 됩니다. 제품 보안은 고객의 신뢰를 유지하고 잠재적 위협으로부터 고객을 보호하기 때문에 HP 에서 가장 중요합니다.

19. HP 서비스 보안

    HP 서비스 보안은 HP 고객에게 제공되는 서비스를 보호하기 위한 필수 관행을 포괄합니다. HP 서비스 보안 정책은 HP 인프라 호스팅, 타사 호스팅, 파트너 호스팅, 고객 호스팅 환경을 포함한 다양한 서비스 보안 영역을 다룹니다. 이러한 조치는 HP 서비스가 사용자에게 안전하고 신뢰할 수 있도록 보장합니다. HP 는 강력한 보안 관행을 구현함으로써 제품 및 서비스의 안전과 무결성을 보장하여 모든 사용자들에게 안전하고 신뢰할 수 있는 환경을 조성합니다.

마지막 업데이트: 2024 년 9 월