TÓM TẮT CÁC BIỆN PHÁP BẢO MẬT CỦA HP

Để bảo vệ dữ liệu Khách hàng, HP tuân thủ một bộ biện pháp kiểm soát bảo mật thông tin mạnh mẽ, bao gồm các chính sách, thực tiễn, quy trình và cấu trúc tổ chức để bảo vệ tính bảo mật, nguyên vẹn và sẵn có cho thông tin của HP và của khách hàng (bao gồm Dữ liệu cá nhân như được định nghĩa trong Phụ lục xử lý dữ liệu và khách hàng của HP). Các biện pháp bảo mật kỹ thuật/tổ chức của HP trên toàn công ty được trình bày dưới đây.

1. Chính sách bảo mật

   HP duy trì các chính sách, tiêu chuẩn và quy trình áp dụng trên toàn cầu nhằm bảo vệ dữ liệu của HP và Khách hàng. Thông tin chi tiết về chính sách bảo mật của HP được giữ bí mật để bảo vệ tính toàn vẹn của dữ liệu và hệ thống của HP. Tuy nhiên, phần dưới đây sẽ tóm tắt nội dung các chính sách quan trọng của chúng tôi.

2. Tổ chức bảo mật thông tin

   Chương trình Bảo mật thông tin của HP được thiết kế để chỉ đạo cũng như duy trì chiến lược và biện pháp kiểm soát bảo mật thông tin của tổ chức. Hệ thống này giúp đảm bảo toàn doanh nghiệp luôn tuân thủ các chính sách và biện pháp kiểm soát bảo mật của HP, cũng như tuân thủ các yêu cầu bảo mật của khách hàng. Khuôn khổ này được xây dựng phù hợp với các khuôn khổ, luật pháp và quy định về an ninh mạng theo tiêu chuẩn ngành, được xem xét hàng năm để thích ứng với các mối đe dọa ngày càng tinh vi nhắm vào HP.

3. Quản lý rủi ro an ninh mạng

   Chương trình quản lý rủi ro an ninh mạng của HP được thiết kế để bảo vệ tính bảo mật, toàn vẹn và sẵn có cho tài sản thông tin của HP. Chương trình này cung cấp cách tiếp cận phù hợp để xác định, đánh giá, ưu tiên, xử lý, khắc phục, theo dõi và báo cáo các rủi ro an ninh mạng. HP định nghĩa Khẩu vị rủi ro là mức độ tiếp xúc với rủi ro chấp nhận được và Mức chịu rủi ro là mức độ chênh lệch so với Khẩu vị này. Các rủi ro được đánh giá bằng phương pháp đã xác định, cho phép HP giảm thiểu rủi ro bảo mật thông tin xuống mức có thể chấp nhận được. Chương trình này phù hợp với quy trình Quản lý rủi ro doanh nghiệp của HP.

4. Bảo mật nhân sự

   Chính sách Bảo mật nhân sự của HP đảm bảo bảo mật thông tin trong suốt vòng đời nhân viên bằng cách thiết lập các quy trình để truy cập vào cơ sở, hệ thống thông tin và các tài sản khác. Điều này bao gồm việc lấy các xác nhận bằng văn bản thông qua thỏa thuận bảo mật và không tiết lộ thông tin, cũng như thực hiện các quy trình kiểm tra lý lịch. Tất cả các ứng viên xin việc tại HP phải hoàn thành quy trình kiểm tra xác minh lý lịch theo đúng luật pháp, quy định và đạo đức liên quan.

5. Quản lý tài sản

   HP có một quy trình để xác định tài sản thông tin kỹ thuật, phân loại tài sản quan trọng và duy trì các quy trình xử lý được ghi nhận cho từng phân loại thông tin, bao gồm cả những tài sản chứa Dữ liệu cá nhân. Những quy trình này bao gồm lưu trữ, truyền tải, giao tiếp, truy cập, ghi nhật ký, lưu giữ, phá hủy, thải bỏ, quản lý sự cố và thông báo vi phạm. Các chính sách và tiêu chuẩn bảo mật của HP cũng yêu cầu thải bỏ phương tiện truyền thông một cách an toàn.

6. Bảo mật dữ liệu

   Chương trình Bảo mật dữ liệu của HP đề ra các thực tiễn bảo mật và biện pháp kiểm soát kỹ thuật cần thực hiện để bảo vệ tính bảo mật, xác thực và nguyên vẹn của dữ liệu. Yêu cầu pháp lý, giá trị, tính quan trọng và độ nhạy cảm với việc tiết lộ hoặc sửa đổi trái phép là một số yếu tố quyết định cách thức phân loại thông tin theo chính sách Bảo mật dữ liệu của HP. Ngoài quy trình xử lý dữ liệu, chính sách còn nêu rõ vấn đề mã hóa, xóa, thu thập và xử lý, lưu giữ, sao lưu và phòng ngừa mất dữ liệu.

7. Kiểm soát truy cập

   HP áp dụng nguyên tắc đặc quyền tối thiểu cho việc kiểm soát truy cập theo logic, cung cấp cho người dùng quyền truy cập thông qua ID người dùng và mật khẩu không trùng lặp. Chính sách mật khẩu định nghĩa độ phức tạp, độ mạnh, thời hạn hiệu lực và kiểm soát lịch sử mật khẩu. Quyền truy cập được xem xét định kỳ và thu hồi khi nhân viên rời khỏi tổ chức. Các quy trình đã thỏa thuận cho việc tạo và xóa tài khoản người dùng được thực hiện để cấp và thu hồi quyền truy cập vào hệ thống khách hàng trong quá trình làm việc.

8. Mã hóa

   HP đã xác định một bộ quy trình mạnh mẽ về mã hóa để đảm bảo tính bảo mật, nguyên vẹn và có sẵn của tài sản thông tin. Các giao thức được phê duyệt yêu cầu mã hóa cho một số tài sản nhất định, bao gồm cả những tài sản chứa dữ liệu cá nhân. Chương trình Mã hóa của chúng tôi có sử dụng các kỹ thuật toán học để bảo mật thông tin và truyền thông, đảm bảo rằng chỉ những bên được ủy quyền mới có thể truy cập dữ liệu. Một thành phần tối quan trọng của chương trình bảo mật thông tin của HP là bảo vệ dữ liệu khỏi hành vi truy cập và can thiệp trái phép.

9. An ninh vật lý và môi trường

   Các cơ sở của HP được bảo vệ bằng nhiều biện pháp vật lý và điện tử để kiểm soát quyền ra vào, bao gồm bảo vệ an ninh, kiểm soát quyền ra vào bằng điện tử và hệ thống camera an ninh (CCTV). Các cơ sở cũng được trang bị hệ thống hỗ trợ cơ sở hạ tầng cần thiết, bao gồm kiểm soát nhiệt độ và nguồn dự phòng điện, sử dụng UPS và/hoặc máy phát điện diesel để hỗ trợ các dịch vụ tối quan trọng. Tất cả nhân viên của HP đều được đăng ký và bắt buộc phải đeo thẻ nhân viên phù hợp.

10. Quản lý vận hành

    HP đã thiết lập các yêu cầu tối thiểu về gia cố cho cơ sở hạ tầng công nghệ, bao gồm các máy trạm, máy chủ và thiết bị mạng. Những thiết bị này sử dụng hình ảnh hệ điều hành được gia cố trước, với các yêu cầu khác nhau theo hệ điều hành và các biện pháp kiểm soát được thực hiện. Ngoài ra, HP đã triển khai các Hệ thống phát hiện/ngăn chặn xâm nhập mạng (NIDS/NIPS) được giám sát và quản lý 24/7.

11. Bảo mật truyền thông

    Bảo mật truyền thông đảm bảo bảo vệ thông tin trong mạng lưới doanh nghiệp. Điều này bao gồm việc cài đặt và quản lý các thành phần bảo mật mạng (ví dụ: tường lửa), phân tách mạng, cũng như kiểm soát lọc web và xử lý email. Ngoài ra, bảo mật truyền thông còn liên quan đến việc giám sát và quản lý các kênh truyền thông để phát hiện và ngăn chặn hành vi truy cập trái phép hoặc xâm phạm dữ liệu.

12. Bảo mật hệ thống

    Chính sách của HP quy định một phương pháp phát triển an toàn cho các hệ thống và phần mềm trong suốt vòng đời của chúng. Vòng đời phát triển phần mềm bao gồm các giai đoạn: khởi tạo, phát triển/mua sắm, triển khai, vận hành và thải bỏ. Tất cả các thành phần hệ thống được đánh giá về tác động của chúng đối với bảo mật tổng thể. HP đã thiết lập các biện pháp kiểm soát cho các giao dịch dịch vụ ứng dụng, bao gồm xác thực thông tin đăng nhập của người dùng, chữ ký số, mã hóa, giao thức truyền thông an toàn và lưu trữ chi tiết giao dịch trong vùng bảo mật mạng phù hợp. Ngoài ra, HP còn thực hiện quét lỗ hổng nội bộ thường xuyên.

13. Bên thứ ba và nhà thầu phụ

    HP có quy trình lựa chọn nhà thầu phụ tuân thủ các yêu cầu bảo mật toàn diện dựa trên hợp đồng. Đối với các nhà cung cấp thuộc phạm vi, phụ trách xử lý dữ liệu của HP hoặc khách hàng, hoặc truy cập vào mạng lưới HP, bộ phận An ninh mạng HP sẽ tiến hành đánh giá rủi ro để xác minh một chương trình bảo mật thông tin với các biện pháp bảo vệ vật lý, kỹ thuật và quản trị. Đánh giá này là bắt buộc trước khi nhà cung cấp có thể truy cập thông tin của HP.

14. Quản lý sự cố bảo mật thông tin

    HP có một quy trình Quản lý sự cố an ninh mạng toàn diện, đề ra mục đích, phạm vi, vai trò, trách nhiệm, cam kết của ban lãnh đạo, cách phối hợp tổ chức, quy trình thực hiện và kiểm tra tuân thủ. Quy trình này được xem xét và cập nhật hàng năm. Đội phản ứng sự cố an ninh mạng, bao gồm nhân viên bộ phận An ninh mạng HP được đào tạo về phản ứng với sự cố và quản lý khủng hoảng, tiến hành đánh giá bàn tròn định kỳ về quy trình và bất kỳ sự cố hoặc sự kiện nào.

15. Quản lý khả năng liên tục hoạt động

    Chương trình Liên tục hoạt động toàn cầu của HP đảm bảo hoạt động liên tục từ đầu đến cuối thông qua các quy trình lập kế hoạch cộng tác, chuẩn hóa và được ghi nhận. Công ty định kỳ thực hiện các kế hoạch đảm bảo liên tục hoạt động để đảm bảo hiệu quả, kiểm tra và cập nhật tất cả các kế hoạch ít nhất hàng năm. Ngoài ra, tất cả nhân viên tham gia vào kế hoạch liên tục hoạt động đều được đào tạo bài bản.

16. Tuân thủ

    Chính sách Tuân thủ định hình cách tiếp cận của HP trong việc đáp ứng các kỳ vọng pháp lý, hợp đồng và nội bộ đối với một chương trình bảo mật thông tin hiệu quả. Các đánh giá bảo mật thông tin thường xuyên đảm bảo rằng các quy trình được tích hợp vào hoạt động của từng nhóm kinh doanh. Quá trình đánh giá cũng cập nhật các tài liệu để phản ánh các nghĩa vụ pháp lý hiện tại khi yêu cầu thay đổi.

17. Ngành thẻ thanh toán

    Khuôn khổ Ngành thanh toán thẻ (PCI) định hướng cách tiếp cận của HP để đạt được trạng thái Tuân thủ PCI, đề ra trách nhiệm kinh doanh và các biện pháp kiểm soát bảo mật phù hợp với PCI DSS. Bằng cách cài đặt và duy trì các biện pháp kiểm soát bảo mật mạng như tường lửa, HP đảm bảo đáp ứng các yêu cầu tuân thủ PCI.

18. Bảo mật sản phẩm HP

    Bảo mật sản phẩm HP bao gồm các thực tiễn thiết yếu để bảo vệ sản phẩm HP, như ký mã, quản lý lỗ hổng bảo mật sản phẩm, phát hành bản tin bảo mật và báo cáo vấn đề bảo mật sản phẩm. Những biện pháp này đảm bảo rằng sản phẩm HP vẫn an toàn và đáng tin cậy cho người dùng. Bảo mật sản phẩm là vô cùng quan trọng tại HP, vì nó giúp duy trì sự tin tưởng của khách hàng và bảo vệ chống lại các mối đe dọa tiềm năng.

19. Bảo mật dịch vụ HP

    Bảo mật dịch vụ HP bao gồm các biện pháp thiết yếu để bảo đảm an toàn cho các dịch vụ cung cấp cho khách hàng của HP. Chính sách này giải quyết các lĩnh vực khác nhau của bảo mật dịch vụ, bao gồm các môi trường được lưu trữ trên cơ sở hạ tầng của HP, được lưu trữ bởi bên thứ ba, được lưu trữ bởi đối tác và được lưu trữ bởi khách hàng. Những biện pháp này đảm bảo rằng dịch vụ HP luôn an toàn và đáng tin cậy cho người dùng. Bằng cách thực hiện các biện pháp bảo mật mạnh mẽ, HP đảm bảo sự an toàn và toàn vẹn của sản phẩm, dịch vụ của mình, tạo ra một môi trường an toàn và đáng tin cậy cho tất cả người dùng.