ملخص التدابير الأمنية في شركة HP

للحفاظ على سلامة بيانات العملاء، تعتمد HP على مجموعة فعالة من ضوابط أمن المعلومات، بما في ذلك السياسات والممارسات والإجراءات والهياكل التنظيمية، لحماية سرية معلوماتها الخاصة ومعلومات عملائها والحفاظ على سلامتها وتسهيل الوصول إليها (وهذا يشمل البيانات الشخصية بحسب تعريفها في ملحقات HP الخاصة بالعملاء ومعالجة البيانات). وفي ما يأتي لمحة عامة حول التدابير الأمنية الفنية/التنظيمية المعتمدة في كل أقسام شركة HP.

١. سياسة الأمن

تلتزم HP بسياسات ومعايير وإجراءات صالحة للتطبيق في كل أنحاء العالم تهدف إلى حماية بيانات HP وبيانات العملاء. وتتم حماية سرية تفاصيل سياسات الأمن في HP لضمان سلامة بيانات HP وأنظمتها. ومع ذلك، سنعرض أدناه ملخصات لأهم السياسات التي نعتمدها.

٢. وحدة أمن المعلومات

لدى HP وحدة أمن معلومات مسؤولة عن وضع إستراتيجيات أمن المعلومات وضوابطه في الشركة وتنفيذها. وتم وضع إطار عمل/نظام إدارة أمن المعلومات لضمان الالتزام بسياسات الأمن وضوابطه المعمول بها في HP والتحقق من الوفاء بمتطلبات الأمن الخاصة بعملائها. إطار العمل هذا يتماشى مع إطار المعهد الوطني الأمريكي (NIST) للأمن المعلوماتي ويخضع للمراجعة سنويًا.

٣. إدارة الأصول

تتبع HP عملية منظمة لتحديد الأصول المعلوماتية الفنية تساعد الشركة على تحديد كل الأصول الخاضعة لمسؤوليتها وتصنيفها بحسب أهميتها. كذلك، تتبع HP مجموعة من إجراءات المعالجة التي يتم توثيقها لكل فئة من المعلومات المصنفة، بما في ذلك الأصول التي تحتوي على بيانات شخصية. وتشمل إجراءات المعالجة تخزين البيانات، ونقلها، ومشاركتها، وحماية الوصول إليها، واستخدامها في عمليات التسجيل، وحفظها، وتدميرها، وحذفها، وإدارة حوادث انتهاكها، والإبلاغ عن اختراقها.

٤. ضبط عمليات الوصول إلى المعلومات

نتبع مبدأ الحد الأدنى من الامتيازات لمنح المستخدمين الامتيازات التي يحتاجون إليها فقط للوصول إلى المعلومات. ويمكن للمستخدمين الوصول إلى المعلومات من خلال معرف مستخدم فريد وكلمة مرور. تتضمن سياسة كلمات المرور في HP ضوابط تستلزم استخدام كلمات مرور معقدة وصالحة يصعب اختراقها وضوابط خاصة باستخدام كلمات المرور القديمة. تتم مراجعة حقوق الوصول إلى المعلومات دوريًا، وتُسحَب من المستخدمين عند تركهم العمل.

يتم تطبيق إجراءات إنشاء حسابات المستخدمين وحذفها المتفق عليها مع العملاء لمنح حقوق الوصول إلى أنظمة العملاء المستخدمة في أثناء تأدية المهمات وسحبها بعد ذلك.

٥. تدريب الموظفين

تشترط HP أن يكمل كل موظفيها تدريب "النزاهة في HP" الذي يهدف إلى تعريفهم بالبرامج والسياسات والموارد التي تحدد لهم معايير السلوك الأخلاقي والتميز والامتثال في HP. ويتضمن برنامج "النزاهة في HP" وحدات حول الأمن وخصوصية البيانات، كما يُطلب من الموظفين حضور دورة تدريبية سنوية لإنعاش ذاكرتهم والاطلاع على المستجدات. كذلك، تشترط HP أن يكمل موظفوها تدريبًا توعويًا متخصصًا في مجال الأمن يخضع للتحديث سنويًا يركز على السياسات الأمنية الأساسية ويسلط الضوء على مسؤوليات الموظفين المتعلقة بإدارة حوادث الانتهاك وخصوصية البيانات وأمن المعلومات.

٦. الجهات الخارجية والمتعاقدون الفرعيون

تتبع HP إجراءات فعالة لاختيار المتعاقدين الفرعيين الذين يمكنهم الوفاء بمتطلبات الأمن التعاقدية الشاملة.

ويجري قسم الأمن المعلوماتي في HP تقييمًا للمخاطر للتحقق من وجود برنامج أمن معلوماتي لدى الموردين المعنيين (الموردين الذين يعالجون بيانات HP وبيانات HP التي يتعامل معها العملاء أو يخزنونها أو ينقلونها أو لديهم وصول إلى شبكة HP). يجب أن يتضمن البرنامج الفعال تدابير حماية مادية وفنية وإدارية. ويجب إجراء هذا التقييم قبل وصول المُورّد إلى معلومات HP.

٧. أمن الأنظمة

تنص السياسة على أن تتبع HP منهجية تطوير آمنة لتطوير الأنظمة والبرامج الداعمة لها، وذلك لضمان الأمن في كل مراحل دورة تطوير الأنظمة/البرامج. تحدد دورة تطوير البرامج المتطلبات التي يجب الوفاء بها المتعلقة ببدء الاستخدام والتطوير/الإتاحة والتفعيل وعمليات التشغيل والتخلص. ويتم تقييم كل مكونات النظام، بما في ذلك الوحدات والمكتبات والخدمات والمكونات المنفصلة، لتحديد مدى تأثيرها في مستوى أمن النظام العام.

وضعت HP ضوابط لضمان سلامة المعاملات ذات الصلة بخدمات التطبيقات. وتشمل هذه الضوابط التحقق من صحة بيانات دخول المستخدمين ودقتها، وفرض استخدام التوقيعات الرقمية والرموز المشفرة، وتنفيذ بروتوكولات اتصال آمنة، وتخزين تفاصيل المعاملات عبر الإنترنت على الخوادم داخل المنطقة الأنسب لأمن الشبكة.

يتم إجراء عمليات تقييم الثغرات الأمنية الداخلية بشكل دوري.

٨. الأمن المادي والبيئي

يتم تأمين مرافق HP باستخدام مجموعة متنوعة من ضوابط الدخول المادية والإلكترونية وإمكانات المراقبة. وقد تشمل هذه الإجراءات، بحسب نوع المرفق، حراس أمن ووسائل تحكم إلكترونية في الدخول وأنظمة مراقبة بالفيديو (CCTV).

يتم تسجيل كل موظفي HP ويُلزَمون بحمل بطاقاتهم التعريفية السارية.

يلزم توفير دعم البنية التحتية للمرافق، بما في ذلك وسائل التحكم في درجة الحرارة ومصادر الطاقة الاحتياطية للاستخدام عند الحاجة، وذلك باستخدام مزودات الطاقة غير المنقطعة (UPS) و/أو مولدات الديزل لدعم الخدمات الحيوية.

٩. إدارة عمليات التشغيل

وضعت HP مجموعة من المتطلبات الأساسية لتقوية البنية التقنية، وهذا يشمل أجهزة العمل والخوادم والمعدات الشبكية. تضم نسخ أجهزة العمل والخوادم أنظمةَ تشغيل تمت تقوية بنيتها التقنية بالفعل. وتختلف متطلبات التقوية باختلاف نوع نظام التشغيل والضوابط المعتمدة.

ثبَّتت HP أنظمة كشف/منع الاختراقات الشبكية (NIDS/NIPS) في شبكتها وتتم مراقبتها وإدارتها على مدار الساعة.

تُلزم سياسات الأمن ومعاييره في HP بالتخلص الآمن من الوسائط.

١٠. التشفير

وضعت HP مجموعة من الإجراءات الفعالة الخاصة بالتشفير لضمان حماية سرية الأصول المعلوماتية والحفاظ على سلامتها وتسهيل الوصول إليها. ويُشترط تشفير بعض الأصول، بما في ذلك تلك التي تحتوي على بيانات شخصية، بموجب البروتوكولات المعتمدة.

١١. إدارة حوادث انتهاك أمن المعلومات

تتبع HP عملية إدارة حوادث انتهاك الأمن المعلوماتي التي تساعد على معالجة مجموعة من جوانب الإدارة، منها الغرض والنطاق والأدوار والمسؤوليات والالتزام الإداري والتنسيق التنظيمي وإجراءات التنفيذ والتحقق من الامتثال. وتقوم HP بمراجعة هذه العملية وتحديثها كل عام.

يعقد فريق الاستجابة لحوادث انتهاك الأمن المعلوماتي، الذي يضم موظفين من قسم الأمن المعلوماتي في HP مدرَّبين على الاستجابة لحوادث الانتهاك وإدارة الأزمات، اجتماعاتٍ دورية لمراجعة العملية ومدى فعاليتها في الأزمات وكذلك مدى الاستعداد لمواجهة أي حوادث أو وقائع.

١٢. إدارة استمرارية الأعمال

تلتزم شركة HP ببرنامج عام لضمان استمرارية الأعمال. يعتمد هذا البرنامج على نهج شامل يضم كل أقسام الشركة لضمان استمرارية الأعمال من بدايتها إلى نهايتها من خلال مجموعة من عمليات التخطيط التعاونية والموحدة والموثقة داخليًا.

تُقيِّم HP خطط استمرارية الأعمال بشكل دوري للتأكد من فعاليتها. وتحرص HP دائمًا على تقييم كل خطط استمرارية الأعمال وتحديثها على الأقل مرة واحدة في العام، كما تحرص على تدريب كل الموظفين الذين لديهم دور في تنفيذ هذه الخطط.

تاريخ المراجعة	وصف موجز للتغيير	الجهة المسؤولة عن المراجعة
مايو ٢٠١٨	النشر للمرة الأولى	Raella Dyke
فبراير ٢٠٢٢	التحديث	Grettel Acuña