



## ملخص التدابير الأمنية المتبعة لدى شركة HP

لحماية بيانات العملاء، تلتزم شركة HP بمجموعة قوية من ضوابط أمن المعلومات بما فيها السياسات والممارسات والإجراءات والهياكل التنظيمية لحماية سرية وسلامة وتوافر معلوماتها ومعلومات عملائها (بما في ذلك البيانات الشخصية كما هو محدد في ملحقات معالجة البيانات والعملاء الخاصة بشركة HP). ويقدم ما يلي نظرة عامة على التدابير الأمنية الفنية/التنظيمية التي تتخذها شركة HP في كل الشركة.

### 1. سياسة الأمان

تطبق شركة HP سياسات ومعايير وإجراءات قابلة للتطبيق عالمياً تهدف إلى حماية بيانات شركة HP والعملاء. وتعتبر تفاصيل سياسات الأمان الخاصة بشركة HP سرية لحماية سلامة بيانات شركة HP وأنظمتها. ومع ذلك، ندرج أدناه ملخصات لسياساتنا الرئيسية.

### 2. مؤسسة أمن المعلومات

تم تصميم برنامج أمن المعلومات الخاص بشركة HP لتوجيه وصيانة استراتيجيات وضوابط أمن المعلومات الخاصة بالمؤسسة. وضمن هذا النظام الامتثال على مستوى المؤسسة لسياسات وضوابط الأمن الخاصة بشركة HP. بالإضافة إلى الالتزام بمتطلبات الأمان الخاصة بعملائها. وتم تصميم الإطار بما يتماشى مع أطر وقوانين وأنظمة الأمن الإلكتروني القياسية في المجال، وتتم مراجعته سنوياً للتكيف مع مشهد التهديدات المتطور الذي تشهده شركة HP.

### 3. إدارة مخاطر الأمن الإلكتروني

تم تصميم برنامج إدارة مخاطر الأمن الإلكتروني الخاص بشركة HP للحفاظ على سرية أصول معلوماتها وسلامتها وتوافرها. ويوفر البرنامج نهجاً متسقاً لتحديد مخاطر الأمن الإلكتروني وتقييمها وإعطائها الأولوية والتعامل معها ومعالجتها وتتبعها والإبلاغ عنها. وتعرف شركة HP رغبتها في المخاطرة على أنها المستوى المقبول للتعرض للخسارة ومستوى تحمل المخاطر على أنه درجة التباين عن هذه الرغبة. ويتم تقييم المخاطر باستخدام منهجية محددة مما يمكن شركة HP من التخفيف من مخاطر أمن المعلومات إلى مستوى مقبول. يتوافق هذا البرنامج مع عملية إدارة المخاطر المؤسسية لدى شركة HP.

### 4. أمن الموارد البشرية (HR)

تضمن سياسة أمن الموارد البشرية في HP أمن المعلومات طوال دورة حياة الموظف من خلال إنشاء عمليات للوصول إلى المنشآت وأنظمة المعلومات والأصول الأخرى. ويتضمن هذا الحصول على إقرارات مكتوبة من خلال اتفاقيات السرية وعدم الإفصاح، فضلاً عن تنفيذ إجراءات الفحص الخلفية. يجب على جميع المرشحين للعمل لدى شركة HP إكمال فحص الخلفية وفقاً للقوانين واللوائح والأخلاقيات ذات الصلة.

### 5. إدارة الأصول

لدى شركة HP عملية لتحديد أصول المعلومات الفنية، وتصنيف الأصول بالغة الأهمية، والحفاظ على إجراءات التعامل الموثقة لكل نوع من أنواع تصنيف المعلومات، بما في ذلك تلك التي تحتوي على "بيانات شخصية". وتغطي هذه الإجراءات التخزين والنقل والانصالات والوصول والتسجيل والاحتفاظ والتدمير والتخلص وإدارة الحوادث والإخطار عن الخروقات. كما تتطلب سياسات ومعايير الأمان الخاصة بشركة HP التخلص الآمن من الوسائط.

## 6. أمن البيانات

يحدد برنامج أمن البيانات الخاص بشركة HP ممارسات الأمان والضوابط الفنية التي يجب تنفيذها لحماية سرية البيانات ومصداقيتها وسلامتها. إن المتطلبات القانونية والقيمة والأهمية والحساسية للإفصاح أو التعديل غير المصرح به تمثل بعض العوامل القليلة التي تحدد كيفية تصنيف المعلومات بموجب سياسة أمن البيانات الخاصة بشركة HP. بالإضافة إلى إجراءات معالجة البيانات، تحدد السياسة تشفير البيانات وحذفها وجمعها ومعالجتها والاحتفاظ بها والنسخ الاحتياطي لها ومنع فقدان البيانات.

## 7. التحكم في الوصول

تستخدم شركة HP مبدأ الحد الأدنى من الامتيازات للتحكم في الوصول المنطقي، مما يوفر وصول المستخدم من خلال معرّفات المستخدمين وكلمات المرور الفريدة. تحدد سياسة كلمة المرور عناصر التحكم في التعقيد والقوة والصلاحيّة وسجلات كلمات المرور. وتتم مراجعة حقوق الوصول بشكل دوري ويتم إلغاؤها عند مغادرة الموظفين. يتم تنفيذ الإجراءات المتفق عليها لإنشاء حسابات المستخدمين وحذفها لمنح وإلغاء الوصول إلى أنظمة العملاء أثناء المشاركات.

## 8. التشفير

لقد حددت شركة HP مجموعة من العمليات القوية للتشفير لضمان سرية أصول المعلومات وسلامتها وتوافرها. وتتطلب البروتوكولات المعتمدة تشفير بعض الأصول، بما في ذلك تلك التي تحتوي على بيانات شخصية. ويتضمن برنامج التشفير الخاص بنا استخدام تقنيات رياضية لتأمين المعلومات والاتصالات، مما يضمن إمكانية وصول الأطراف المصرح لها وحدها إلى البيانات. تُعد حماية البيانات من الوصول غير المصرح به والتلاعب بها أحد المكونات الأساسية لبرنامج أمن المعلومات الخاص بشركة HP.

## 9. الأمن المادي والبيئي

يتم تأمين منشآت HP باستخدام العديد من ضوابط الوصول المادية والإلكترونية، بما في ذلك حراس الأمن، والتحكم الإلكتروني في الوصول، والدائرة التلفزيونية المغلقة (CCTV). كما تم تجهيز المنشآت بدعم البنية التحتية اللازمة، بما في ذلك التحكم في درجة الحرارة واحتياطات الطاقة، باستخدام أجهزة UPS و/أو مولدات الديزل لدعم الخدمات الحيوية. يتم تسجيل جميع موظفي شركة HP ويجب عليهم حمل شارات التعريف المناسبة.

## 10. إدارة العمليات

وضعت شركة HP الحد الأدنى من متطلبات التعزيز للبنية التحتية للتكنولوجيا، بما في ذلك محطات العمل، والخوادم، ومعدات الشبكات. وتستخدم هذه الأجهزة صوراً مسبقة التجهيز لأنظمة التشغيل، مع متطلبات تختلف حسب نظام التشغيل والضوابط المطبقة. بالإضافة إلى ذلك، نشرت شركة HP أنظمة الكشف عن التطفل على الشبكة والوقاية منه (NIDS/NIPS) التي تتم مراقبتها وإدارتها على مدار الساعة وطوال أيام الأسبوع.

## 11. أمن الاتصالات

يضمن أمن الاتصالات حماية المعلومات داخل شبكات الشركات. ويتضمن هذا تثبيت مكونات أمن الشبكة وإدارتها (مثل جدران الحماية)، وفصل الشبكات، بالإضافة إلى عناصر التحكم في تصفية الويب ومعالجة الرسائل الإلكترونية. بالإضافة إلى ذلك، يتضمن هذا مراقبة قنوات الاتصال وإدارتها لاكتشاف الوصول غير المصرح به أو خروقات البيانات ومنعها.

## 12. أمن الأنظمة

تفرض سياسة شركة HP منهجية تطوير أمانة للأنظمة والبرامج طوال دورة حياتها. وتشمل دورة حياة تطوير البرامج البدء، والتطوير/الاستحواذ، والتنفيذ، والعمليات، والتخلص. يتم تقييم كل مكونات النظام لمعرفة تأثيرها على الأمن ككل. أنشأت شركة HP ضوابط لمعاملات خدمات التطبيقات، بما في ذلك التحقق من صحة بيانات اعتماد المستخدم، والتوافق الرقمي، والتشفير، وبروتوكولات الاتصال الآمنة، وتخزين تفاصيل المعاملات داخل منطقة أمن الشبكة المناسبة. كما يتم إجراء عمليات فحص داخلية منتظمة للثغرات.

### 13. الجهات الخارجية والمتعاقدون من الباطن

تضطلع شركة HP بعمليات لاختيار المتعاقدين من الباطن الذين يلتزمون بمتطلبات الأمن التعاقدية الشاملة. وبالنسبة للموردين المعنيين الذين يتعاملون مع بيانات شركة HP أو العملاء، أو يصلون إلى شبكة HP، يجري قسم الأمن الإلكتروني في شركة HP تقييمًا للمخاطر للتحقق من برنامج أمان المعلومات باستخدام الضمانات المادية والفنية والإدارية. هذا التقييم مطلوب قبل أن يتمكن المورد من الوصول إلى معلومات شركة HP.

### 14. إدارة حوادث أمن المعلومات

تتمتع شركة HP بعملية شاملة لإدارة الحوادث الإلكترونية تحدد الغرض والنطاق والأدوار والمسؤوليات والتزام الإدارة والتنسيق التنظيمي وإجراءات التنفيذ والتحقق من الامتثال. تتم مراجعة هذه العملية ويتم تحديثها سنويًا. يقوم فريق الاستجابة للحوادث الإلكترونية، بما في ذلك موظفو الأمن الإلكتروني في شركة HP المدربون على الاستجابة للحوادث وإدارة الأزمات، بإجراء مراجعات دورية على مستوى المكتب للعملية وأي حوادث أو أحداث.

### 15. إدارة استمرارية الأعمال

يضمن برنامج استمرارية العمليات العالمي من شركة HP الاستمرارية الشاملة من خلال عمليات التخطيط التعاونية والموحدة والموثقة. وتطبق الشركة خطط استمرارية الأعمال بشكل دوري لضمان فعاليتها. واختبار كل الخطط وتحديثها سنويًا على الأقل. بالإضافة إلى ذلك، يتلقى جميع الموظفين المشاركين في خطة استمرارية الأعمال التدريب المناسب.

### 16. الامتثال

يُشكّل الامتثال نهج شركة HP في تلبية التوقعات القانونية والتعاقدية والداخلية لبرنامج فعال لأمن المعلومات. وتضمن مراجعات أمن المعلومات المنتظمة دمج البروتوكولات في عمليات كل مجموعة أعمال. كما تعمل عملية المراجعة على تحديث المستندات لتعكس الالتزامات القانونية الحالية مع تطور المتطلبات.

### 17. مجال بطاقات الدفع

يرشد إطار عمل صناعة بطاقات الدفع (PCI) نهج شركة HP لتحقيق الامتثال لمعايير صناعة بطاقات الدفع، ويحدد مسؤوليات العمل وضوابط الأمن المتوافقة مع معيار أمن بيانات صناعة بطاقات الدفع (PCI DSS). من خلال تثبيت عناصر التحكم في أمن الشبكة، مثل جدران الحماية وصيانتها، تضمن شركة HP تلبية متطلبات الامتثال لصناعة بطاقات الدفع (PCI).

### 18. أمن منتجات HP

يشتمل أمن منتجات HP على الممارسات الأساسية لتأمين منتجات HP، مثل التوقيع بالتعليمات البرمجية، وإدارة ثغرات أمان المنتجات، وإصدار نشرات الأمان، والإبلاغ عن مشكلات أمن المنتجات. وتضمن هذه التدابير أن تظل منتجات HP آمنة وموثوقة للمستخدمين. يعد أمن المنتجات ذا أهمية قصوى لدى شركة HP، لأنه يساعد في الحفاظ على ثقة العملاء وحماية من التهديدات المحتملة.

### 19. أمن خدمات HP

يشتمل أمن خدمات HP على الممارسات الأساسية لتأمين الخدمات المقدمة لعملاء شركة HP. تعالج هذه السياسة مجالات مختلفة لأمن الخدمة، بما في ذلك البنية الأساسية المستضافة من HP، والبيئات المستضافة من قبل جهات خارجية، والمستضافة من قبل الشركاء، والمستضافة من قبل العملاء. وتضمن هذه التدابير أن تظل خدمات HP آمنة وموثوقة للمستخدمين. من خلال تنفيذ ممارسات أمنية قوية، تضمن شركة HP سلامة وأمن منتجاتها وخدماتها، مما يعزز بيئة آمنة وجديرة بالثقة لجميع المستخدمين.