RÉSUMÉ DES MESURES DE SÉCURITÉ HP

Pour protéger les données de ses clients, HP se conforme à un ensemble solide de contrôles de sécurité de l'information comprenant des politiques, des pratiques, des procédures et des structures organisationnelles pour sauvegarder la confidentialité, l'intégrité et la disponibilité de ses propres informations et de celles de ses clients (y compris les données personnelles telles qu'elles sont définies dans les addenda de HP relatifs aux clients et au traitement des données). Le texte qui suit présente une vue d'ensemble des mesures de sécurité techniques et organisationnelles prises par HP dans l'ensemble de l'entreprise.

1. Politique de sécurité

   HP maintient des politiques, des normes et des procédures applicables à l'échelle mondiale et destinées à protéger les données de HP et du Client. Le détail des politiques de sécurité de HP est confidentiel afin de protéger l'intégrité des données et des systèmes de HP. Toutefois, des résumés de nos principales politiques sont inclus ci-dessous.

2. Organisation de la sécurité de l'information

   Le programme de sécurité de l'information de HP est conçu pour diriger et maintenir la stratégie et les contrôles de sécurité de l'information de l'organisation. Ce système garantit la conformité à l'échelle de l'entreprise avec les politiques et les contrôles de sécurité de HP, ainsi que le respect des exigences de sécurité de ses clients. Structuré en fonction des cadres de cybersécurité, des lois et des réglementations en vigueur dans le secteur, le cadre est révisé chaque année pour s'adapter à l'évolution du paysage des menaces de HP.

3. Gestion du risque de cybersécurité

   Le programme de gestion des risques de cybersécurité de HP est conçu pour préserver la confidentialité, l'intégrité et la disponibilité de ses actifs informationnels. Le programme fournit une approche cohérente pour l'identification, l'évaluation, la hiérarchisation, le traitement, la correction, le suivi et la notification des risques de cybersécurité. HP définit son appétit pour le risque comme le niveau acceptable d'exposition aux pertes et sa tolérance au risque comme le degré d'écart par rapport à cet appétit. Les risques sont évalués à l'aide d'une méthodologie définie, ce qui permet à HP de réduire les risques liés à la sécurité de l'information à un niveau acceptable. Ce programme s'aligne sur le processus de gestion des risques de l'entreprise HP.

4. Sécurité RH

   La politique de sécurité des ressources humaines de HP garantit la sécurité des informations tout au long du cycle de vie des employés en établissant des processus d'accès aux installations, aux systèmes d'information et à d'autres actifs. Il s'agit notamment d'obtenir des reconnaissances écrites par le biais d'accords de confidentialité et de non-divulgation, ainsi que de mener des procédures de vérification des antécédents. Tous les candidats à un emploi chez HP doivent faire l'objet d'une vérification de leurs antécédents conformément aux lois, réglementations et règles de déontologie en vigueur.

5. Gestion des ressources

   HP dispose d'un processus d'identification des ressources techniques, de catégorisation des ressources critiques et de maintien de procédures de traitement documentées pour chaque type de classification des informations, y compris celles contenant des données à caractère personnel. Ces procédures couvrent le stockage, la transmission, la communication, l'accès, l'enregistrement, la conservation, la destruction, l'élimination, la gestion des incidents et la notification des violations. Les politiques et normes de sécurité de HP imposent également l'élimination sécurisée des supports.

6. Sécurité des données

   Le programme de sécurité des données de HP décrit les pratiques de sécurité et les contrôles techniques qui doivent être mis en œuvre pour protéger la confidentialité, l'authenticité et l'intégrité des données. Les exigences légales, la valeur, la criticité et la sensibilité à la divulgation ou à la modification non autorisée sont quelques-uns des facteurs qui déterminent la classification des informations dans le cadre de la politique de sécurité des données de HP. Outre les procédures de traitement des données, la politique décrit le chiffrement, la suppression, la collecte et le traitement des données, la conservation, la sauvegarde et la prévention des pertes de données.

7. Contrôle d'accès

   HP utilise le principe du moindre privilège pour le contrôle de l'accès logique, en fournissant un accès aux utilisateurs par le biais d'identifiants et de mots de passe uniques. La politique en matière de mots de passe définit la complexité, la force, la validité et les contrôles de l'historique des mots de passe. Les droits d'accès sont périodiquement réexaminés et révoqués en cas de départ du personnel. Des procédures convenues pour la création et la suppression de comptes d'utilisateurs sont mises en œuvre pour accorder et révoquer l'accès aux systèmes des clients pendant les missions.

8. Cryptographie

   HP a défini un ensemble de processus robustes pour la cryptographie afin de garantir la confidentialité, l'intégrité et la disponibilité des informations. Les protocoles approuvés exigent le chiffrement de certains actifs, y compris ceux qui contiennent des données à caractère personnel. Notre programme de cryptographie implique l'utilisation de techniques mathématiques pour sécuriser les informations et les communications, en veillant à ce que seules les parties autorisées puissent accéder aux données. Un élément essentiel du programme de sécurité de l'information de HP est la protection des données contre l'accès non autorisé et la falsification.

9. Sécurité physique et environnementale

   Les installations de HP sont sécurisées par divers contrôles d'accès physiques et électroniques, notamment par des agents de sécurité, un contrôle d'accès électronique et la télévision en circuit fermé (vidéosurveillance). Les installations sont également équipées de l'infrastructure nécessaire, y compris le contrôle de la température et les sauvegardes électriques, en utilisant des onduleurs et/ou des générateurs diesel pour soutenir les services critiques. Tout le personnel de HP est enregistré et doit porter des badges d'identification appropriés.

10. Gestion des opérations

    HP a établi des exigences minimales de renforcement pour l'infrastructure technologique, y compris les postes de travail, les serveurs et l'équipement de réseau. Ces dispositifs utilisent des images de système d'exploitation pré-endurcies, les exigences variant selon le système d'exploitation et les contrôles mis en œuvre. En outre, HP a déployé des systèmes de détection et de prévention des intrusions dans le réseau (NIDS/NIPS) qui sont surveillés et gérés 24 heures sur 24 et 7 jours sur 7.

11. Sécurité des communications

    La sécurité des communications assure la protection des informations au sein des réseaux d'entreprise. Cela comprend l'installation et la gestion des composants de sécurité du réseau (par exemple, les pare-feu), la séparation des réseaux, ainsi que le filtrage du web et les contrôles du traitement du courrier électronique. En outre, il s'agit de surveiller et de gérer les canaux de communication afin de détecter et de prévenir les accès non autorisés ou les violations de données.

12. Sécurité des systèmes

    La politique de HP impose une méthodologie de développement sécurisée pour les systèmes et les logiciels tout au long de leur cycle de vie. Le cycle de vie du développement de logiciels couvre l'initiation, le développement/l'acquisition, la mise en œuvre, les opérations et l'élimination. Tous les composants du système sont évalués en fonction de leur impact sur la sécurité globale. HP a mis en place des contrôles pour les transactions des services d'application, notamment la validation des informations d'identification de l'utilisateur, les signatures numériques, le cryptage, les protocoles de communication sécurisés et le stockage des détails de la transaction dans la zone de sécurité appropriée du réseau. Des analyses internes régulières des vulnérabilités sont également effectuées.

13. Tiers et sous-traitants

    HP a mis en place des processus de sélection des sous-traitants qui respectent des exigences contractuelles complètes en matière de sécurité. Pour les fournisseurs concernés qui traitent les données de HP ou de ses clients, ou qui accèdent au réseau HP, le service de cybersécurité de HP procède à une évaluation des risques afin de vérifier l'existence d'un programme de sécurité de l'information assorti de mesures de protection physiques, techniques et administratives. Cette évaluation est requise avant que le fournisseur ne puisse accéder aux informations sur le HP.

14. Gestion des incidents liés à la sécurité de l'information

    HP dispose d'un processus complet de gestion des cyber-incidents qui décrit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination organisationnelle, les procédures de mise en œuvre et la vérification de la conformité. Ce processus est revu et mis à jour chaque année. L'équipe de réponse aux cyber-incidents, qui comprend du personnel du service de cybersécurité de HP formé à la réponse aux incidents et à la gestion de crise, procède régulièrement à des examens sur table du processus et de tout incident ou événement.

15. Gestion de la continuité des activités

    Le programme mondial de continuité des opérations de HP assure une continuité de bout en bout grâce à des processus de planification collaboratifs, normalisés et documentés. L'entreprise met périodiquement à l'épreuve ses plans de continuité des activités afin d'en garantir l'efficacité, en testant et en mettant à jour tous les plans au moins une fois par an. En outre, tout le personnel impliqué dans le plan de continuité des activités reçoit une formation adéquate.

16. Conformité

    La conformité définit l'approche de HP pour répondre aux attentes légales, contractuelles et internes d'un programme efficace de sécurité de l'information. Des examens réguliers de la sécurité de l'information permettent de s'assurer que les protocoles sont intégrés dans les activités de chaque groupe d'entreprises. Le processus de révision permet également de mettre à jour les documents afin qu'ils reflètent les obligations légales en vigueur au fur et à mesure de l'évolution des besoins.

17. Industrie des cartes de paiement

    Le cadre PCI (Payment Card Industry pour « Industrie des cartes de paiement ») guide l'approche de HP pour atteindre la conformité PCI, en soulignant les responsabilités de l'entreprise et les contrôles de sécurité alignés sur la norme PCI DSS. En installant et en maintenant des contrôles de sécurité du réseau tels que des pare-feu, HP s'assure de répondre aux exigences de conformité PCI.

18. Sécurité des produits HP

    La sécurité des produits HP englobe les pratiques essentielles pour sécuriser les produits HP, telles que la signature du code, la gestion des vulnérabilités de sécurité des produits, la publication de bulletins de sécurité et le signalement des problèmes de sécurité des produits. Ces mesures garantissent que les produits HP restent sûrs et fiables pour les utilisateurs. La sécurité des produits est d'une importance capitale chez HP, car elle permet de maintenir la confiance des clients et de les protéger contre les menaces potentielles.

19. Sécurité des services HP

    La sécurité des services HP englobe les pratiques essentielles pour sécuriser les services fournis aux clients HP. Cette politique aborde différents domaines de la sécurité des services, y compris les environnements hébergés par l'infrastructure HP, hébergés par des tiers, hébergés par des partenaires et hébergés par des clients. Ces mesures garantissent que les services HP restent sûrs et fiables pour les utilisateurs. En mettant en œuvre des pratiques de sécurité robustes, HP garantit la sécurité et l'intégrité de ses produits et services, favorisant ainsi un environnement sûr et fiable pour tous les utilisateurs.