RÉSUMÉ DES MESURES DE SÉCURITÉ DE HP

Afin de protéger les données des clients, HP met en œuvre un ensemble robuste de contrôles de sécurité de l'information, y compris des politiques, des pratiques, des procédures et des structures organisationnelles ayant pour objectif de protéger la confidentialité, l'intégrité et la disponibilité de ses propres informations ainsi que celles de ses clients (y compris les renseignements personnels tels que définis dans les Appendices relatifs au traitement des données des clients de HP). Ce document présente un récapitulatif des mesures de sécurité techniques et organisationnelles de HP au sein de la société.

1. Politique de sécurité

   HP tient à jour des politiques, des normes et des procédures applicables à l'échelle mondiale visant à protéger ses propres données ainsi que les données de ses clients. Les détails des politiques de sécurité de HP sont confidentiels pour garantir l'intégrité des systèmes et des données de HP. Cependant, les résumés de nos principales politiques sont fournis ci-dessous.

2. Structure organisationnelle de la sécurité de l'information

   Le programme de sécurité de l'information de HP est conçu pour piloter et soutenir la mise en œuvre de la stratégie et des contrôles de sécurité de l'information au sein de l'organisation. Ce système garantit la conformité, à l'échelle de la société, avec les politiques et les contrôles de sécurité de HP, ainsi que le respect des exigences de sécurité de ses clients. Aligné sur les cadres de cybersécurité, les lois et les réglementations qui définissent la norme de l'industrie, le cadre est revu annuellement pour qu'il reflète l'évolution des menaces auxquelles HP fait face.

3. Gestion des risques en matière de cybersécurité

   Le programme de gestion des risques en matière de cybersécurité de HP a pour objectif de protéger la confidentialité, l'intégrité et la disponibilité de ses actifs informationnels. Le programme propose une approche systématique pour cerner, évaluer, prioriser, traiter, éliminer, suivre et rapporter les risques en matière de cybersécurité. HP définit son « appétit pour le risque » comme le niveau d'exposition à la perte jugé acceptable, tandis que la « tolérance au risque » représente le degré de variance par rapport à cet appétit. Les risques sont évalués selon une méthodologie précise, ce qui permet à HP d'atténuer les risques en matière de sécurité de l'information jusqu'à un niveau acceptable. Ce programme est aligné sur le processus de gestion des risques d'entreprise de HP.

4. Sécurité des RH

   La politique de sécurité des ressources humaines de HP garantit la sécurité de l'information tout au long du cycle de vie des employés en mettant en place des processus d'accès aux installations, aux systèmes d'information et à d'autres actifs. Cela comprend la collecte d'accusés de réception écrits au moyen d'ententes de confidentialité et de non-divulgation, ainsi que la mise en œuvre de procédures de vérification des antécédents. Tous les candidats à un emploi chez HP doivent se soumettre à une vérification des antécédents conformément aux lois, règlements et normes éthiques en vigueur.

5. Gestion des actifs

   HP a mis en place un processus pour déterminer quels sont les actifs d'information technique, classer les actifs essentiels et tenir à jour des procédures de gestion documentées pour chaque type de classification de l'information, y compris ceux contenant des Renseignements personnels. Ces procédures englobent le stockage, la transmission, la communication, l'accès, la consignation, la conservation, la destruction, l'élimination, la gestion des incidents et la notification en cas d'atteinte à la vie privée. Les politiques et normes de sécurité de HP exigent également une élimination sécurisée des supports.

6. Sécurité des données

   Le programme de sécurité des données de HP donne un aperçu des pratiques de sécurité et des contrôles techniques qui doivent être mis en œuvre pour protéger la confidentialité, l'authenticité et l'intégrité des données. Les critères de classification de l'information dans le cadre de la politique de sécurité des données de HP incluent, parmi d'autres facteurs, les exigences légales, la valeur, la criticité et la sensibilité à la divulgation ou à la modification non autorisée. En plus des procédures de traitement des données, la politique précise les aspects relatifs au chiffrement des données, à leur suppression, à leurs collecte et traitement, à leur conservation, à leur sauvegarde, ainsi qu'à la prévention de la perte de données.

7. Contrôle de l'accès

   HP utilise le principe de moindre privilège pour contrôler l'accès logique, permettant aux utilisateurs d'accéder au système au moyen de noms de connexion et de mots de passe uniques. La politique relative aux mots de passe définit la complexité, la robustesse, la validité et les contrôles de l'historique des mots de passe. Les droits d'accès font l'objet d'une révision régulière et sont révoqués lors du départ d'un employé. Des procédures convenues pour la création et la suppression des comptes utilisateurs sont mises en œuvre pour accorder et révoquer l'accès aux systèmes des clients au cours des interventions.

8. Cryptographie

   HP a établi un ensemble de procédures solides en matière de cryptographie pour garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels. Les protocoles approuvés exigent le chiffrement de certains actifs, y compris ceux qui contiennent des renseignements personnels. Notre programme de cryptographie utilise des techniques mathématiques pour sécuriser les informations et les communications, garantissant que seules les parties autorisées peuvent accéder aux données. Une composante clé du programme de sécurité de l'information de HP est axée sur la protection des données contre l'accès non autorisé et l'altération.

9. Sécurité physique et environnementale

   Les installations de HP sont protégées par plusieurs systèmes de contrôle d'accès, tant physiques qu'électroniques, tels que des agents de sécurité, un contrôle d'accès électronique et la surveillance par télévision (CCTV). Les installations disposent également du soutien d'infrastructure nécessaire, comprenant le contrôle de la température et des systèmes d'alimentation électrique d'urgence, utilisant des systèmes d'alimentation sans coupure ou des groupes électrogènes diesel, et ce, pour garantir des services essentiels. Tous les membres du personnel de HP sont enregistrés et doivent posséder des insignes d'identité appropriées.

10. Gestion des opérations

    HP a mis en place des exigences minimales en matière de sécurisation renforcée de l'infrastructure technologique, y compris pour les postes de travail, les serveurs et l'équipement réseau. Ces dispositifs emploient des images de systèmes d'exploitation ayant subi une sécurisation renforcée, avec des exigences qui varient selon le système d'exploitation et les contrôles mis en place. De plus, HP a déployé des systèmes de détection et de prévention d'intrusion dans le réseau qui sont surveillés et gérés en permanence.

11. Sécurité des communications

    La sécurité des communications garantit la protection des informations au sein des réseaux d'entreprise. Cela comprend l'installation et la gestion des composants de sécurité réseau (par exemple, des pare-feu), la séparation des réseaux, ainsi que le filtrage Web et les contrôles de gestion des courriels. De plus, cela implique la surveillance et la gestion des canaux de communication pour détecter et empêcher tout accès non autorisé ou toute atteinte à la protection des données.

12. Sécurité des systèmes

    La politique de HP impose une méthodologie d'élaboration sécurisée pour les systèmes et les logiciels tout au long de leur cycle de conception. Le cycle de conception des logiciels comprend l'initiation, l'élaboration et l'acquisition, la mise en œuvre, les opérations et l'élimination. Tous les composants des systèmes sont évalués pour déterminer leur effet sur la sécurité globale. HP a mis en place des mesures de contrôle pour les transactions de services applicatifs, telles que la validation des éléments d'identification de l'utilisateur, les signatures numériques, le chiffrement, les protocoles de communication sécurisés, ainsi que le stockage des détails liés aux transactions dans la zone de sécurité de réseau appropriée. Des évaluations internes en matière de vulnérabilité sont également menées régulièrement.

13. Tiers et sous-traitants

    HP dispose de processus pour sélectionner des sous-traitants qui respectent des exigences contractuelles détaillées en matière de sécurité. Pour les fournisseurs concernés qui traitent des données de HP ou de ses clients, ou qui accèdent au réseau de HP, le service de cybersécurité de HP mène une évaluation des risques pour vérifier si les fournisseurs disposent d'un programme de sécurité de l'information qui intègre des mesures de protection physiques, techniques et administratives. Cette évaluation est nécessaire avant que le fournisseur puisse accéder aux données de HP.

14. Gestion des incidents de sécurité de l'information

    HP dispose d'un processus complet de gestion des incidents de cybersécurité qui décrit brièvement l'objectif, la portée, les rôles, les responsabilités, l'engagement pris par les gestionnaires, la coordination organisationnelle, les procédures d'exécution et le contrôle de conformité. Ce processus est révisé et actualisé une fois par an. L'équipe de réponse aux incidents de cybersécurité, qui inclut des membres du personnel de cybersécurité de HP formés à la réponse aux incidents et à la gestion des crises, effectue régulièrement des examens sur table des processus et des incidents ou événements.

15. Gestion de la continuité des activités

    Le programme mondial de continuité des activités de HP veille à la continuité de l'ensemble des opérations grâce à des processus de planification collaboratifs, normalisés et documentés. La société met périodiquement en pratique ses plans de continuité des activités pour garantir leur efficacité, en testant et en mettant à jour tous les plans au moins une fois par an. En outre, tous les membres du personnel participant au plan de continuité des activités reçoivent une formation appropriée.

16. Conformité

    La conformité détermine la façon dont HP aborde le respect des exigences légales, contractuelles et internes pour un programme de sécurité de l'information efficace. Des examens réguliers de la sécurité de l'information garantissent que les protocoles sont intégrés dans les activités de chaque groupe d'entreprise. Ces examens garantissent également que les documents sont mis à jour pour refléter les obligations légales actuelles au fur et à mesure que les exigences évoluent.

17. Secteur des cartes de paiement

    Le cadre du Secteur des cartes de paiement (SCP) guide l'approche de HP pour atteindre la conformité SCP, en décrivant brièvement les responsabilités commerciales et les contrôles de sécurité conformes à la norme de sécurité des données du secteur des cartes de paiement (PCI DSS). En mettant en place et en maintenant des contrôles de sécurité réseau tels que des pare-feu, HP garantit qu'il répond aux exigences de conformité PCI.

18. Sécurité des produits HP

    La sécurité des produits HP englobe des pratiques essentielles pour protéger la sécurité des produits HP, telles que la signature numérique, la gestion des vulnérabilités en matière de sécurité des produits, la publication de bulletins de sécurité et le signalement des problèmes de sécurité des produits. Ces mesures garantissent la sécurité et la fiabilité des produits HP pour les utilisateurs. La sécurité des produits revêt une importance primordiale chez HP, car elle contribue à maintenir la confiance des clients et à se protéger contre les menaces.

19. Sécurité des services HP

    La sécurité des services HP englobe des pratiques essentielles pour garantir la sécurité des services proposés aux clients de HP. Cette politique couvre plusieurs aspects de la sécurité des services, y compris les infrastructures hébergées par HP, par des tiers, par des partenaires et les environnements hébergés par des clients. Ces mesures garantissent la sécurité et la fiabilité des services HP pour les utilisateurs. En mettant en œuvre des pratiques de sécurité robustes, HP assure la sécurité et l'intégrité de ses produits et services, créant ainsi un environnement sûr et fiable pour tous les utilisateurs.