RÉSUMÉ DES MESURES DE SÉCURITÉ
DE HP

Pour protéger les données de ses Clients, HP se conforme à un ensemble solide de contrôles de sécurité de l'information, y compris des politiques, des pratiques, des procédures et des structures organisationnelles visant à préserver la confidentialité, l'intégrité et la disponibilité de ses propres informations et de celles de ses clients (y compris les Données Personnelles telles que définies dans les addenda de HP relatifs aux Clients et au Traitement des Données). Les paragraphes suivants présentent une vue d'ensemble des mesures de sécurité techniques et organisationnelles prises par HP à l'échelle de la société.

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 des Clients. 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

HP dispose d'une Organisation de Sécurité de l'Information chargée de diriger et de gérer les contrôles et la stratégie de sécurité de l'information de l'entreprise. Un Cadre/Système de Gestion de la Sécurité de l'Information est mis en place pour garantir la conformité avec les contrôles et les politiques de sécurité de HP et confirmer que les exigences de sécurité de ses clients sont respectées. Ce Cadre est structuré conformément au NIST Cybersecurity Framework et fait l'objet d'une révision annuelle.

3. Gestion des actifs

HP a instauré un processus d'identification des actifs d'information technique qui lui permet de déterminer tous les actifs sous sa responsabilité et de classer par catégories les actifs critiques. HP dispose en outre d'un ensemble de procédures de traitement documentées pour chaque type de classification de l'information, y compris les actifs contenant des Données Personnelles. Les procédures de traitement 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.

4. Contrôle d'accès

Le principe de moindre privilège est utilisé pour fournir un contrôle d'accès logique. L'accès des utilisateurs se fait par le biais d'un identifiant et d'un mot de passe uniques. La politique de HP en matière de mots de passe a défini des contrôles liés à la complexité, à la force, à la validité et à l'historique des mots de passe. Les droits d'accès sont réexaminés périodiquement et révoqués en cas de départ du membre du personnel.

Des procédures de création et de suppression de comptes d'utilisateurs, convenues d'un commun accord, sont mises en œuvre pour accorder et révoquer l'accès aux systèmes du client utilisés au cours de la mission.

5. Formation du personnel

Les employés de HP doivent suivre la formation Integrity at HP afin de s'assurer qu'ils connaissent le programme, les politiques et les ressources qui régissent les attentes de HP en matière de comportement éthique, d'excellence et de conformité. Le programme Integrity at HP comprend des modules sur la sécurité et la confidentialité des données, et les employés sont également tenus de suivre un cours de « recyclage » annuel. Les employés de HP doivent également suivre une formation de sensibilisation à la sécurité actualisée chaque année, axée sur les politiques de sécurité essentielles et mettant l'accent sur les responsabilités des employés en matière de gestion des incidents, de confidentialité des données et de sécurité de l'information.

6. Tiers et sous-traitants

HP a mis en place des processus permettant de sélectionner des sous-traitants capables de se conformer à des exigences contractuelles complètes en matière de sécurité.

Pour les fournisseurs concernés (fournisseurs qui traitent, stockent ou transmettent des données HP et des données du client détenues par HP ou qui ont accès au réseau HP), HP Cybersecurity procède à une évaluation des risques afin de vérifier l'existence d'un programme de sécurité de l'information. Un programme adéquat doit comprendre des protections physiques, techniques et administratives. Cette évaluation doit être effectuée avant que le fournisseur n'ait accès aux informations de HP.

7. Sécurité des systèmes

Par principe, le développement de systèmes et de logiciels de soutien au sein de HP suit une méthodologie de développement sécurisée visant à garantir la sécurité tout au long du cycle de vie du système/logiciel. Le cycle de vie du développement logiciel définit les exigences en matière de lancement, de développement/acquisition, de mise en œuvre, d'exploitation et d'élimination. Tous les composants du système, y compris les modules, les bibliothèques, les services et les composants discrets, sont évalués afin de déterminer leur impact sur l'état de sécurité global du système.

HP a défini des contrôles pour la protection des transactions des services d'application. Ces contrôles comprennent la validation et la vérification des informations d'identification des utilisateurs, l'obligation d'utiliser des signatures numériques et le chiffrement, la mise en œuvre de protocoles de communication sécurisés, le stockage des détails des transactions en ligne sur des serveurs situés dans la zone de sécurité appropriée du réseau.

Des analyses de vulnérabilité internes sont effectuées régulièrement.

8. Sécurité physique et environnementale

Les installations de HP sont sécurisées au moyen de divers contrôles d'accès physiques et électroniques et de capacités de surveillance. Selon l'établissement, il peut s'agir d'agents de sécurité, de contrôle d'accès électronique et de télévision en circuit fermé (CCTV).

L'ensemble du personnel de HP est enregistré et doit porter un badge d'identification approprié.

Les installations disposent de l'infrastructure de soutien requise avec un contrôle de la température et un système d'alimentation de secours, le cas échéant, au moyen d'onduleurs et/ou de générateurs diesel pour soutenir les services critiques.

9. Gestion des opérations

HP a défini un ensemble minimum d'exigences de renforcement de la sécurité pour l'infrastructure technologique, y compris les stations de travail, les serveurs et les équipements de réseau. Les images des stations de travail/serveurs contiennent des systèmes d'exploitation à sécurité renforcée en amont. Les exigences en matière de renforcement de la sécurité varient en fonction du type de système d'exploitation et des contrôles applicables mis en œuvre.

HP a déployé des Systèmes de Détection et de Prévention d'Intrusions sur Réseau (NIDS/NIPS) qui sont surveillés et gérés 24 heures sur 24 et 7 jours sur 7.

Les politiques et normes de sécurité de HP imposent une élimination sécurisée des supports.

10. Cryptographie

HP a défini un ensemble de processus robustes pour la cryptographie afin de garantir la confidentialité, l'intégrité et la disponibilité des informations détenues. Les protocoles approuvés exigent le chiffrement de certains actifs, y compris ceux qui contiennent des données personnelles.

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

HP suit un Processus de Gestion des Incidents Cybernétiques qui couvre 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. HP revoit et met à jour ce processus chaque année.

Une Équipe de Réponse aux Incidents Cybernétiques, composée de membres du personnel de HP Cybersecurity formés à la réponse aux incidents et à la gestion de crise, est constituée pour examiner régulièrement sur table les processus et tout incident ou événement.

12. Gestion de la continuité des activités

HP a mis en place un programme mondial de Continuité des Activités. Ce programme adopte une approche globale, à l'échelle de la société, de la continuité de bout en bout, grâce à un ensemble de processus de planification collaboratifs, normalisés et documentés en interne.

HP met périodiquement à l'épreuve ses plans de continuité des activités afin de s'assurer de leur efficacité. HP teste et met à jour tous les plans au moins une fois par an et veille à ce que les personnes jouant un rôle dans le plan de continuité des activités soient formées.

Date de révision	Brève description de la modification	Interlocuteur de l'autorité de révision
Mai 2018	Première publication	Raella Dyke
Février 2022	Actualisation	Grettel Acuña