DELL Technologies

Addendum relatif aux mesures de sécurité des informations d'APEX

Les Services APEX utilisent un modèle de responsabilité de sécurité partagée dans lequel vous et Dell avez chacun certaines responsabilités, car ces services sont hébergés dans Vos locaux ou sur un Site en colocation et n'impliquent généralement pas l'hébergement du Contenu client sur des serveurs dans des centres de données gérés par Dell. Vos responsabilités sont précisées dans la Description de l'offre de service applicable.

Dell a mis en place et appliquera les mesures de sécurité internes suivantes pour les Services APEX. Ces mesures, ainsi que les mesures de sécurité énoncées dans la Description d'offre de service correspondante, constituent la seule responsabilité de Dell en ce qui concerne la sécurité des Services APEX. Sauf indication contraire dans le présent document, tous les termes commençant par une majuscule qu'il contient auront le sens qui leur est attribué dans le Contrat APEX.

Fonction	Mesures
Programme de sécurité des informations	Dell a mis en place et appliquera un programme de sécurité des informations (incluant l'adoption de politiques et de normes internes) qui est conçu pour : (a) identifier les risques en matière de sécurité raisonnablement prévisibles pour les parties, le cas échéant, des centres de données, serveurs, équipements de gestion de réseau, pare-feu et systèmes logiciels hôtes de l'entreprise Dell qui sont utilisés pour fournir les services APEX (« **Réseau Dell** »), et (b) déployer des efforts commercialement raisonnables pour atténuer les risques en matière de sécurité identifiés pour le Réseau Dell, selon les modalités que Dell juge appropriées, notamment par des évaluations et des tests des risques réguliers. Dell a désigné un ou plusieurs agents de sécurité chargés de coordonner, de surveiller et d'appliquer le programme de sécurité des informations. Dell appliquera un programme de gestion des menaces et des failles de sécurité qui détecte les failles de sécurité dans le Réseau Dell de façon continue. Les failles de sécurité sont identifiées à l'aide de plusieurs sources ou méthodes qui peuvent inclure des fournisseurs, des chercheurs en sécurité, des analyses des failles de sécurité, des activités d'équipe rouge, des tests d'intrusion et des signalements de collaborateurs. Les failles de sécurité tierces qui sont rendues publiques sont passées en revue afin de vérifier leur pertinence dans l'environnement Dell. Les analyses et évaluations des failles de sécurité sont effectuées de manière régulière et automatique sur l'infrastructure de l'application Dell. Ces processus sont conçus pour permettre d'identifier et de résoudre les failles de sécurité de manière proactive, mais aussi pour aider Dell à respecter ses exigences réglementaires et de conformité.
Cycle de vie du développement sécurisé et réponse aux failles de sécurité	Dell a mis en place et applique un programme de cycle de vie de développement sécurisé qui définit les étapes à suivre pour s'assurer que ses offres ont été dûment évaluées, développées et conditionnées dans le cadre d'un programme de gouvernance officiel avec un cycle de vie de développement sécurisé défini. Ce programme, complété par le programme de sécurité des informations de Dell, permet de résoudre les problèmes de sécurité tout au long du cycle de vie de développement et de maintenance du Système APEX. Dell utilise un processus rigoureux pour évaluer et améliorer continuellement ses pratiques de développement sécurisé et de résolution des

	failles de sécurité. Dell compare également de façon régulière ces pratiques avec les pratiques normalisées de l'industrie. Après avoir enquêté sur une vulnérabilité signalée dans le Système APEX et après l'avoir validée, Dell tentera d'identifier, de développer et de qualifier une solution appropriée conformément à la politique de réponse aux failles de sécurité publiée par Dell, actuellement consultable à l'adresse https://www.dell.com/support/contents/article/product-support/self-support-knowledgebase/security-antivirus/alerts-vulnerabilities/dell-vulnerability-response-policy. Dell communique des mesures correctives à ses clients par le biais d'avis de sécurité, le cas échéant. Dell s'efforce de fournir des mesures correctives dans un délai commercialement raisonnable, le cas échéant. Les délais de réponse dépendent de nombreux facteurs, tels que la gravité, la complexité de la solution ou le composant affecté.
Gestion du parc informatique	Dell suit et gère les ressources physiques et logiques du Réseau Dell. Les actifs que Dell peut suivre, et les contrôles qu'elle peut mettre en œuvre, incluent par exemple : (a) les ressources logicielles, comme les applications et les logiciels système ; (b) les ressources physiques, comme les serveurs, les ordinateurs de bureau ou portables, les bandes de sauvegarde ou d'archives, les imprimantes et les équipements de communication ; et (c) les ressources d'information, comme les bases de données, les plans de reprise après sinistre, les plans de continuité d'activité, la classification des données et les informations archivées. Dell classifie les actifs en fonction de leur degré d'importance pour l'entreprise et/ou de la sensibilité de classification des données. Une telle classification permet de restreindre de manière appropriée l'accès à l'actif en question.
Sécurité des ressources humaines	Dans le cadre du processus de recrutement, les employés Dell doivent signer un accord de confidentialité lors de l'embauche et passer par un processus d'examen préalable sous réserve des lois applicables et conformément à celles-ci. Bien que Dell se réserve le droit de réviser ses politiques et de mettre en œuvre la sécurité du personnel à sa seule discrétion, en vertu de la politique en vigueur et sous réserve de la législation locale et de la disponibilité locale, Dell réalise un ou plusieurs des examens préalables suivants lors du recrutement : dépistage des drogues, recherche du numéro de sécurité sociale, recherche de casier judiciaire, vérification des formations et emplois précédents, et vérification de l'éligibilité à l'emploi. Dell tente de répondre aux normes de l'industrie en vigueur pour des entreprises similaires dans le secteur d'activité de Dell. Toutefois, Dell ne peut adapter son processus de sécurité et d'examen préalable du personnel pour répondre aux attentes spécifiques d'un Client particulier. Les tiers ou les sous-traitants externes sont soit sélectionnés par Dell, soit sélectionnés dans le cadre du contrat, soit sélectionnés par le sous-traitant selon une procédure approuvée par Dell. Dell applique une procédure disciplinaire pour prendre des mesures contre tout membre du personnel qui ne respecterait pas les exigences du programme de sécurité des informations, notamment, sans toutefois s'y

	limiter, celles qui sont mises en place dans ses engagements et exigences en matière de sécurité, disponibilité et confidentialité. Dell dispense une formation annuelle de sensibilisation à la sécurité à l'ensemble du personnel concerné et exige que les sous-traitants concernés dispensent cette formation à leur personnel.
Sécurité physique	Dell applique des politiques et des contrôles visant à restreindre l'accès physique aux installations contenant les composants physiques du Réseau Dell au personnel autorisé. Ces politiques et contrôles ont également pour objectif de prévenir toute entrée non autorisée dans ces installations. Des contrôles basés sur les risques sont en place dans les installations abritant les composants physiques du Réseau Dell (par exemple, les centres de données). Les contrôles d'accès peuvent inclure des agents de sécurité, des registres de sécurité, des dispositifs de surveillance, des alarmes, un accès limité aux zones sécurisées, la protection des voies d'accès, des caméras de surveillance, des badges et/ou l'authentification à deux facteurs. Cette disposition s'applique aux Sites en colocation gérés par Dell.
Sécurité du réseau	Dell peut accéder électroniquement au Réseau Dell dans la mesure où cela est nécessaire pour fournir les Services APEX. Dell appliquera des politiques et des contrôles d'accès pour gérer l'accès autorisé au Réseau Dell depuis chaque connexion. Elle utilisera notamment des pare-feu et des contrôles d'authentification. Grâce à la mise en place de contrôles, Dell assure la protection contre l'utilisation malveillante d'actifs et de logiciels malveillants au sein du Réseau Dell en fonction des risques. De tels contrôles peuvent notamment inclure : des politiques de sécurité, des contrôles d'accès restrictifs, des environnements distincts consacrés au développement et au test, la détection des logiciels malveillants sur les serveurs, ordinateurs de bureau et ordinateurs portables, l'analyse antivirus des pièces jointes aux e-mails, les analyses de conformité des systèmes, la surveillance et la réponse en matière de prévention des intrusions, la journalisation et l'alerte lors d'événements clés suspects, les procédures de gestion des informations basées sur le type de données, les applications d'e-commerce et la sécurité des réseaux, l'utilisation d'actifs externes, ainsi que l'analyse des failles de sécurité du système et des applications. Dell exige le chiffrement des données en transit et au repos lorsque cela est nécessaire et conformément à son programme de sécurité des informations. Dell utilise le chiffrement ainsi que des protocoles appropriés (tels que TLS) en cas d'accès à distance au système d'un client sur des réseaux ouverts. Lorsque ses clés de chiffrement ne sont pas utilisées, Dell les stocke dans des solutions approuvées conçues pour appliquer des pratiques de gestion de clé acceptées par l'industrie.
Contrôles d'accès	Dell met en œuvre des contrôles d'accès appropriés conçus pour prévenir l'accès non autorisé au Réseau Dell. Afin de réduire le risque d'utilisation abusive, intentionnelle ou autre, l'accès est contrôlé en respectant les principes de « moindre privilège » et de « nécessité de connaître ». Les contrôles d'accès que Dell peut déployer comprennent des vérifications d'accès, la maintenance des comptes de service, l'accès privilégié aux applications, des paramètres de niveau de système pour l'accès et la génération de rapports concernant l'accès.

	Dell s'appuie sur des pratiques normalisées de l'industrie, notamment, le cas échéant, l'authentification à deux facteurs, pour identifier et authentifier les utilisateurs du Réseau Dell. Dell requiert l'utilisation de mots de passe complexes sur le Réseau Dell. Dell (a) interdit aux utilisateurs du Réseau Dell de partager, noter, envoyer par e-mail ou message instantané, ou stocker des mots de passe non chiffrés sur tout système, et (b) verrouille les comptes après une série de tentatives consécutives de saisie de mot de passe incorrect. Dell utilise les pratiques normalisées de l'industrie pour renforcer les contrôles d'accès, notamment : (a) fermeture automatique des sessions utilisateur en cas d'inactivité ; (b) identification et mot de passe obligatoires pour rouvrir la session ; (c) protection contre l'accès externe au moyen d'un ou plusieurs pare-feu conformes aux normes industrielles, dont la connexion à Internet, le cas échéant, est protégée par une connexion VPN ; (d) masquage des mots de passe lorsqu'ils sont affichés ou saisis, le cas échéant ; et (e) chiffrement approprié et conforme aux normes industrielles des mots de passe lors de leur transmission.
Gestion des incidents	Dell s'appuie sur un cadre de réponse aux incidents pour préparer, gérer et réduire au maximum les effets des événements de sécurité et y répondre. Ce cadre comprend des procédures à suivre en cas d'incident de sécurité, notamment : (a) une équipe interne de réponse aux incidents avec un chef d'intervention ; (b) une équipe d'investigation chargée d'effectu une analyse des causes profondes et d'identifi les parties concernées ; (c) des processus internes de rapport et de notification ; (d) la documentation des actions réactives et des plans de remédiation ; et (e) un examen des événements après l'incident.
Gestion de la continuité d'activité	Dell applique des plans de continuité d'activité (« **BCP** ») pour la reprise après une interruption d'activité et le retour à la normale des opérations commerciales dès que raisonnablement possible. Dans ces circonstances, Dell déploiera tous les efforts raisonnables et opportuns pour Vous contacter en cas d'interruption d'activité ayant un impact important sur Votre/Vos Service(s) APEX.