Dernière mise à jour : 02/04/2024

Ces mesures de sécurité (« **Mesures de sécurité** ») font partie de l'accord signé entre NTICO et le Client qui fait référence au présent document. L'exécution des services par NTICO doit être conforme à l'Accord et aux présentes Mesures de sécurité. Les termes utilisés ici, mais qui ne sont pas définis ici, sont définis dans l'Accord.

NTICO se réserve le droit de modifier périodiquement ces Mesures de sécurité pour refléter les pratiques de sécurité actuelles, et cette modification entrera automatiquement en vigueur.

NTICO déploiera des efforts commercialement raisonnables pour prévenir la perte, le vol ou l'endommagement des données client provenant des services. Les Mesures de sécurité établissent les exigences nécessaires pour maintenir un programme de sécurité et garantir que des mesures de sécurité physiques, opérationnelles et techniques suffisantes sont en place pour la protection des Données du Client dans les Services. Ces Mesures de sécurité s'appliquent lorsque NTICO fournit les Services et l'Assistance au Client.

1. Gestion de la sécurité de l'information

1.1 Système de gestion de la sécurité de l'information. NTICO maintient et améliore continuellement un système de gestion de la sécurité de l'information documenté conformément aux pratiques standard de l'industrie et aux cadres acceptés pour la fourniture des services et de l'assistance OpCon, dont son personnel doit être informé et se conformer (« Système de gestion de la sécurité de l'information »).

1.2 Certification. Pendant la durée de l'accord, NTICO doit maintenir son rapport AICPA SOC2 ou équivalent, ainsi qu'un mécanisme de transfert légal pour l'exportation de données personnelles hors de l'Union européenne.

1.3 Tests. NTICO effectue au moins une fois par an des tests de sécurité par des tiers sur les applications et l'infrastructure utilisées pour soutenir la fourniture de services et d'assistance afin d'identifier les vulnérabilités de sécurité.

2. Sécurité organisationnelle

2.1 Responsabilités en matière de sécurité de l'information. NTICO a des rôles dédiés avec des responsabilités clairement définies pour l'administration du système de gestion de la sécurité de l'information.

2.2 Politiques de sécurité. Dans le cadre de l'administration du système de gestion de la sécurité de l'information, NTICO a créé des politiques de sécurité de l'information qui définissent la responsabilité de la protection de ses systèmes et des données du client (« politiques de sécurité de l'information »). Les politiques de sécurité de l'information comprennent des exigences conçues pour surveiller la conformité aux politiques et procédures de confidentialité et de sécurité de l'information.

3. Classification des actifs

3.1 Gestion d'actifs. NTICO maintient une politique de gestion des actifs conforme aux pratiques standard de l'industrie, y compris la classification des actifs (*par exemple* , informations, logiciels, matériel) et un inventaire des appareils et des systèmes qui administrent les services et le support pour permettre à NTICO de protéger les données et les actifs des clients.

3.2 Contrôles des actifs. NTICO a mis en place des contrôles de sécurité physiques, organisationnels et techniques pour protéger les données des clients contre tout accès et toute divulgation non autorisés.

4. Sécurité des personnes

4.1 Employés de NTICO. Les employés de NTICO doivent se comporter de manière cohérente avec ces Mesures de sécurité pour assurer une sécurité efficace. NTICO sensibilise ses employés à leurs responsabilités dans le maintien de contrôles de sécurité efficaces, en particulier en ce qui concerne l'utilisation de mots de passe, l'élimination des informations, les attaques d'ingénierie sociale, le signalement d'incidents et la sécurité physique et technique des utilisateurs et de l'équipement de l'entreprise par le biais de formations de sensibilisation à la sécurité/d'intégration. NTICO publie des politiques de sécurité documentées, les met à jour si nécessaire et fournit une formation mensuelle à la sécurité.

4.2 Vérification des antécédents. NTICO s'assure que ses employés impliqués dans la fourniture des Services et de l'Assistance ont passé avec succès les vérifications de base des antécédents conçues pour valider l'exhaustivité et l'exactitude des CV, la confirmation des qualifications professionnelles et la vérification de l'identité lorsque la loi le permet.

5. Sécurité physique et environnementale

5.1 Accès physique. Lorsque NTICO dispose d'un bureau physique, elle s'assure que seuls les utilisateurs autorisés ont un accès physique au réseau, aux systèmes et applications critiques, aux salles de serveurs, aux salles de communication et aux environnements de travail. NTICO maintient des contrôles pour surveiller les tentatives d'accès non autorisé. Des contrôles supplémentaires sont maintenus pour empêcher ou détecter le retrait d'un tel équipement.

5.2 Transfert de données. NTICO n'autorise pas le transfert des données du client vers un support de stockage externe ou amovible.

6. Gestion des communications et des opérations

6.1 Gestion des vulnérabilités/correctifs. NTICO a mis en place un processus de gestion des vulnérabilités/correctifs qui garantit que tous les systèmes utilisés pour fournir les Services et l'Assistance, y compris les périphériques réseau, les serveurs et les ordinateurs de bureau/portables, sont corrigés contre les vulnérabilités de sécurité connues dans un délai raisonnable en fonction de la criticité du correctif et de la sensibilité des Données du Client accessibles via les systèmes.

6.2 Configuration sécurisée du système. NTICO a mis en place des contrôles pour s'assurer que tous les systèmes utilisés pour fournir les services et l'assistance sont configurés en toute sécurité et de manière reproductible. Cela implique des modifications des paramètres

par défaut pour améliorer la sécurité du système (*par exemple, le* « renforcement » du système), des modifications des mots de passe de compte par défaut et la suppression de logiciels ou de services/démons inutiles. De plus, les appareils des employés utilisés pour interagir ou gérer les systèmes qui fournissent les Services et l'Assistance doivent également être configurés de manière reproductible. Des exigences supplémentaires spécifiques au-delà de ce qui existe également dans ces Mesures de sécurité comprennent :

6.2.1 Chiffrement complet/entier du disque ; et

6.2.2 Effacement et verrouillage des données à distance en cas de perte ou de vol de l'appareil

6.3 Prévention des logiciels malveillants. NTICO a mis en place des contrôles de détection et de prévention pour se protéger contre les logiciels malveillants et des procédures appropriées de sensibilisation des utilisateurs. NTICO maintient et met à jour les contrôles techniques et évalue régulièrement tous les systèmes pour l'existence de logiciels malveillants. NTICO effectue des analyses en temps réel ou régulières des appareils appartenant à NTICO pour détecter les virus, les logiciels malveillants et les éventuels incidents de sécurité.

6.4 Journalisation et audit. NTICO a mis en place un programme complet de gestion des journaux définissant la portée, la production, la transmission, le stockage, l'analyse et l'élimination des journaux en fonction des pratiques actuelles de l'industrie. Les systèmes et les services fournissent des capacités de journalisation conformément aux principes suivants :

6.4.1 Le champ d'application de la journalisation et la politique de conservation sont basés sur une approche basée sur les risques, avec une conservation minimale de six (6) mois ;

6.4.2 les registres sont recueillis pour permettre l'analyse scientifique des incidents de sécurité de l'information ;

6.4.3 les journaux, enregistrent les modifications administratives apportées aux Services ;

6.4.4 les registres sont conservés pratiquement en toute sécurité pour éviter toute falsification ;

6.4.5 Les mots de passe et autres éléments de données sensibles ne sont en aucun cas enregistrés ;

6.4.6 effectuer régulièrement l'analyse des journaux pour évaluer la sécurité ;

6.4.7 configurer tous les systèmes concernés pour fournir une journalisation en temps réel de tout événement susceptible d'indiquer une compromission du système, un événement de déni de service ou toute autre violation de la sécurité, y compris la notification d'un administrateur lorsque des seuils d'événements prédéterminés sont dépassés ; et

6.4.8 Les journaux sont protégés contre tout accès ou modification non autorisés.

7. Planification de la reprise après sinistre et de la continuité des activités

7.1 Programmes. NTICO a mis en place des programmes de reprise après sinistre et de continuité des activités et veille à ce que ces plans permettent de garantir la confidentialité et l'intégrité des données client pendant les opérations de récupération. NTICO s'assure que les programmes ne permettent aucune réduction de la sécurité.

7.2 Sauvegardes. Il est de la responsabilité du client de sauvegarder régulièrement sa ou ses bases de données.

8. Incidents de sécurité

8.1 Détection des incidents. NTICO a établi et maintient une capacité opérationnelle de détection des incidents et un programme d'intervention en cas d'incident clairement documenté pour répondre aux incidents de sécurité ou aux violations de système soupçonnés ou connus. Les plans d'intervention en cas d'incident comprennent des méthodes pour protéger les preuves d'activité contre la modification ou l'altération, et pour permettre l'établissement d'une chaîne de possession des preuves.

8.2 Réponse aux incidents. En cas d'incident affectant les données client, NTICO utilise les efforts standard de l'industrie pour répondre aux incidents et atténuer le risque pour le client et les données client.

8.3 Notification d'incident. Dans le cas d'un incident confirmé qui affecte les données du client, NTICO informera le client de l'incident de sécurité dans les 48 (quarante-huit) heures ouvrées suivant la confirmation.

9. Contrôle d'accès

9.1 Authentification. NTICO prend en charge les mécanismes d'authentification unique (SSO) permettant au client d'interagir avec Solution Manager (*par exemple,* Okta).

9.2 Accès au support. Si NTICO permet à ses employés d'accéder aux données client par le biais d'une interface de support d'application, cette interface, au minimum, doit (a) identifier de manière unique l' employé de NTICO qui l'a utilisée.

9.3 Mots de passe des utilisateurs. NTICO fournit aux employés une formation raisonnablement conçue pour s'assurer que les employés ont des exigences suffisantes en matière de complexité et d'expiration ou qu'ils ont besoin d'une couche de sécurité supplémentaire avec l'authentification multifacteur.

9.3.1 Authentification et authentification à deux facteurs. L'expression « authentification à deux facteurs » désigne l'authentification par la combinaison d'un élément qu'une personne connaît, tel qu'un nom d'utilisateur et un mot de passe, en combinaison avec un élément possédant, tel qu'un jeton d'authentification déconnecté, ou d'un facteur biométrique, tel qu'une empreinte digitale. NTICO utilise plusieurs facteurs d'authentification lorsqu'ils sont disponibles, et NTICO utilise au moins une authentification à deux facteurs pour accéder aux comptes utilisés pour fournir des services d'hébergement de données. Tout accès administratif par les employés de NTICO doit nécessiter une authentification à deux facteurs. Si NTICO utilise Google Apps pour gérer ses comptes, la vérification à deux facteurs doit être activée.

9.3.2 L'inactivité. Tous les appareils appartenant à NTICO se verrouillent automatiquement après une période d'inactivité raisonnable.

9.3.3 Départ d'un employé ou d'un consultant. Au moment du départ d'un employé, d'un sous-traitant ou d'un consultant tiers, l'accès de la personne aux réseaux, systèmes et comptes utilisés pour fournir les Services et l'Assistance, ainsi que l'accès à toutes les Données du Client, est résilié.

9.3.4 Autorisation. Le Client est le seul à contrôler et à donner accès aux Données Client. 9.6.5 Contrôles d'accès au réseau. Tous les réseaux utilisés par NTICO pour fournir les Services et l'Assistance sont protégés par l'utilisation de contrôles capables de bloquer le trafic réseau non autorisé, à la fois entrant (entrant) et sortant (sortant).

10. Sécurité des données

10.3 Chiffrement.

10.3.1 Données en transit. NTICO s'assure que HTTPS est activé dans toute interface Web liée au produit ou au service. NTICO permet au client d'utiliser TLS 1.2 ou supérieur pour les applications Web.

10.3.2 Données au repos. Les données client au repos pour les clients OpCon sur site relèvent de la responsabilité du client. Pour les clients d'OpCon Cloud, il est crypté à tout moment à l'aide des normes de cryptographie acceptées par l'industrie. Cela comprend au minimum :

10.3.2.1 Utilisation de la norme AES (Advanced Encryption Standard) définie dans la norme FIPS 197.

10.3.2.2 Lorsque différents algorithmes sont utilisés, ils ont des forces comparables (*par exemple,* si une clé AES-256 doit être chiffrée, une clé AES-256 ou supérieure, ou RSA-3072 ou supérieure peut être utilisée pour la chiffrer).