PHOENIX TOWER
INTERNATIONAL

POLITIQUE DE SÉCURITÉ DES INFORMATIONS DE PHOENIX TOWER INTERNATIONAL

À COMPTER DE À PARTIR DU 15 AOÛT 2023

OBJECTIF

Phoenix Tower US Holdings, L.P. et ses filiales et Sociétés affiliées dans le monde entier (collectivement « PTI », « Phoenix Tower » ou « Société »), s'engagent à protéger la sécurité des informations et à poursuivre l'apprentissage et l'amélioration, comme indiqué dans la présente Politique de sécurité des informations (la « Politique »). Le cadre de la présente Politique se veut complet et comprendra les exigences de la Société en matière de sécurité et de protection des actifs PTI, y compris les informations personnellement identifiables (« PII »), dans toute la Société et ses fournisseurs agréés sur les lieux de travail et hors de ceux-ci. Tous les employés doivent examiner et suivre les informations contenues dans la présente Politique.

PORTEE

La présente Politique s'applique à tous les employés et fournisseurs de Phoenix Tower qui prennent en charge ou interagissent avec Phoenix Tower et ses actifs d'information. Chaque section de la présente Politique s'applique à des aspects spécifiques du programme de sécurité des informations de PTI.

DEFINITIONS

- **Informations confidentielles : comprennent, sans s'y limiter**, toutes les informations matérielles, non publiques, liées aux affaires, les droits de propriété intellectuelle, les secrets commerciaux, le savoir-faire commercial, sous forme écrite ou orale, qu'elles soient ou non identifiées comme telles, relatives à des questions telles que la stratégie commerciale, les processus, les finances, les plans de marketing, les contrats et/ou la technologie. Les exemples incluent, mais ne sont pas limités à :
    - Contrats, à la fois signés et sous forme de projet ;
    - Matériel de marketing en cours de développement ; ou alors
    - Projections de ventes ou de revenus.
- **Sécurité des informations :** les processus et méthodologies qui sont conçus et mis en œuvre pour protéger les informations ou les données imprimées, électroniques ou toute autre forme d'informations ou de données confidentielles, privées ou sensibles contre l'accès, l'utilisation non autorisés, la mauvaise utilisation, la divulgation, la destruction, la modification ou la perturbation.
- **Employé :** une personne physique identifiée ou identifiable qui agit en tant qu'administrateur, dirigeant, membre de l'équipe, employé, sous-traitant ou consultant de PTI, à temps plein ou à temps partiel, à titre temporaire ou permanent.
- **Dispositifs destinés aux utilisateurs finaux :** tout outil ou dispositif technologique utilisé par un employé de PTI pour stocker des informations ou accéder aux systèmes de PTI, y compris le courrier électronique. Des exemples

de dispositifs destinés aux utilisateurs finaux comprennent les ordinateurs, les ordinateurs portables, les smartphones, les disques durs externes et le stockage USB.

- **Informations personnellement identifiables (« PII ») :** toute donnée qui pourrait potentiellement identifier une personne spécifique, comme le nom, l'adresse e-mail, les informations financières, le numéro de sécurité sociale, le numéro de passeport, etc.

SURVEILLANCE DES POLITIQUES

Phoenix Tower considère la sécurité des informations comme l'un des aspects les plus importants de son activité.

- La direction générale de Phoenix Tower montrera l'exemple en veillant à ce que la sécurité des informations soit une grande priorité dans toutes les activités et initiatives commerciales actuelles et futures.
- La présente Politique et chacune de ses annexes seront revues annuellement par le Directeur juridique mondial pour s'assurer qu'elles sont pertinentes et à jour et révisées, si nécessaire, pour s'assurer qu'elles sont adéquates à la lumière de l'évolution des obligations légales, de la technologie et des besoins commerciaux.
- La direction communiquera les révisions de la politique à tout le personnel par divers moyens, tels que des mises à jour électroniques, des séances d'information, des formations, des bulletins d'information, etc.

Pour atteindre ou dépasser ces objectifs, les pratiques suivantes ont été mises en place :

- Les employés signent un avis de réception, d'examen et d'accusé de réception de la Politique de sécurité des informations lorsqu'ils sont embauchés/retenus.
- La sensibilisation du personnel sera périodiquement renforcée pour faire des questions de sécurité de l'information une priorité.
- La formation à la sécurité de l'information est obligatoire dès le début, en commençant par l'intégration des employés. Toute formation technique doit être appropriée aux responsabilités de la fonction du poste. Lorsque les membres du personnel changent de poste ou de fonction, leurs besoins en matière de sécurité de l'information doivent être réévalués et une nouvelle formation doit être dispensée en priorité.

1. ORGANISATION DE LA SÉCURITÉ

1.1 DÉFINITION DES RÔLES ET RESPONSABILITÉS

Les rôles suivants sont établis dans PTI liés à la sécurité de l'information :

RÔLES	RESPONSABILITÉS

Directeur des technologies de l'information	Déterminer les exigences de sécurité des services fournis en évaluant l'impact d'un incident affectant la sécurité des services au détriment de la disponibilité, de l'authenticité, de l'intégrité, de la confidentialité ou de la traçabilité.
Directeur des technologies de l'information	Détermine les exigences de sécurité des informations traitées, en évaluant l'impact qu'un incident affectant la sécurité des informations aurait sur la disponibilité, l'authenticité, l'intégrité, la confidentialité ou la traçabilité.
Directeur des technologies de l'information	Doit déterminer les décisions pour satisfaire aux exigences de sécurité de l'information et des services, superviser la mise en œuvre des mesures nécessaires et rendre compte de ces questions.
Responsable principal des technologies de l'information	Responsable du développement de la manière spécifique de mettre en œuvre la sécurité dans les systèmes et de la supervision du fonctionnement quotidien des systèmes, et peut déléguer aux administrateurs ou opérateurs sous sa responsabilité.
Responsable principal des technologies de l'information	Responsable des tâches de sécurité technique, qui les exécute.

2. INFORMATIONS PERSONNELLEMENT IDENTIFIABLES

Cette section est destinée à guider la protection des PII collectées auprès des propriétaires, des locataires, des prospects et des employés, et elle aidera les employés à déterminer quelles informations peuvent être divulguées à des non-employés, ainsi que la sensibilité relative des informations qui ne seront pas divulguées en dehors de Phoenix Tower sans autorisation appropriée.

2.1 Définitions

Phoenix Tower reconnaît son besoin de maintenir la confidentialité des PII et comprend que ces informations sont uniques à chaque individu et sont généralement limitées aux données pertinentes et nécessaires à ses objectifs. Les PII couvertes par la présente Politique peuvent provenir de divers types d'individus exécutant des tâches au nom de la Société et comprennent les employés, les postulants/candidats, les entrepreneurs

indépendants et toutes les PII conservées sur sa base de clients. Les PII comprennent toutes les informations identifiables sur les propriétaires, les locataires, les prospects et les employés :

- Coordonnées personnelles (numéros de téléphone, adresses, etc.) ;
- Numéros de sécurité sociale (ou leur équivalent émis par des entités gouvernementales en dehors des États-Unis) ;
- Numéros d'identification fiscale (ou leur équivalent émis par des entités fiscales gouvernementales en dehors des États-Unis) ;
- Numéros d'identification d'employeur (ou leur équivalent émis par des entités gouvernementales en dehors des États-Unis) ;
- Numéros de permis de conduire d'État ou étrangers ou copies de cartes d'identité ;
- Numéros de passeport ou copies de passeports ;
- Date de naissance ;
- Numéros de carte de crédit ou de débit de l'entreprise ou détenus individuellement (y compris numéros PIN ou d'accès) conservés dans les registres de l'organisation ou des fournisseurs approuvés ; ou
- Informations de compte bancaire de PTI ou de ses partenaires commerciaux.

Les PII peuvent résider dans des copies papier ou des enregistrements électroniques ; les deux formes de PII entrent dans le cadre de la présente Politique.

2.2 Stockage et gestion des informations contenant des PII

PII électroniques

Les PII peuvent être enregistrées électroniquement par une variété de méthodes et sur une variété de dispositifs destinés aux utilisateurs finaux, comprenant mais sans s'y limiter :

- Des dispositifs informatiques mobiles (c'est-à-dire ordinateurs portables, smartphones, tablettes, ordinateurs, PDA, etc.).
- Des programmes de messagerie électronique, d'Internet et de messagerie instantanée qui stockent, traitent ou transmettent des données.
- Les supports électroniques amovibles, tels que les clés USB, les lecteurs de CD, les disques durs externes, etc., ne doivent être utilisés que pour les PII non sensibles. Les PII sensibles, telles que les numéros de sécurité sociale, les informations de passeport et les données bancaires ou d'autres données financières ne doivent pas être enregistrées sur un support électronique amovible.
- Serveurs locaux et Cloud PTI.
- Serveurs tiers basés sur le cloud.

Cette section de politique définit les exigences et le processus d'approbation pour les dispositifs destinés aux utilisateurs finaux qui sont détenus, gérés ou loués par PTI. Tous dispositifs destinés aux utilisateurs finaux qui ne sont pas détenu, loués ou gérés par PTI

ne seront pas autorisés à accéder aux serveurs locaux contenant des PII ou à supprimer ceux-ci, sauf autorisation écrite du Directeur juridique mondial.

- **Dispositifs informatiques mobiles (c'est-à-dire ordinateurs portables, smartphones, tablettes, PDA, etc.)** – Les PII peuvent être enregistrées sur des dispositifs informatiques mobiles, mais ces dispositifs doivent être protégés par mot de passe, cryptés et avoir des capacités d'effacement à distance. Ce n'est pas une méthode préférée de stockage des PII et les informations stockées sur les dispositifs informatiques mobiles doivent être considérées comme un emplacement de stockage temporaire et les PII doivent être déplacées vers un serveur PTI dès que possible.
- **Programmes de messagerie électronique, d'Internet et de messagerie instantanée –** La Société ne recommande pas la transmission des PII via Internet ou des programmes de messagerie instantanée. Lorsque des II doivent être transférées par courriel, les étapes suivantes doivent être prises pour garantir une transmission sécurisée et minimiser le risque de violation une fois que ces PII sont confirmées comme ayant été enregistrées sur le serveur local :
    1. Le mot de passe protège le document, qu'il soit PDF, Word ou Excel. Si le document est dans un format qui n'est pas facilement protégé (par exemple, gif ou jpeg), convertissez le document en un fichier pdf, protégez-le par mot de passe dans ce format et réenregistrez-le. Le format « original » peut être supprimé à ce moment et retiré de la corbeille.
    2. Envoyez le document par courriel avec pour langue « **CONFIDENTIEL** » comme étiquette après le nom du sujet
       dans la ligne d'objet.
    3. Contactez le destinataire par téléphone pour confirmer que le destinataire a reçu le courrier électronique et fournissez-lui le mot de passe. ***NE JAMAIS ENVOYER LE MOT DE PASSE PAR COURRIEL***
    4. Supprimez la pièce jointe du courrier électronique envoyé.

Les PII sensibles, telles que les numéros de sécurité sociale, les informations de passeport et les données bancaires ou d'autres données financières ne doivent **pas** être transmises par courrier électronique.

Si PTI reçoit des PII par l'intermédiaire de l'Internet ou des programmes de messagerie instantanée, ou tout autre moyen non sécurisé, les informations doivent être transférées immédiatement au serveur PTI (première préférence) ou déplacées vers le stockage d'un dispositif informatique mobile, puis supprimées définitivement du programme dans lequel il a été reçu.

- **Supports électroniques amovibles –** les PII peuvent être enregistrées sur des supports électroniques amovibles, tels que des clés USB, dans le but de transporter des informations entre les supports. Les dispositifs de support amovibles doivent être protégés par mot de passe et cryptés. Ce n'est pas une méthode préférée de stockage des PII. Les informations stockées sur un support

électronique amovible doivent être considérées comme un emplacement de stockage temporaire et les PII doivent être déplacées vers un serveur PTI dès que possible et supprimées du support amovible. Les PII sensibles, telles que les numéros de sécurité sociale, les informations de passeport et les données bancaires ou d'autres données financières ne doivent **pas** être enregistrées sur un support électronique amovible.

- **Serveur local ou Cloud PTI** – L'emplacement préféré pour le stockage de toutes les PII est sur les serveurs locaux ou cloud appartenant à PTI et cette méthode de stockage doit toujours être utilisée en premier lorsqu'elle est disponible. Tous les dossiers et données contenant des PII doivent être clairement étiquetés comme tels et l'accès à ces dossiers sera limité uniquement aux employés qui doivent y avoir accès dans le cadre des fonctions quotidiennes de leur travail.
- **Stockage sur papier (sur site)** – Les PII stockées dans les bureaux doivent être sécurisées dans des tiroirs verrouillés et de préférence derrière des portes verrouillées si possible. L'accès à ces emplacements devrait être limité aux employés qui ont besoin des informations dans l'exercice de leurs fonctions de travail quotidiennes. Les clés de ces emplacements sécurisés doivent être conservées uniquement par le directeur du service et tout accès fourni aux employés doit être documenté dans un format de journal. En aucun cas ordinaire, des documents contenant des PII ne doivent être retirés du bureau et de tels cas nécessitant la suppression des PII du bureau nécessiteront l'approbation du PDG. L'ensemble des informations, données et documents contenant des PII doivent être clairement étiquetés afin que tous les utilisateurs soient conscients de la propriété, de la classification et de la valeur des informations. Les informations, données et documents contenant des PII seront transportés en toute sécurité et détruits en toute sécurité, pour éviter toute divulgation involontaire. Les informations, données et documents contenant des PII seront stockés en toute sécurité lorsqu'ils ne sont pas utilisés.
- **Stockage sur papier (hors site) –** Le stockage des PII en format papier hors site n'est généralement pas autorisé sans l'approbation écrite du PDG. Les données contenant des PII au format papier ne doivent pas être envoyées à des installations de stockage hors site dans le cadre des fichiers du site, et en aucun cas ces données ne doivent être stockées au domicile des employés. L'ensemble des informations, données et documents contenant des PII doivent être clairement étiquetés afin que tous les utilisateurs soient conscients de la propriété, de la classification et de la valeur des informations. Les informations, données et documents contenant des PII seront transportés en toute sécurité et détruits en toute sécurité, pour éviter toute divulgation involontaire. Les informations, données et documents contenant des PII seront stockés en toute sécurité lorsqu'ils ne sont pas utilisés.
- **Transport de copies papier –** Lorsque les PII doivent être transportées hors des locaux du bureau dans des situations approuvées, cela ne doit être effectué que par des employés directs de PTI. Il convient de veiller à ce que les données contenant des PII soient sécurisées (mallette verrouillée, etc.) et que ces données soient toujours en la possession de l'employé pendant le transport.
- **Impressions sur papier** – L'impression de données contenant des PII et

stockées électroniquement doit être évitée autant que possible. Dans les situations où cela n'est pas possible, l'employé qui imprime les données devra recevoir l'approbation préalable du directeur du service, indiquant quels documents sont imprimés et pour quelle raison. L'employé sera également responsable de la destruction des copies papier et fournira au directeur du service une déclaration contenant la date de destruction, la description du matériel détruit et la méthode utilisée.

2.3 Accès aux PII par les employés

Chaque directeur du service est chargé d'identifier et de maintenir une liste des utilisateurs de son service qui devraient avoir accès aux fichiers (électroniques ou papier). La liste devrait être mise à jour au besoin et au minimum révisée chaque année et lors d'un événement personnel (p. Ex. Embauche, départ, licenciement, promotion). La liste sera fournie au service informatique qui, à son tour, sera chargé de veiller à ce que l'accès aux fichiers électroniques contenant des PII soit restreint conformément à la liste. Chaque directeur du service sera chargé de veiller à ce que l'accès aux fichiers papier contenant des PII soit restreint conformément à la liste. Les directeurs du service et/ou les responsables qu'ils désignent doivent examiner l'accès des utilisateurs en cas de changement des rôles et responsabilités de la personne concernée, ou du statut d'employé/d'entrepreneur indépendant (y compris, mais sans s'y limiter, le licenciement) et communiquer tout changement en temps opportun au service informatique.

2.4 Exigences réglementaires

La politique de la Société est de se conformer à toutes les lois et réglementations internationales, fédérales ou étatiques concernant l'accès, l'utilisation, le stockage et la conservation des PII. Le ou les services juridiques et/ou de conformité de Phoenix Tower superviseront toutes les questions de conformité réglementaire. Si une disposition de la présente Politique entre en conflit avec une exigence statutaire de la loi internationale, fédérale ou étatique régissant les PII, la ou les dispositions de la politique qui sont en conflit seront remplacées.

2.5 Formation

Toutes les nouvelles recrues qui entrent dans la Société reçoivent une formation initiale concernant la gestion et la protection appropriées des PII, et reçoivent une copie de la présente Politique et des procédures de mise en œuvre pour le service auquel elles sont assignées (le cas échéant). Les employés occupant des postes avec un accès régulier et continu aux PII ou ceux transférés à de tels postes reçoivent une formation renforçant la présente Politique et les procédures de maintenance des données PII et reçoivent une formation concernant la sécurité et la protection des

données PII et des données exclusives de la Société au moins une fois par an. La formation sera animée par le service informatique et fera partie de l'orientation des nouveaux employés dans le cas des nouveaux employés. Si un employé existant est ajouté à la liste d'accès PII, l'employé recevra une formation distincte sur les dispositions de la présente Politique.

2.6 Confirmation de confidentialité

Tous les employés de la Société doivent maintenir la confidentialité des PII ainsi que des informations confidentielles de la Société auxquelles ils peuvent avoir accès et comprendre que ces PII doivent être réservées uniquement aux personnes ayant un besoin professionnel de connaître.

2.7 Violations de données PII/Incidents de sécurité

Si un employé prend connaissance d'une utilisation, d'un accès ou d'un transfert de PII qui est en conflit avec la présente Politique ou de tout incident de sécurité, l'employé doit le signaler immédiatement au service juridique de Phoenix Tower. Les bases de données ou ensembles de données qui incluent des PII peuvent être violés par inadvertance ou par intrusion illicite. Veuillez consulter la section 6 de la présente Politique pour de plus amples informations.

2.8 Violations des Politiques et Procédures de PII

Phoenix Tower considère que la protection des données personnelles est de la plus haute importance. Les infractions à la présente Politique ou à ses procédures entraîneront des mesures disciplinaires pouvant inclure une suspension ou un licenciement en cas de violations graves ou répétées.

2.9 Surveillance de l'utilisation des systèmes informatiques

La Société a le droit et la capacité de surveiller les informations électroniques créées et/ou communiquées par des personnes utilisant les systèmes et réseaux informatiques de la Société, y compris les messages électroniques et l'utilisation d'Internet. Il n'est pas dans la politique ou l'intention de la Société de surveiller en permanence toute utilisation de l'ordinateur par les employés ou d'autres utilisateurs des systèmes et du réseau informatiques de la Société. Cependant, les utilisateurs des systèmes doivent être conscients que la Société peut surveiller l'utilisation, y compris, mais sans s'y limiter, les modèles d'utilisation d'Internet (par exemple, accès au site, durée en ligne, accès à l'heure de la journée), et les fichiers électroniques et les messages des employés dans la mesure nécessaire pour garantir que l'Internet et les autres communications électroniques sont utilisés conformément à la loi et à la

politique de la Société. L'utilisation des systèmes et réseaux informatiques de la Société sera considérée comme une attestation et un consentement affirmatifs de la surveillance décrite ci-dessus.

3. UTILISATION ACCEPTABLE

Le but de cette section est d'assurer l'utilisation acceptable de l'équipement informatique détenu, loué ou géré par Phoenix Tower. Une utilisation inappropriée expose Phoenix Tower à des risques tels que des attaques de virus, une compromission des systèmes et des services réseau, des atteintes à la réputation et des problèmes juridiques.

3.1 Utilisation générale et propriété

- Les utilisateurs seront conscients que les données qu'ils créent ou les applications utilisant les données des systèmes d'entreprise restent la propriété de Phoenix Tower. Les employés ne doivent avoir aucune attente de confidentialité pour leurs activités lorsqu'ils utilisent l'équipement informatique PTI et aucune attente de propriété, y compris lors de la séparation de la Société.
- Pour des raisons de sécurité et de maintenance du réseau, les personnes autorisées au sein de Phoenix Tower peuvent surveiller l'équipement, les systèmes et le trafic réseau à tout moment.
- Phoenix Tower se réserve le droit de vérifier périodiquement les réseaux et les systèmes afin de garantir la conformité à la présente Politique.

3.2 Sécurité et informations exclusives

- Les informations conservées sur les systèmes de Phoenix Tower qui contiennent des PII seront clairement étiquetées comme telles conformément à la section Informations personnellement identifiables de la présente Politique. Les utilisateurs s'efforceront de protéger ces informations.
- Protégez vos mots de passe et ne partagez pas de comptes. Les utilisateurs autorisés sont responsables de la sécurité et de l'intégrité de leurs mots de passe et comptes.
- Les employés doivent faire preuve d'une extrême prudence lors de l'ouverture des pièces jointes reçues d'expéditeurs inconnus, qui peuvent contenir des virus ou des logiciels malveillants.
- Les systèmes stockant des informations confidentielles de Phoenix Tower ou utilisés pour le traitement des informations ne doivent pas être retirés des locaux de Phoenix Tower sans l'approbation officielle de la direction.
- Les employés ne doivent pas utiliser les fonctionnalités de remplissage automatique du navigateur Web ou d'autres fonctionnalités qui enregistrent les informations d'ID d'utilisateur et de mot de passe dans des applications

commerciales en ligne.

3.3 Activités interdites

- Le fait de s'engager dans toute activité illégale en vertu des lois locales, étatiques, fédérales ou internationales tout en utilisant les ressources appartenant à Phoenix Tower.
- L'exportation de logiciels, d'informations techniques, de logiciels ou de technologies de cryptage, en violation des lois internationales ou régionales de contrôle des exportations, est illégale. La direction appropriée sera consultée avant l'exportation de tout matériel en question.
- L'utilisation d'un actif informatique de Phoenix Tower pour s'engager activement dans l'acquisition ou la transmission de matériel qui est en violation des lois sur le harcèlement sexuel ou les lieux de travail hostiles.
- Le contournement de l'authentification des utilisateurs ou de la sécurité de tout hôte, réseau ou compte. L'utilisation non autorisée d'un identifiant de réseau autre que le vôtre est strictement interdite.
- Toutes tentatives non autorisées de contourner la sécurité du réseau, la protection des données, la sécurité par mot de passe ou l'installation/l'utilisation de logiciels conçus pour contourner toute sécurité ou politique créée et mise en œuvre par Phoenix Tower.
- Toute tentative de falsifier ou de manipuler des communications réseau ou des fichiers d'un autre employé.
- La violation des lois sur les droits d'auteur et leurs dispositions sur l'utilisation équitable. Cela inclut la copie ou le « piratage » de logiciels ou la violation de licences/d'accords de logiciels.
- Installation d'applications non officielles sur tous les actifs de Phoenix Tower sans le consentement préalable du service informatique.
- Divulgation d'informations confidentielles et/ou de secrets commerciaux.
- Les utilisateurs ne doivent pas s'engager délibérément à accéder aux systèmes de la Société pour lesquels ils n'ont pas d'autorisation ou qu'ils ont besoin de connaître.

4. UTILISATION DU COURRIER ELECTRONIQUE

Cette section a pour but de fournir des directives pour une utilisation acceptable des courriers électroniques et de décrire les procédures de conservation des courriers électroniques.

4.1 Utilisation autorisée

- Les systèmes de courrier électronique et de courrier électronique de la Société doivent être utilisés à des fins commerciales uniquement et doivent être conformes aux politiques et procédures de PTI en matière de conduite éthique, de sécurité et de conformité aux lois et pratiques commerciales applicables.

Toutes les communications personnelles sur les courriers électroniques de la société doivent être limitées.

- Les employés ne doivent pas s'attendre à la confidentialité de tout ce qu'ils stockent, envoient ou reçoivent sur le système de courrier électronique de la Société. PTI peut surveiller les messages sans préavis.
- Les employés doivent se plaindre avec l'authentification multi-facteurs.

4.2 Courrier électronique contenant des PII

- Si des II doivent être transférées par courriel, les étapes suivantes doivent être prises pour garantir une transmission sécurisée et minimiser le risque de violation une fois que ces PII sont confirmées comme ayant été enregistrées sur le serveur local :
    1. Le mot de passe protège le document, qu'il soit PDF, Word ou Excel. Si le document est dans un format qui n'est pas facilement protégé (par exemple, gif ou jpeg), convertissez le document en un fichier pdf, protégez-le par mot de passe dans ce format et réenregistrez-le. Le format « original » peut être supprimé à ce moment et retiré de la corbeille.
    2. Envoyez le document par courriel avec pour langue « **CONFIDENTIEL** » comme étiquette après le nom du sujet
       dans la ligne d'objet.
    3. Contactez le destinataire par téléphone pour confirmer que le destinataire a reçu le courrier électronique et fournissez-lui le mot de passe. ***NE JAMAIS ENVOYER LE MOT DE PASSE DANS LE MÊME COURRIEL QUE LES PII***
    4. Supprimez la pièce jointe du courrier électronique envoyé.

- Les PII sensibles, telles que les numéros de sécurité sociale, les informations de passeport et les données bancaires ou d'autres données financières ne doivent **pas** être envoyées par courrier électronique.
- Si PTI reçoit des PII par l'intermédiaire d'un courrier électronique, de l'Internet ou des programmes de messagerie instantanée, les informations doivent être transférées immédiatement au serveur local (première préférence) ou déplacées vers le stockage d'un dispositif informatique mobile, puis supprimées définitivement du programme dans lequel il a été reçu.

4.3 Activités de messagerie électronique et de communication interdites

- L'utilisation du courrier électronique de PTI à des fins commerciales non liées au PTI ou pour un usage personnel fréquent.
- Le transfert automatique des courriers électroniques de PTI vers des systèmes ou plates-formes de messagerie électronique tiers.
- La suppression ou la modification du message de non-responsabilité juridique généré par le système joint à chaque courrier électronique de PTI.

- L'envoi de courriers électroniques non sollicités, y compris l'envoi de « pourriel » ou de tout autre matériel publicitaire ou de sollicitation à des personnes qui n'ont pas spécifiquement demandé ce matériel (courrier indésirable).
- La création ou la diffusion de tout message perturbateur ou offensant. Les employés qui reçoivent des courriers électroniques contenant ce contenu de la part d'un employé de Phoenix Tower le signaleront immédiatement à leur superviseur.
- L'utilisation de comptes de messagerie n'appartenant pas à Phoenix Tower (Hotmail, Gmail et autres) pour les activités officielles de Phoenix Tower, ou le transfert des courriers électroniques reçus dans les comptes de messagerie Phoenix Tower vers des comptes de messagerie personnels ou n'appartenant pas à Phoenix Tower (Hotmail, Gmail et autres).
- La souscription à des services électroniques ou à d'autres contrats utilisant des adresses de courriel de PTI sans raison commerciale valable.

4.4 Dispositifs mobiles

- Les employés doivent obtenir l'approbation préalable de leur responsable ou superviseur avant d'essayer d'accéder au courrier électronique de PTI par l'intermédiaire des dispositifs mobiles personnels.
- Phoenix Tower permet d'accéder au courrier électronique par l'intermédiaire des dispositifs personnels mobiles conformément à la présente Politique. Phoenix Tower n'est pas responsable de la perte de données en cas d'effacement des données d'un dispositif (soit en raison d'une erreur de l'utilisateur, soit en raison de fonctionnalités de sécurité mises en œuvre). La présente politique s'applique à tous les dispositifs d'utilisateurs finaux portables et à tout autre dispositif pouvant accéder aux services de messagerie de Phoenix Tower et/ou aux données protégées de Phoenix Tower. Le respect de la présente Politique est une exigence pour tous les dispositifs informatiques portables stockant ou accédant aux données protégées de Phoenix Tower.
- Les utilisateurs qui utilisent un dispositif informatique portable pour accéder au courrier électronique, aux données, aux enregistrements ou aux documents de Phoenix Tower doivent mettre en œuvre les fonctions de sécurité suivantes dans la mesure où elles sont disponibles sur le dispositif :
    - Être configuré pour se déconnecter ou s'éteindre pas plus de dix (10) minutes après la dernière activité de l'utilisateur.
    - Exiger un mot de passe ou un code d'accès de mise sous tension.
    - Exiger une longueur de mot de passe minimale de quatre (4) caractères ou clés.
    - Fournir une réinitialisation du dispositif (effacement des données) si un mot de passe incorrect est entré plus de huit (8) fois consécutives, lorsque cela est techniquement possible.
    - Le dispositif doit être chiffré.

- Les utilisateurs qui utilisent un dispositif informatique portable pour accéder au courrier électronique, aux données, aux enregistrements ou aux documents de Phoenix Tower doivent apporter leur dispositif au service informatique pour s'assurer que ces fonctionnalités de sécurité sont mises en œuvre.

4.5 Mise au rebut de l'équipement

Avant la mise au rebut ou le transfert, toutes les données de Phoenix Tower doivent être entièrement effacées de tous les dispositifs informatiques portables et des cartes mémoire associées. Lors de l'expiration de l'accès d'un employé aux systèmes de Phoenix Tower, l'individu apportera son dispositif informatique portable au service informatique afin que le service informatique puisse supprimer toutes les données de Phoenix Tower du dispositif.

4.6 Rapports

- La perte, le vol ou toute utilisation non autorisée d'un dispositif d'utilisateur final portable qui a été utilisé pour stocker ou accéder aux informations protégées de Phoenix Tower constitue une divulgation et doit être signalé(e) à Phoenix Tower IT.
- Le service informatique se coordonnera avec le service juridique et le superviseur des utilisateurs pour déterminer dans quelle mesure les données d'un dispositif d'utilisateur final appartenant à PTI ou personnel doivent être effacées en cas de perte ou de vol et à la fin de l'emploi de l'utilisateur chez PTI. S'il est déterminé qu'un effacement à distance est nécessaire et possible, le service informatique tentera de limiter les données effacées aux seules informations de Phoenix Tower dans la mesure techniquement possible sur les dispositifs appartenant à PTI et/ou les dispositifs pour lesquels des remboursements s'appliquent.

5. UTILISATION DE L'INTERNET

La Société fournira un accès Internet aux employés et entrepreneurs qui sont connectés au réseau interne et qui ont un besoin commercial pour cet accès.

L'Internet est un outil commercial pour la Société. Il doit être utilisé à des fins commerciales telles que : la communication par courrier électronique avec les fournisseurs et les partenaires commerciaux, l'obtention d'informations commerciales utiles et la recherche de sujets techniques et commerciaux pertinents.

Le service Internet ne peut pas être utilisé pour transmettre, récupérer ou stocker des communications de nature discriminatoire ou harcelante ou qui sont désobligeantes pour tout individu ou groupe, obscènes ou pornographiques, ou de nature diffamatoire ou menaçante pour des « lettres à chaînes » ou pour toute autre fin illégale ou pour un gain personnel.

6. PERSONNEL

L'objectif de cette section est de réduire le risque d'erreur humaine, de vol, de fraude ou de mauvaise utilisation des installations. Étant donné que la sécurité de nos actifs d'information est un élément essentiel de notre modèle d'entreprise, il est essentiel que tous les employés de Phoenix Tower soient soumis à certaines normes pour garantir leur crédibilité et leur sécurité.

6.1 Stockage des PII sur les systèmes de la Société

- Nonobstant le respect de Phoenix Tower pour la vie privée des employés sur le lieu de travail, Phoenix Tower se réserve le droit d'avoir accès à toutes les informations créées et stockées sur ses systèmes.
- Phoenix Tower a le droit de surveiller toutes les informations reçues, stockées, transmises et/ou créées sur les systèmes
  Phoenix Tower.

6.2 Partage d'informations confidentielles

- Les informations confidentielles ne seront partagées qu'avec d'autres personnes autorisées.
- Les informations sur l'organisation ont leurs propres niveaux de sensibilité et ne doivent pas être divulguées au personnel qui n'est pas autorisé à accéder à ces informations.
- Toutes les données et informations n'appartenant pas au domaine public, relatives aux activités de Phoenix Tower et à ses employés, doivent rester confidentielles à tout moment.
- Les informations confidentielles ne doivent pas être divulguées aux membres de la famille qui n'ont pas l'autorisation de recevoir de telles informations.

7. SECURITE PHYSIQUE

Cette section interdit l'accès physique non autorisé aux locaux et aux informations de Phoenix Tower et évite tout dommage ou toute interférence avec les opérations commerciales normales. La présente Politique couvre également toute la sécurité physique des entrées, des installations de travail de bureau et d'autres zones essentielles qui doivent être sécurisées afin de protéger les actifs.

7.1 Sécurité physique

- Des portes de sécurité, des lecteurs de badges et des claviers à code PIN sont utilisés pour sécuriser les zones contenant des informations essentielles. Seuls les employés autorisés peuvent pénétrer dans ces zones sécurisées.
- Le personnel sera surveillé électroniquement en fonction des zones auxquelles il a été autorisé à accéder. Ceci afin d'atténuer les risques de vol, de vandalisme

et d'utilisation non autorisée des systèmes.
- Les zones dans lesquelles des informations sécurisées sont traitées (y compris le traitement des informations et les installations informatiques) seront soumises à des contrôles d'accès stricts pour garantir qu'aucun employé non autorisé ou qu'aucune personne extérieure à l'organisation ne puisse y accéder.

7.2 Sécurisation des postes de travail et des installations de travail sans surveillance

- L'équipement doit toujours être protégé de manière appropriée, en particulier lorsqu'il est laissé sans surveillance.
- Avant de quitter votre bureau, si votre bureau est hors de vue, votre ordinateur doit être déconnecté ou verrouillé afin d'empêcher tout accès non autorisé.
- Les imprimantes et les télécopieurs seront quotidiennement débarrassés des données sensibles. Les documents sensibles envoyés aux imprimantes ou aux télécopieurs doivent être sécurisés à mesure qu'ils sont imprimés.

7.3 Prêt des clés, des codes de sécurité ou des badges d'accès de sécurité à d'autres

- L'utilisation de clés, qu'elles soient physiques ou électroniques, pour accéder aux zones sécurisées doit être strictement limitée à l'employé auquel les clés ont été attribuées. Le prêt de clés, de codes de sécurité ou de badges d'accès de sécurité à des employés non PTI et/ou à des personnes extérieures est interdit.
- Le non-respect de la présente Politique peut être considéré comme une atteinte à la sécurité et peut faire l'objet de mesures disciplinaires.

7.4 Gestion des étrangers dans les locaux

- Si un étranger n'est pas accompagné d'un employé de Phoenix Tower, les employés contesteront la présence de l'étranger dans les locaux de l'organisation.

8. CONTROLE D'ACCES

Un élément fondamental de notre Politique de sécurité des informations est le contrôle de l'accès aux ressources d'information essentielles qui nécessitent une protection contre la divulgation ou la modification non autorisée. La signification fondamentale du contrôle d'accès est que les autorisations sont attribuées à des individus ou des systèmes autorisés à accéder à des ressources spécifiques. Des contrôles d'accès existent à différentes couches du système, y compris le réseau. Le contrôle d'accès est mis en œuvre par ID de connexion et mot de passe. Au niveau de l'application et de la base de données, d'autres méthodes de contrôle d'accès peuvent être mises en œuvre pour restreindre davantage l'accès. Les systèmes d'application et de base de données peuvent limiter le nombre d'applications et

de bases de données disponibles pour les utilisateurs en fonction des exigences de leur travail.

8.1 Système d'utilisateur et accès au réseau – Identification de l'utilisateur normal

Tous les utilisateurs devront avoir un ID de connexion et un mot de passe uniques pour accéder aux systèmes. Le mot de passe de l'utilisateur doit rester confidentiel et NE DOIT PAS être partagé avec le personnel de direction et de supervision et/ou tout autre employé que ce soit. Tous les utilisateurs doivent se conformer aux règles suivantes concernant la création et la maintenance des mots de passe :

- Le mot de passe doit être complexe. :
  - La longueur minimale d'un mot de passe doit être de 8 caractères.
  - Il doit être composé d'une combinaison de caractères alphanumériques (lettres majuscules et minuscules, chiffres et caractères spéciaux).
  - Alphabet minuscule.
  - Alphabet majuscule.
  - Symboles : . : { } ! @ # $ % ^ & * ? _ ~ -
  - Chiffres de 0 à 9.
  - Il ne doit pas contenir de caractères identiques consécutifs.
  - À titre de recommandation, le mot de passe ne doit pas être le même que l'un des 5 derniers mots de passe utilisés.
- Autrement dit, n'utilisez aucun nom commun, nom, verbe, adverbe ou adjectif. Ces mots de passe faciles peuvent être facilement piratés au moyen des « outils de piratage » standard.
- Les mots de passe ne doivent pas être affichés sur des terminaux informatiques ou à proximité de ceux-ci ou être facilement accessibles dans le terminal.
- Le mot de passe doit être modifié tous les 60 jours.
- Les comptes d'utilisateurs seront gelés après 5 tentatives de connexion infructueuses.
- Les identifiants de connexion et les mots de passe seront suspendus après 20 jours sans utilisation.

Les utilisateurs ne sont pas autorisés à accéder aux fichiers de mots de passe sur aucun composant d'infrastructure réseau. Les fichiers de mots de passe sur les serveurs seront surveillés contre l'accès par des utilisateurs non autorisés. La copie, la lecture, la suppression ou la modification d'un fichier de mot de passe sur tout système informatique est strictement interdite.

Les utilisateurs ne seront pas autorisés à se connecter en tant qu'administrateur système. Les utilisateurs qui ont besoin de ce niveau d'accès aux systèmes de production doivent demander un compte d'accès spécial comme indiqué ailleurs dans ce document.

Les identifiants de connexion et les mots de passe des employés seront désactivés dès que possible si l'employé est démis de ses fonctions, licencié, suspendu, mis en congé ou quitte d'une autre manière le bureau de la Société.

Les superviseurs/responsables doivent immédiatement et directement contacter le service informatique de la Société pour signaler tout changement de statut d'employé qui nécessite la résiliation ou la modification des privilèges d'accès des employés.

Les employés qui oublient leur mot de passe doivent appeler le service informatique ou suivre les outils fournis au service informatique pour obtenir un nouveau mot de passe attribué à leur compte. L'employé doit s'identifier par (par exemple, numéro d'employé) auprès du service informatique.

Les employés seront responsables de toutes les transactions se produisant pendant les sessions de connexion initiées par l'utilisation du mot de passe et de l'ID de l'employé. Les employés ne doivent pas se connecter à un ordinateur et permettre ensuite à une autre personne d'utiliser l'ordinateur ou de partager autrement l'accès aux systèmes informatiques.

8.2 Accès d'administrateurs système

Les administrateurs système, les administrateurs réseau et les administrateurs de sécurité disposeront d'un accès à privilèges élevés aux systèmes hôtes, routeurs, concentrateurs et pare-feu selon les besoins pour accomplir leurs tâches.

Tous les mots de passe d'administrateurs système seront **SUPPRIMÉS** immédiatement après que tout employé ayant accès à ces mots de passe soit démis de ses fonctions, licencié, ou ait quitté de toute autre manière l'emploi de la société. Les employés mis en congé administratif ou disciplinaire verront leur mot de passe suspendu jusqu'à ce que leur statut d'emploi actif soit rétabli.

8.3 Accès spécial

Des comptes d'accès spéciaux sont fournis aux personnes nécessitant des privilèges d'administrateurs système temporaires pour effectuer leur travail. Ces comptes sont surveillés par la Société et nécessitent l'autorisation du service informatique de la Société de l'utilisateur. La surveillance des comptes d'accès spéciaux se fait en saisissant les utilisateurs dans une zone spécifique et en générant périodiquement des rapports à la direction. Les rapports indiqueront qui possède actuellement un compte d'accès spécial, pour quelle raison et quand il expirera. Les comptes spéciaux expireront dans 2 jours et ne seront pas automatiquement renouvelés sans autorisation écrite.

8.4 Connexion à des réseaux tiers

La présente politique est établie pour garantir une méthode sécurisée de connectivité fournie entre la Société et toutes les Sociétés tierces et autres entités tenues d'échanger électroniquement des informations avec la Société.

Le terme « tiers » fait référence aux fournisseurs, consultants et partenaires commerciaux qui font des affaires avec la Société et à d'autres partenaires qui ont besoin d'échanger des

informations avec la Société. Les connexions réseau de tiers ne doivent être utilisées que par les employés des tiers, uniquement à des fins commerciales de la Société. La Société tierce s'assurera que seuls les utilisateurs autorisés seront autorisés à accéder aux informations sur le réseau de la Société. Le tiers ne permettra pas au trafic Internet ou à tout autre trafic de réseau privé de circuler dans le réseau de la Société. Une connexion réseau d'un tiers est définie comme l'une des options de connectivité suivantes :

- Une connexion réseau se terminera sur un pare-feu et le tiers sera soumis aux règles d'authentification standard de la société.

La présente politique s'applique à toutes les demandes de connexion tierces et à toutes les connexions tierces existantes. Dans les cas où les connexions réseau tierces existantes ne répondent pas aux exigences décrites dans ce document, elles seront conçues à nouveau selon les besoins.

Toutes les demandes de connexions tierces doivent être effectuées en soumettant une demande écrite et approuvées par le service informatique.

8.5 Connexion des dispositifs au réseau

Seuls les dispositifs autorisés peuvent être connectés au(x) réseau(s) de la Société. Les dispositifs autorisés comprennent les PC et les postes de travail appartenant à la Société qui sont conformes aux directives de configuration de la Société. Les autres dispositifs autorisés comprennent les dispositifs d'infrastructure réseau utilisés pour la gestion et la surveillance du réseau.

Les utilisateurs ne doivent pas se connecter au réseau : des ordinateurs n'appartenant pas à la Société qui ne sont pas autorisés, détenus et/ou contrôlés par la Société. Il est expressément interdit aux utilisateurs de connecter au réseau de la Société des dispositifs non-professionnels tels que des ordinateurs portables, des ordinateurs, des disques durs externes, des téléphones, des tablettes.

NOTE : les utilisateurs ne sont pas autorisés à connecter un dispositif qui modifierait les caractéristiques topologiques du réseau ou des dispositifs de stockage non autorisés (par exemple, des clés USB et des CD inscriptibles).

8.6 Accès à distance

Seules les personnes autorisées peuvent accéder à distance au réseau de la Société. L'accès à distance est fourni aux employés, entrepreneurs et partenaires commerciaux de la Société qui éprouvent un besoin commercial légitime d'échanger des informations, de copier des fichiers ou des programmes ou d'accéder à des applications informatiques. Les connexions autorisées peuvent être un PC distant vers le réseau ou un réseau distant vers une connexion réseau de la société. La seule méthode acceptable de connexion à distance au réseau interne consiste à utiliser un identifiant sécurisé.

8.7 Accès à distance non autorisé

La connexion de concentrateurs au PC ou à la station de travail d'un utilisateur qui est connecté au réseau local (LAN) de la Société, sans l'autorisation écrite de la Société, est interdite. De plus, les utilisateurs ne peuvent pas installer de logiciel personnel conçu pour fournir une commande à distance du PC ou de la station de travail. Ce type d'accès à distance contourne les méthodes d'accès à distance hautement sécurisées autorisées et constitue une menace pour la sécurité de l'ensemble du réseau.

9. REACTION AUX INCIDENTS ET RAPPORTS SUR LES VIOLATIONS DE DONNEES

En cas d'incident de sécurité, il est important que les employés de Phoenix Tower soient en mesure de s'identifier et de réagir de manière appropriée. Chaque incident potentiel fera l'objet d'une enquête à un niveau jugé approprié par les services juridiques et informatiques. Une réaction appropriée et opportune aux incidents de sécurité des informations contribuera à protéger les actifs de Phoenix Tower.

9.1 Rapports

- Chaque employé est responsable de signaler toutes les faiblesses identifiées ou soupçonnées de la sécurité des informations, y compris, mais sans s'y limiter, les violations de données PII potentielles ou réelles, immédiatement au service informatique et/ou juridique/de conformité :
    - Numéro vert : 1-844-348-5247 ou https://secure.ethicspoint.com
    - E-mail : privacy@phoenixintnl.com
- Une violation de la confidentialité ou une divulgation non autorisée des informations confidentielles de Phoenix Tower est également considérée comme un incident de sécurité des informations et doit être signalée comme indiqué ci-dessus.
- Le service informatique enregistrera les incidents de sécurité signalés pour surveiller à la fois les types d'incidents de sécurité et le volume d'incidents survenant au niveau de Phoenix Tower.
- Les preuves relatives à une violation de la sécurité des informations doivent être correctement collectées selon les instructions du responsable du service informatique et transmises au service informatique. Elles doivent être collectées pour se conformer aux obligations légales, réglementaires ou contractuelles et éviter les violations de droit pénal ou civil.
- Après avoir mené une première enquête, le responsable du service informatique déterminera si l'événement est effectivement un incident de sécurité des informations. Si un incident de sécurité s'est produit, le service juridique déterminera si l'incident constitue une violation de données pour laquelle un signalement est requis, et des violations de données impliquant des PII.
- Le service juridique conservera un registre des incidents de sécurité signalés qui

constituent une violation de données.

- Les informations relatives aux incidents de sécurité des informations ne peuvent être divulguées que par des personnes autorisées. Les employés ne peuvent divulguer aucune information concernant un incident de sécurité en dehors de PTI sans l'autorisation expresse de l'équipe juridique.
- À la suite de l'incident ou de la violation de données, le service informatique sera chargé d'organiser une réunion avec tous les employés et parties concernés/applicables pour examiner les résultats de l'enquête et discuter de la cause profonde de l'incident. Tous les employés impliqués dans la découverte ou l'enquête sur
- un incident de sécurité sont tenus d'assister à cette réunion.
- Les employés de Phoenix Tower ou les entrepreneurs tiers impliqués dans un incident de sécurité ou ayant enfreint la Politique de sécurité des informations de Phoenix Tower, quelle que soit leur intention, feront face à un comité disciplinaire, qui déterminera la faute, les mesures correctives et d'autres mesures appropriées.

9.2 Notification de violation de données

- **Notification à l'autorité de contrôle :** PTI, en tant que responsable du traitement, notifie immédiatement l'autorité nationale de contrôle (dès qu'elle prend connaissance de l'incident) et, au plus tard, dans les 72 heures suivant la connaissance de l'incident, y compris les heures écoulées pendant les week-ends et jours fériés. Pour la communication, PTI doit utiliser le formulaire de notification, par pays, fourni dans **la procédure de gestion des incidents**.

- **Notification des personnes concernées :** PTI, en tant que responsable de traitement, doit informer les personnes concernées des failles de sécurité lorsque la violation pourrait avoir un impact négatif sur leurs données personnelles ou leur vie privée.

10. CONFIDENTIALITÉ PAR CONCEPTION

PTI s'engage à adopter les mesures techniques et organisationnelles nécessaires pour concrétiser les dispositions et principes de protection des données et ainsi garantir les droits des personnes concernées. Pour ce faire, le PTI doit envisager l'adoption des mesures juridiques, techniques et organisationnelles nécessaires dès la phase de développement et de conception des produits et services ou à partir du moment initial où tout projet, initiative ou idée impliquant le Traitement de Données personnelles est proposé par le PTI.

Pour la mise en œuvre de mesures légales, le responsable des questions de protection des données doit être consulté, et pour les mesures techniques et organisationnelles, le chef du service informatique doit être consulté.

À cette fin, chaque responsable de domaine, de projet ou de nouveau processus doit s'assurer que la confidentialité est mise en œuvre par conception et par défaut, en plus de respecter les principes de base de la réglementation.

11. MESURES DE SECURITE SUPPLEMENTAIRES

Pour protéger l'intégrité, la confidentialité et la disponibilité des informations, PTI a mis en place les mesures de sécurité suivantes :

11.1 Détection et gestion des vulnérabilités et des logiciels malveillants.

En relation avec le processus continu de détection et de gestion des vulnérabilités, cette mesure de sécurité est mise en œuvre pour identifier, évaluer, traiter et signaler les vulnérabilités de sécurité dans les systèmes. À cette fin, PTI a mis en place les outils Microsoft Defender et Zscaler pour la détection et la gestion des vulnérabilités et des logiciels malveillants.

11.2 Politique de gestion des correctifs

En ce qui concerne la gestion des correctifs, PTI a développé une politique de gestion des correctifs, qui stipule que les correctifs publiés par Microsoft seront installés en tant qu'Intune, Zero day. Contrôle d’accès au réseau.

11.3 Mécanismes de chiffrement

En ce qui concerne les mécanismes de cryptage, PTI a mis en place de tels mécanismes, à la fois dans la base de données et sur le disque dur des ordinateurs portables. De cette façon, les informations stockées sur les appareils ne sont pas accessibles en cas d'accès non autorisé. Des mécanismes de cryptage sont utilisés, à la fois dans les bases de données et dans le disque dur des ordinateurs portables. Dans ce cas, un mécanisme d'effacement a été mis en place, en cas de perte ou de vol de matériel qui en plus des mesures de sécurité de cryptage des données, un effacement à distance peut être effectué.

11.4 Gestion des comptes.

En relation avec la gestion des comptes. PTI a mis en place des mécanismes appelés Privileged Identity Management (PIM) et Privileged Access Management (PAM).