CHARTE INFORMATIQUE

1 PREAMBULE

- La présente charte informatique (la « **Charte** »), vise à régir l'utilisation du système d'information et de communication nécessaire à l'activité des sociétés du groupe Groupe Triomphe Sécurité (ci-après le « **Groupe** »), dont Monsieur Walid Nahra[i] est le représentant, incluant la société tête de pont Groupe Triomphe Sécurité[ii], et ses filiales, les sociétés Triomphe Sécurité[iii], Groupe Etoile Protection[iv], Etoile Protection[v], Exit Conseil[vi], Triomphe Welcome Events[vii], Triomphe Elite Guard[viii], Triomphe Events and Protection[ix], Triomphe Haute Protection[x] et Cèdre Racing Team[xi].

  Dans le cadre de la Charte, le terme « **Utilisateur** » désigne toutes personnes qui utilise les systèmes d'information et de communication du Groupe, ainsi que ses équipements informatiques, quel que soit son statut, tel que listées à l'article 2.1 ci-après.

- Le Groupe met en œuvre un système d'information et de communication, comprenant notamment un réseau informatique et téléphonique, ainsi que des outils mobiles, tels que listés à l'article 2.2 ci-après. **L'utilisation du système d'information et de communication du Groupe doit se faire exclusivement à des fins professionnelles, sauf exception prévue** dans la Charte.

  Dans un but de transparence à l'égard des Utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et de communication du Groupe, la Charte pose les règles relatives à l'utilisation de ces ressources.

---

[i] *En sa qualité notamment de Président de Groupe Triomphe Sécurité.*
[ii] *Groupe Triomphe Sécurité, SAS au capital de 2.192.140 € sise 41-45, boulevard Romain Rolland 75014 Paris et enregistrée au RCS de Paris sous le numéro 507 630 366.*
[iii] *478 951 080 R.C.S. Paris.*
[iv] *507 670 933 R.C.S. Evry.*
[v] *485 047 385 R.C.S. Evry.*
[vi] *489 471 672 R.C.S. Evry.*
[vii] *508 763 695 R.C.S Paris.*
[viii] *827 836 081 R.C.S. Paris.*
[ix] *821 320 868 R.C.S. Paris.*
[x] *844 516 740 R.C.S. Paris.*
[xi] *908 569 668 RCS Paris.*

WN

- **La Charte a pour objectifs** :

  i) **sensibiliser les Utilisateurs aux risques** liés à la sécurité informatique en matière de libertés et de vie privée, notamment à travers les traitements de données à caractère personnel qu'ils sont amenés à effectuer ;

  ii) **d'informer** les Utilisateurs sur :

  - les **usages** permis des moyens informatiques mis à sa disposition ;
  - les règles de **sécurité** en vigueur ;
  - les mesures de **contrôle** prises par le Groupe ;
  - les **sanctions** éventuellement encourues par les Utilisateurs ;

  iii) de **formaliser les règles générales de sécurité** que les Utilisateurs s'engagent à respecter, en contrepartie de la mise à disposition des systèmes d'information et des équipements informatiques du Groupe, et ainsi de déterminer les droits et devoirs des utilisateurs.

  Elle permet ainsi de **réduire les difficultés relatives à la preuve des abus d'usage** du système d'information et de communication, les Utilisateurs étant informés des règles d'utilisation et de la mise en place éventuelle de moyens de surveillance.

  Elle dispose d'un aspect réglementaire et est **annexée au règlement intérieur du Groupe**. Elle ne remplace en aucun cas les lois en vigueur que nul n'est censé ignorer.

  Ces règles s'inscrivent dans une démarche responsable afin de protéger d'une part le patrimoine informationnel et l'image de marque du Groupe, et d'autre part les libertés et la vie privée des Utilisateurs et des tiers en lien avec le Groupe (salariés, prestataires externes, partenaires…).

2 CHAMP D'APPLICATION

2.1 Utilisateurs concernés

Sauf mention contraire, la Charte s'applique à tous les Utilisateurs réguliers ou occasionnels du système d'information et de communication du Groupe, quel que soit leur statut, y compris notamment les mandataires sociaux, salariés, intérimaires, stagiaires, employés de sociétés prestataires, visiteurs occasionnels. Le cas échéant, la Charte sera annexée aux contrats de prestations.

Les Utilisateurs veillent à faire accepter valablement les règles posées dans la Charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

2.2 Système d'information et de communication du Groupe

Le système d'information et de communication du Groupe est notamment constitué des éléments suivants :

- ordinateurs (fixes ou portables) ;
- périphériques y compris clés USB ;
- assistants personnels ;
- réseau informatique (serveurs, routeurs et connectique) ;
- photocopieurs ;
- télécopieurs ;
- téléphones ;

WN

- smartphones ;
- tablettes et clés 3G ;
- logiciels ;
- fichiers ;
- données et bases de données ;
- système de messagerie ;
- connexion internet ;
- intranet ;
- extranet ;
- abonnements à des services interactifs ;
- I-COMETE ;
- Plateformes GSAO et GSAO ;
- main courante électronique ;
- toute autre plateforme à laquelle pourrait avoir accès les Utilisateurs dans le cadre de leurs activités pour le Groupe et, notamment, les plateformes de pointage, étant entendu que toutes les plateformes relèvent du Règlement Général sur la Protection des Données (« **RGPD** »).

2.3 Règles relatives à l'installation de matériels externes et de logiciels

- En règle générale, aucun matériel périphérique (i.e. clés USB, disques durs externes, lecteurs de musique, etc.) ne doit être connecté aux matériels du réseau local du Groupe et encore moins installé sur ceux-ci. Il en va de même pour les logiciels non connus du Groupe.

- Il est également **interdit de connecter un matériel du Groupe sur un réseau extérieur**. Seul l'administrateur du réseau local du Groupe peut valider une telle demande après avoir pris toutes les précautions d'usage afin de garantir l'intégrité du réseau.

- **L'utilisation du matériel personnel (smartphone, tablette, ordinateur portable, etc.) à des fins professionnelles** est possible uniquement dans le cadre du télétravail. Un **compartiment hermétique dit « professionnel » devra être aménagé sur les appareils personnels des Utilisateurs** afin de recueillir les applications, fichiers et usages professionnels. Aucune donnée à caractère personnel ne doit être intégrée dans ce compartiment dédié aux activités professionnelles, et le contrôle du Groupe ne pourra s'effectuer qu'au sein de ce compartiment « professionnel ».

2.4 Autres accords sur l'utilisation du système d'information

La Charte est sans préjudice des accords particuliers pouvant porter sur l'utilisation du système d'information et de communication du Groupe par les institutions représentatives, l'organisation d'élections par voie électronique ou la mise en télétravail des Utilisateurs.

3 CONFIDENTIALITE

3.1 Paramètres d'accès au système d'information et de communication

- L'accès à certains éléments du système d'information du Groupe (i.e. messagerie électronique ou téléphonique, sessions sur les postes de travail, réseau, certaines applications ou services interactifs) est **protégé par des paramètres de connexion** (i.e. identifiant, mot de passe).

- Ces paramètres sont **personnels à l'Utilisateur et pourraient être gardés confidentiels**. Ils permettent en particulier d'identifier toute personne utilisant un ordinateur et de contrôler son activité.

WN

Ils ne peuvent, sauf avec l'accord expresse de l'Utilisateur, être communiqués. Dans la mesure du possible, ces paramètres doivent être mémorisés par l'Utilisateur et ne pas être conservés, sous quelque forme, notamment écrite, que ce soit. En tout état de cause, **ils ne doivent pas être transmis à des tiers ou être aisément accessibles**. Ils doivent être saisis par l'Utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

- L'Utilisateur est personnellement responsable de l'utilisation qui peut en être faite, notamment au regard des données du Groupe.

  Aucun Utilisateur ne doit se servir, pour accéder au système d'information du Groupe, d'un autre compte que celui qui lui a été attribué. Il ne doit pas non plus déléguer à un tiers les droits d'utilisation qui lui sont attribués.

- Lorsqu'ils sont choisis par l'Utilisateur, ces paramètres doivent respecter un certain degré de complexité. Un mot de passe doit, pour être efficace, comporter au moins huit caractères alphanumériques. Il ne doit pas être, notamment, identique au login, même en inversant les caractères, comporter le nom et/ou prénom de l'Utilisateur ou de membres de sa famille, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l'Utilisateur, être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu.

- Les **mots de passe permettant d'accéder aux serveurs doivent être couplés avec un service de double authentification** basé sur une application standard compatible avec tous systèmes. Dans l'hypothèse où l'Utilisateur ne dispose pas de téléphone professionnel, un boitier doit lui être fourni s'il ne souhaite pas utiliser son smartphone personnel.

- Le Groupe, du fait de son activité, recourt à certains logiciels **spécifiques et notamment le logiciel Comète**.

3.2 Données

Chaque Utilisateur est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Les règles de confidentialité ou d'autorisation préalable avant diffusion externe ou publication sont définies par le Groupe et applicables quel que soit le support de communication utilisé.

L'Utilisateur doit être particulièrement vigilant sur le risque de divulgation de ces informations dans le cadre d'utilisation des outils informatiques professionnels dans des lieux autres que ceux de du Groupe (hôtels, lieux publics, etc.).

4 SECURITE

4.1 Rôle de du Groupe

Le Groupe met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. À ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des Utilisateurs.

Le Service Informatique, entendu au sens du terme comme le responsable informatique, est responsable du contrôle du bon fonctionnement du système d'information et de communication. Il doit prévoir un plan de sécurité et de continuité du service, en particulier en cas de défaut matériel. Il veille à l'application des règles de la Charte. Les membres du Service Informatique sont assujettis à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître.

WN

4.2 Rôle de l'Utilisateur

- L'Utilisateur est **responsable quant à lui des ressources** qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection desdites ressources, en faisant preuve de prudence et de vigilance.

  En particulier, il doit signaler à la direction informatique toute violation ou tentative de violation de l'intégrité de ces ressources, et, de manière générale tout dysfonctionnement, incident ou anomalie.

  De même, la sortie, à l'extérieur des locaux du Groupe ou des lieux d'activité professionnelle des Utilisateurs pour le Groupe, de matériel appartenant au Groupe doit être justifiée par des obligations professionnelles et nécessite l'accord exprès de la direction.

  En cas d'absence, même temporaire, il est impératif que l'Utilisateur **verrouille l'accès** au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

- L'Utilisateur doit effectuer des **sauvegardes régulières** des fichiers dont il dispose sur le matériel mis à sa disposition en suivant les procédures définies par le Service Informatique. Il doit régulièrement supprimer les données devenues inutiles sur les espaces communs du réseau ; les données anciennes mais qu'il souhaite conserver doivent être archivées avec l'aide du Service Informatique.

  L'Utilisateur doit **éviter d'installer ou de supprimer des logiciels**, de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein du Groupe. Il ne doit pas non plus modifier les paramétrages de son poste de travail ou des différents outils mis à sa disposition, ni contourner aucun des systèmes de sécurité mis en œuvre au sein du Groupe. Il doit dans tous les cas en alerter le Service Informatique.

- L'Utilisateur doit en toutes circonstances se conformer à la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité concurrente à celle du Groupe ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication du Groupe.

5 INTERNET

5.1 Accès aux sites

- La connexion Internet mise à disposition des Utilisateurs doit être **utilisée à des fins professionnelles**. L'utilisation d'Internet à des fins privées est tolérée dans des **limites raisonnables** et à condition que la navigation n'entrave pas l'accès professionnel.

- Pour des raisons de sécurité ou de déontologie, **l'accès à certains sites peut être limité ou prohibé** par le Service Informatique. Ce dernier est habilité à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites et/ou restreignant le téléchargement de certains fichiers.

  L'utilisation d'Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives est strictement interdite. Il est aussi prohibé de

WN

créer ou mettre à jour au moyen de l'infrastructure du Groupe tout site Internet, notamment des pages personnelles.

- Il est interdit de se connecter à des sites Internet dont la consultation est prohibée par la loi (notamment, les publications à caractère injurieux, raciste, pornographique, pédophile, diffamatoire, sur le harcèlement sexuel/moral, etc.) ou dont le contenu est contraire à l'ordre public, aux bonnes mœurs, aux intérêts et/ou à la réputation du Groupe, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information du Groupe ou engageant financièrement celui-ci.

5.2 Autres utilisations

- Chaque Utilisateur doit prendre conscience **qu'il est dangereux pour le Groupe** :

  i) de communiquer à des tiers des informations techniques concernant son matériel ;
  ii) de connecter un micro à Internet par le biais d'un modem (sauf autorisation spécifique) ;
  iii) de diffuser des informations sur le Groupe par le biais de sites Internet ;
  iv) de participer à des forums (même professionnels) ;
  v) de participer à des conversations en ligne (« chat »).

  La contribution des Utilisateurs à des forums de discussion, systèmes de discussion instantanée, chats, blogs, sites n'est donc **autorisée qu'à titre professionnel et sur autorisation expresse du Service Informatique.**

- De même, **tout téléchargement de fichier, en particulier de fichier média, est prohibé**, sauf justification professionnelle dûment validée par le Service Informatique.

- Il est rappelé que les Utilisateurs ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte aux intérêts du Groupe ou à la sécurité de son système d'information et de communication.

  Les Utilisateurs sont informés que **le Service Informatique enregistre leur activité sur Internet** et que ces traces pourront être exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi, en particulier en cas de perte importante de bande passante sur le réseau du Groupe.

6 MESSAGERIE ELECTRONIQUE

- La messagerie électronique est un moyen d'amélioration de la communication au sein du Groupe et avec les tiers. L'Utilisateur dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique normalisée attribuée par le Service Informatique.

- Les messages électroniques reçus sur la messagerie professionnelle de l'Utilisateur font l'objet d'un **contrôle antiviral et d'un filtrage anti-spam**. Les Utilisateurs sont invités à informer le Service Informatique des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

6.1 Conseils généraux

- L'attention des Utilisateurs est attirée sur le fait qu'un message électronique **a la même portée qu'un courrier postal**. Il obéit donc aux mêmes règles d'envoi, en particulier en matière d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à l'autorité hiérarchique.

WN

- Un message électronique peut être communiqué très rapidement à des tiers. Il convient donc de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information et de communication du Groupe, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale du Groupe et/ ou des Utilisateurs.

  - Avant tout envoi, il est impératif de **bien vérifier l'identité des destinataires** du message et leur **qualité à recevoir communication des informations transmises**.

  - **Aucune information stratégique** (à caractère confidentiel) ne doit circuler de cette manière, sauf accord de la direction du Groupe. En présence de telles informations, les vérifications mentionnées à l'alinéa précédent devront être renforcées, toute erreur pouvant être sanctionnée.

  - **En cas d'envoi à une pluralité de destinataires**, l'Utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités.

    Il doit également **envisager l'opportunité de dissimuler certains destinataires**, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires.

    En cas d'envoi à une liste de diffusion, il est important de **vérifier la liste des abonnés** à celle-ci, l'existence d'archives accessibles par le public et les modalités d'abonnement.

  - Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes. Les **messages importants doivent donc être envoyés avec un accusé de réception**. Ils doivent, **le cas échéant, être doublés** par un envoi de fax ou de courrier postal.

  - Les Utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent pas comporter d'éléments illicites, tels que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire, des atteintes à l'ordre public ou à la dignité humaine, etc.

- La forme des messages professionnels doit respecter les règles définies par la direction, pour ce qui concerne la mise en forme et la signature des messages.

  En cas d'absence supérieure à 3 jours, l'Utilisateur doit mettre en place un **message automatique d'absence.**

6.2 Limites techniques

- Pour des raisons techniques, l'envoi de messages électroniques n'est possible, directement, que vers un **nombre limité de destinataires**, fixé par le Service Informatique. Cette limite est susceptible d'être levée temporairement ou définitivement sur demande adressée au Service Informatique.

  De même, le Service Informatique peut **limiter la taille**, le nombre et le type des pièces jointes pour éviter l'engorgement du système de messagerie.

WN

- Pour des raisons de **capacité mémoire**, les messages électroniques sont conservés chez un prestataire à des fins d'archivage. La durée de conservation est convenue avec le prestataire.

  Sur les serveurs du Groupe, les messages électroniques sont sauvegardés et restaurables pendant 10 (dix) jours maximum. En cas de départ d'un Utilisateur, une copie des messages électroniques à usage d'archivage peut être faite et conservée sur les serveurs du Groupe.

  Passé les délais visés au paragraphe précédent, les messages pourront être supprimés. Si l'Utilisateur souhaite conserver des messages au-delà de ce délai, il lui appartient d'en faire des sauvegardes avec l'aide du Service Informatique si nécessaire. Pour des raisons opérationnels, il est possible de conserver les messages de certains Utilisateurs.

6.3 Utilisation de la messagerie à titre personnel

- La messagerie doit être utilisée à des fins professionnelles et tout message envoyé ou reçu depuis le poste de travail fourni par le Groupe est présumé être de nature professionnelle.

- Toutefois, au vu du principe de proportionnalité, l'utilisation de la messagerie professionnelle à titre personnel est tolérée, à condition d'être raisonnable ; ce qui sous-entend que cet usage ne doit pas altérer le bon fonctionnement du Groupe (en ce compris l'intégrité de son réseau informatique et la productivité des Utilisateurs).

  Les messages envoyés à titre personnel doivent être signalés par la mention "Privé" ou "Personnel" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon. Les messages personnels reçus doivent également être classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Personnel". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

6.4 Utilisation de la messagerie par la délégation du personnel

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent également être **signalés et classés** dans un dossier dédié, en utilisant la **mention "Délégué"** dans leur objet à l'émission et dans le dossier où ils doivent être classés.

7 TELEPHONIE

- Pour leur activité professionnelle, les Utilisateurs peuvent disposer d'un poste fixe et/ou d'un terminal mobile, smartphone, tablette ou clé 3G.

- Pour ce qui est de l'utilisation des terminaux mobiles en connexion pour accès à des sites Internet ou à la messagerie électronique, les règles édictées ci-dessus s'appliquent de la même manière.

  De plus, il est rappelé que l'envoi de SMS est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel. Il est donc soumis aux règles énoncées plus haut.

  Enfin, les connexions depuis l'étranger sont strictement interdites sauf autorisation exceptionnelle de la hiérarchie en cas de nécessité professionnelle.

- L'utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, **à condition qu'elle reste raisonnable** en termes de temps passé et de quantité d'appels. Les surcoûts pour le Groupe engendrés par l'utilisation de la téléphonie à des fins personnelles devront être

WN

remboursés par les Utilisateurs concernés. Il s'agit tout particulièrement des appels à des numéros surtaxés et des appels depuis l'étranger ou à destination de l'étranger, au sens de la facturation téléphonique.

- Les Utilisateurs sont informés que le Service Informatique **enregistre leur activité téléphonique, aussi bien sur les postes fixes que sur les mobiles**. Ces données seront exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi. Toutefois, seule la direction pourra avoir accès aux numéros détaillés, permettant d'identifier les interlocuteurs d'un Utilisateur, et seulement en cas de différend avec lui.

8 DONNEES PERSONNELLES

La Loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, dite Loi Informatique et Libertés, l'ordonnance n°2018-1125 du 12 décembre 2018, ainsi que le Règlement général sur la protection des données (RGPD) viennent définir les conditions dans lesquelles des traitements de données à caractère personnel peuvent être opérés.

La Loi Informatique et Libertés et le RGPD instituent des droits, au profit des personnes concernées par les traitements réalisés par les Utilisateurs, que la Charte invite à respecter, tant à l'égard des Utilisateurs que des tiers.

A cet égard, les Utilisateurs s'engagent à :

- ne pas utiliser les données à caractère personnel auxquelles ils peuvent accéder à des fins autres que celles prévues par leurs attributions ;

- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;

- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de leurs fonctions ;

- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de leurs attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;

- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;

- assurer, dans la limite de leurs attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;

- ne pas accéder, tenter d'accéder ou supprimer les données en dehors de leurs attributions ;

- respecter les droits des personnes concernées (droit d'accès, de rectification, d'opposition, effacement...) conformément aux procédures mises en place par le Groupe ;

- en cas de cessation de leurs fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données ;

- respecter l'ensemble des procédures liées à la protection des données mises en place par le Groupe, et à respecter et favoriser l'ensemble des mesures techniques et organisationnelles mises en place par le Groupe afin de se conformer à la réglementation applicable.

WN

Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle, prévus dans la Charte. Ils sont, en tant que de besoin, déclarés conformément à la loi du 6 janvier 1978. Tout Utilisateur pourra avoir accès aux données le concernant sur une période maximale d'un an.

Le **CPO du Groupe est l'interlocuteur de référence** pour toute information complémentaire concernant le traitement des données personnelles de l'Utilisateur. Ses coordonnées sont les suivantes : **cpo@triomphe-securite.fr**.

Il est rappelé aux Utilisateurs que les traitements de données à caractère personnel doivent être déclarés à la Commission nationale de l'informatique et des libertés, en vertu de la loi n°78-17 du 6 janvier 1978. Les Utilisateurs souhaitant réaliser, dans le cadre professionnel, des traitements relevant de ladite loi sont invités à prendre contact avec le CPO avant d'y procéder.

Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée et au Règlement européen n°2016/679/UE du 27 avril 2016 (applicable depuis le 25 mai 2018), les salariés de l'entreprise bénéficient d'un droit d'accès, de rectification, de portabilité et d'effacement de leurs données personnelles ou encore de limitation de leur traitement. Ils peuvent également, pour des motifs légitimes, s'opposer au traitement des données les concernant. La collecte et le traitement de ces données personnelles permettent à l'entreprise d'effectuer la gestion du personnel, des paies, des formations conformément aux règlementations qui nous sont imposées dans le cadre du contrat de travail liant l'entreprise aux salariés. Les données personnelles des salariés sont protégées par un ensemble de mesures, et la société s'engage à informer le(s) salarié(s) en cas d'accès non autorisé, dans les plus brefs délais et par tout moyen mis à disposition de l'entreprise.

Parallèlement, le personnel de l'entreprise peut être amené à détenir pour des raisons de sécurité et d'exploitation, des données personnelles des sociétés clientes de l'entreprise ou du groupe, des usagers des sites, prestataires ou salariés de ces mêmes sociétés clientes. S'agissant de ces données, le personnel est tenu de respecter les mêmes obligations en matière de données personnelles.

9 CESSATION DE L'UTILISATION

Lors de son départ du Groupe, l'Utilisateur doit respecter la procédure de départ et restituer l'ensemble des moyens informatiques et de communication électronique qui lui ont été remis (ordinateur, périphériques, mobile, carte d'accès, moyen d'authentification à distance, badges, supports de stockage, etc.) en bon état général de fonctionnement et ne conserver aucun matériel ou aucune donnée permettant d'accéder au système d'information et de communication du Groupe. De plus, l'Utilisateur s'interdit, avant son départ, de détruire des informations et des données professionnelles.

Sauf nécessité liée à la continuité du service et pour un temps raisonnable au regard de l'exploitation, le **compte messagerie de l'Utilisateur est supprimé le jour de son départ**.

Dans le cas où le compte messagerie est toujours actif, même après le départ d'un Utilisateur, une redirection des messages peut être mise en place par le Groupe vers l'Utilisateur ayant repris le poste de l'Utilisateur ayant quitté le Groupe ou toute autre personne occupant une fonction similaire.

Ses **identifiants sont également désactivés**.

Sauf dérogation accordée au cas par cas par le responsable des systèmes d'information du Groupe et qui ne peut en aucun cas excéder une durée de 30 jours, les éléments marqués « privé » ou « personnel » doivent être supprimés par l'Utilisateur au plus tard la veille de son départ du Groupe.

10 CONTROLE DES ACTIVITES PAR LE GROUPE

WN

10.1 Contrôles automatisés

- Le système d'information et de communication du Groupe **s'appuie sur des fichiers journaux ("logs"), créés en grande partie automatiquement** par les équipements informatiques et de télécommunication du Groupe. Ces fichiers sont stockés sur les postes informatiques et sur le réseau du Groupe. Ils permettent d'assurer le bon fonctionnement du système, en **protégeant la sécurité** des informations du Groupe, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des Utilisateurs et des tiers accédant au système d'information.

- L'attention des Utilisateurs est attirée sur le fait **qu'il est ainsi possible de contrôler leur activité** et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

  Il est précisé que **chaque Utilisateur pourra avoir accès aux informations enregistrées** lors de ces contrôles le concernant sur demande préalable à la direction. De plus, les fichiers journaux énumérés ci-dessus sont **automatiquement détruits dans un délai maximum de 6 mois** après leur enregistrement.

  Sont notamment surveillées et conservées les données relatives aux éléments suivants :

  ❖ <u>Messagerie électronique</u>

  Dans l'hypothèse la plus courante, le contrôle éventuellement mis en œuvre porte sur :
  - ✓ le nombre des messages échangés ;
  - ✓ la taille des messages échangés ;
  - ✓ le format des pièces jointes ;
  - ✓ les destinataires.

  ❖ <u>Accès Internet</u>

  Dans l'hypothèse la plus courante, les contrôles portent sur :
  - ✓ les durées des connexions ;
  - ✓ les sites les plus visités ;
  - ✓ en cas d'abus, le Groupe pourra mettre en œuvre un contrôle visant à contrôler le bon usage de l'Internet.

  ❖ <u>Filtrage des accès Internet</u>

  Les **pares-feux vérifient tout le trafic sortant du Groupe**, aussi bien local que distant. Ils vérifient également le **trafic entrant** constitué des échanges de la messagerie électronique, de l'échange de fichiers ainsi que la navigation Internet.

  Ils **détiennent toutes les traces de l'activité qui transite par eux**, s'agissant :

  - ✓ **de la navigation sur Internet** : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels) ;
  - ✓ **des messages envoyés et reçus** : expéditeur, destinataire(s), objet, nature de la pièce jointe (et éventuellement texte du message).

  Ils filtrent les URL (Universal Resource Locator) des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont notamment les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste, ou contenant des données jugées comme offensantes.

WN

❖ Sauvegardes

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations et un dispositif miroir destiné à doubler le système en cas de défaillance.

Ceci implique, entre autres, que **la suppression par un Utilisateur d'un fichier de son disque dur n'est pas absolue et qu'il en reste une copie** :

- ✓ sur le dispositif de sauvegarde ou miroir ;
- ✓ sur le serveur ;
- ✓ sur le proxy ;
- ✓ sur le firewall (pare-feu) ;
- ✓ chez le fournisseur d'accès.

10.2 Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le Service Informatique, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs Utilisateurs.

Le contrôle concernant un Utilisateur peut porter sur les fichiers contenus sur le **disque dur** de l'ordinateur, sur un **support de sauvegarde** mis à sa disposition ou sur le **réseau** du Groupe, ou sur sa **messagerie**.

Dans ce cas, sauf risque ou événement particulier, la direction ne peut ouvrir les fichiers ou messages identifiés par l'Utilisateur comme personnels ou liés à la délégation de personnel conformément à la Charte, qu'en présence de l'Utilisateur ou celui-ci dûment appelé et éventuellement représenté par un délégué du personnel.

11 INFORMATION DES UTILISATEURS ET OPPOSABILITE DE LA CHARTE

La Charte est affichée publiquement en **annexe du règlement intérieur**.

La Charte et l'ensemble des règles techniques sont **disponibles sur le dossier Comète**.

Elle est pleinement opposable aux Utilisateurs à compter de sa publication et/ou de sa transmission.

Le Service Informatique est à la disposition des Utilisateurs pour leur fournir toute information concernant l'utilisation du système d'information et de communication du Groupe, en particulier sur les procédures de sauvegarde et de filtrage. Elle les informe régulièrement sur l'évolution des limites techniques du système d'information et de communication du Groupe ainsi que sur les menaces susceptibles de peser sur sa sécurité.

Chaque Utilisateur doit se conformer aux procédures et règles de sécurité édictées par le Service Informatique dans le cadre de la Charte.

En cas de besoin, les Utilisateurs pourront être formés par le Service Informatique pour appliquer les règles d'utilisation du système d'information et de communication prévues.

12 SANCTIONS

Il est rappelé que la Charte est un document à portée juridique, et donc contraignante pour les Utilisateurs.

WN

En effet, **tout manquement aux règles et mesures de sécurité décrites dans la Charte est susceptible d'engager la responsabilité de l'Utilisateur** et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication du Groupe, voire des sanctions disciplinaires, proportionnées à la gravité des faits constatés. Dans ce dernier cas, les procédures prévues dans le règlement intérieur et dans le Code du travail seront appliquées.

L'utilisation reconnue à des fins personnelles de certains services payants à travers le système de communication du Groupe donnera lieu à remboursement de la part de l'Utilisateur concerné.

Le Groupe ou son représentant légal, se réserve également le droit d'engager ou de faire engager des poursuites pénales indépendamment des sanctions disciplinaires mises en œuvre, notamment en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret des correspondances.

Le responsable des systèmes d'information et de communication du Groupe peut effacer ou isoler et conserver aux fins de preuve toute trace de logiciels, progiciels, programmes ou fichiers créés ou introduits dans le système d'Information du Groupe, en violation des droits des tiers, notamment de propriété intellectuelle, et dénoncer tout acte délictueux aux autorités, sans préjudice de l'application de sanctions dans le cadre de son statut.

13 ENTREE EN VIGUEUR

La Charte est applicable à compter du 04/08/2022

Elle a été adoptée après information et consultation du CSE en date du 28 juin 2022
Elle a été déposée au conseil des prud'hommes de Paris le 4 juillet 2022.

Walid NAHRA
Président

Le 4 juillet 2022

TRIOMPHE SECURITE
182 rue de Vaugirard 75015 PARIS
Tél. : 01 48 24 27 72
SIRET 478 951 080 00033 - Code APE 8010Z
AUT-075-2112-12-04-20130360188
Article L612-14 du LIVRE VI DU CSI - L'autorisation d'exercice ne confère aucune prérogative de puissance publique à l'entreprise ou aux personnes qui en bénéficient

WN