POLITIQUE DE SECURITE DE L'INFORMATION INNOHA

09/04/2025

Votre contact :
Ronan MORICE – Responsable d'Affaires
Directeur des Opérations
INNOHA
rmorice@INNOHA.com
+33 (0)6 88 01 65 79
8, rue de Berri,
75008 Paris

SOMMAIRE

A. AVANT PROPOS

Nos engagements, tels qu'ils sont synthétisés dans cette « Politique de sécurité de l'information », ont pour ambition de vous détailler les dispositions mises en œuvre par Innoha visant à assurer la sécurité des données de nos clients et les règles d'usage des moyens électroniques, informatiques et de communication.

Construite de façon à répondre au mieux à vos exigences et être en tous points compliant à vos pratiques et à votre modèle opérationnel, notre charte est également largement fondée sur nos expériences en matière de mise à disposition de ressources chez nos clients.

Soucieux des exigences en matière de sécurité de nos Clients comme de nos acheteurs, nous nous employons quotidiennement à déployer les méthodes, outils et processus les plus rigoureux, afin de garantir la mise en œuvre des solutions et prestations de services compliants aux spécificités de nos donneurs d'ordre et de l'ensemble de leurs parties prenantes

B. CHARTE INFORMATIQUE INNOHA

CONTEXTE

Cette charte (la « Charte ») s'applique à tout utilisateur[1] (i) des moyens électroniques ou informatiques et des moyens de communication (la messagerie ou les plateformes collaboratives notamment) de Innoha ou de ses filiales (l'ensemble ci-après indifféremment dénommé « Innoha » ou le « Groupe ») ainsi que (ii) des moyens électroniques ou informatiques ou de communication qui ne sont pas mis à sa disposition par Innoha et utilisés dans le cadre de ses activités professionnelles.

D'une façon générale, les moyens électroniques, informatiques et de communication de Innoha sont composés de tous les outils informatiques et/ou de télécommunication mis à la disposition des utilisateurs.

Ainsi, ils sont notamment constitués des éléments suivants :

- Les ordinateurs fixes et portables,
- Les périphériques : imprimantes, photocopieurs, fax, clés USB, assistants personnels,
- Le réseau informatique : serveurs, routeurs et connectique,
- Les services intranet, Internet, les systèmes de messagerie, plateformes collaboratives, abonnements à des services interactifs,
- Les téléphones fixes et les téléphones mobiles permettant ou non de se connecter au SI,
- Les logiciels et les fichiers : tous les logiciels, fichiers, données et bases de données,
- Les moyens mis en œuvre dans le cadre du télétravail (ordinateur, téléphone, réseau informatique, connexion à l'intranet, l'Internet, aux systèmes de messagerie, à tous les logiciels et les fichiers) permettant notamment de se connecter à distance au serveur de Innoha.

L'objectif de cette Charte est de définir les règles d'usage des moyens électroniques ou informatiques et des moyens de communication tels que visés ci-dessus, étant préalablement rappelés notamment (i) l'obligation de loyauté des collaborateurs de Innoha envers leur employeur, et ce afin de garantir la sécurité des ressources du Groupe et de protéger ses outils et ses utilisateurs, ainsi que (ii) le droit à la déconnexion des collaborateurs le soir, pendant les week-ends et congés (hors organisation spécifique de travail).

ARTICLE 1 – REGLES GENERALES

L'utilisateur s'engage à utiliser les moyens électroniques ou informatiques et les moyens de communication dans le cadre des activités professionnelles en conformité avec les règlementations applicables ainsi que les règles internes à Innoha (notamment les principes posés par le Code de Conduite des Affaires ou les politiques de Innoha). Ainsi, notamment, les utilisateurs doivent veiller à :

- La protection et à la non-divulgation des informations considérées comme confidentielles et/ou privilégiées (telles que ces notions sont définies notamment au sein du Code de Conduite des Affaires de Innoha) et identifiées ou communiquées comme telles. S'agissant des informations en provenance de tiers (clients, partenaires, etc.) l'utilisateur doit se référer à l'accord de confidentialité signé avec ce tiers. En cas de doute, l'utilisateur peut contacter (i) l'émetteur ou le diffuseur de l'information lorsque celle-ci est relative à Innoha ou (ii) le service juridique lorsque l'information est relative à un tiers.

[1] Dans le cadre de la présente politique, "utilisateur" désigne toute personne, sans exception, disposant d'un accès, utilisant ou intervenant, à titre professionnel, sur les ressources informatiques (mandataires sociaux, collaborateurs - quels que soient leurs fonctions, leur poste ou leur lieu de travail, à plein temps ou à temps partiel, en contrat à durée indéterminée ou déterminée-, stagiaires ou intérimaires, prestataires extérieurs, sous-traitants...).

- Se conformer aux réglementations applicables et notamment

    - Les lois relatives à la protection de la propriété intellectuelle (en particulier les brevets, droits d'auteurs et marques), Il est ainsi interdit de porter atteinte aux droits des tiers, dont les droits de propriété intellectuelle, qu'il s'agisse de marques, de logos, de créations multimédias, de logiciels, de textes, de photos, d'images de toute nature. Toute mention relative au droit de l'auteur ne peut faire l'objet d'une suppression et toute reproduction, adaptation ou modification de l'œuvre de celui-ci sans son consentement constitue une contrefaçon susceptible de sanctions pénale
    - Les règlementations sur la protection des données personnelles,
    - Les législations en matière de droit de la concurrence,
    - Les législations nationales et internationales régissant l'exportation et la réexportation de certaines données, notamment, le Règlement CE 428/2009 du Conseil de l'Union Européenne, l'Export Administration Regulations et l'International Traffic in Arms Regulations des Etats-Unis d'Amérique. En cas de doute ou de question, les utilisateurs peuvent s'adresser au Manager « Export Compliance » de Innoha.

- Respecter les dispositions du Code de Conduite des Affaires de Innoha et de toute autre politique de Innoha en vigueur

L'utilisateur s'interdit, dans le cadre de l'utilisation dans un contexte professionnel des différents moyens électroniques ou informatiques et des moyens de communication et, notamment, dans et par ses contributions (textes, photos, vidéos, design etc.) :

- De tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement, sans autorisation de l'intéressé ;
- De participer à des jeux et/ou agissements visant à obtenir des profits et gains personnels ;
- D'exercer une activité commerciale personnelle ou un travail clandestin ;
- Toute action susceptible d'entraîner la responsabilité civile et/ou pénale de Innoha.
- De créer de faux en-têtes ou manipuler par quelque moyen que ce soit quelconque identifiant afin de modifier l'origine de tout contenu,
- D'utiliser les différents moyens électroniques ou informatiques et les moyens de communication d'une manière pouvant endommager, désactiver, surcharger ou détériorer tout serveur, système informatique ou tout réseau de Innoha, sauf nécessité au regard de l'activité professionnelle,
- D'entraver ou perturber tout ou partie des systèmes informatiques et/ou des réseaux, de quelque manière que ce soit et, notamment, par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites (virus, chevaux de Troie, logiciels espions (spywares…), sauf nécessité au regard de l'activité professionnelle,
- D'enfreindre quelque pré requis que ce soit, procédures et/ou règles applicables,
- De modifier, adapter ou tenter de pirater les différents moyens électroniques ou informatiques et les moyens de communication,
- D'utiliser les moyens électroniques ou informatiques et des moyens de communication pour une autre utilisation que celles expressément spécifiées au sein de la présente Charte,
- D'obtenir ou tenter d'obtenir des informations ou éléments par un moyen qui ne serait pas intentionnellement mis à disposition par Innoha,
- D'interférer dans l'utilisation par les autres utilisateurs des différents moyens électroniques ou informatiques et des moyens de communication,
- D'accéder ou tenter d'accéder frauduleusement aux comptes des autres utilisateurs des moyens de communication, à leur matériel informatique, réseaux connectés, aux serveurs de Innoha ou à tout espace dont l'accès est protégé par un mot de passe.

L'utilisateur est tenu de respecter les règles en matière de sécurité informatique, applicables au sein du Groupe.

En particulier, l'utilisateur s'engage à ne désactiver aucune des applications mises en place par le Groupe pour optimiser la sécurité.

Toute question sur les règles applicables en matière de sécurité informatique peut être posée à dpo@innoha.com et rmorice@innoha.com.
En tout état de cause, les échanges professionnels doivent nécessairement avoir lieu au travers des seuls moyens de communication de Innoha (à titre d'exemple, les courriels à caractère professionnels ne peuvent être échangés qu'au travers de la messagerie professionnelle, à l'exclusion de toute autre service d'email externe).

ARTICLE 2 – REGLES D'UTILISATION PROPRES AUX LOGICIELS BASES DE DONNES ET DONNEES DE TOUTE NATURE (LES « DATA »)

Les utilisateurs s'engagent à respecter les règles et principes suivants en cas d'utilisation de data :

CONCERNANT LES DATA N'APPARTENANT PAS A INNOHA :

2.1.1. Un contrat doit être établi avant toute acquisition de data, que cette data soit gratuite ou payante, hors logiciels payants de Innoha.

La notion d'"acquisition" doit être entendue au sens large : installation, importation ou transmission de data au sein de Innoha. Cette règle est valable quel que soit le type de support employé (réseau, CD, messagerie...) et s'applique à tout type de data (y compris les jeux, drivers, musique...) à l'exclusion des logiciels payants de Innoha.

L'utilisateur contactera le service juridique, qui l'aidera à établir le contrat (ou reverra les conditions d'utilisation implicites acceptées lors du téléchargement) ou répondra à toutes interrogations.

Le téléchargement de data sur des moyens électroniques ou informatiques de Innoha en vue d'une utilisation non professionnelle est interdit.

Le téléchargement de data à licence gratuite (y compris les data sous licence d'évaluation) en vue d'une utilisation dans le cadre professionnel est toléré sous réserve de la validation préalable et expresse du supérieur hiérarchique du collaborateur concerné et à condition que les data téléchargées ne soient ni utilisées pour développer des produits ou services de Innoha ni embarquées dans les produits ou services du Groupe.

L'utilisation de data à licence gratuite pour développer des produits ou services Innoha ou l'intégration de data à licence gratuite dans les produits ou services du Groupe sont ainsi interdites, sauf autorisation expresse et préalable par les services juridique et R&D.

Il est interdit, sauf nécessité professionnelle avérée et sous réserve de l'accord préalable de la hiérarchie et du service juridique, d'utiliser des data provenant de l'open source (tous types de licence). En cas de doute, l'utilisateur contactera le service juridique.

2.1.2 Les utilisateurs doivent s'assurer de l'existence d'un contrat ou d'un droit d'usage avant toute exploitation de data extérieur au Groupe.

Par défaut, toute data extérieure à Innoha est considérée comme étant protégée par le droit d'auteur et la propriété intellectuelle.

En cas de doute, l'utilisateur pourra contacter le service juridique.

2.1.3 Toute data acquise par l'utilisateur dans un contexte professionnel doit être justifiée par les besoins de l'activité professionnelle et utilisé comme tel.

2.1.4 La reproduction et la modification (arrangements, traduction...) de data extérieur au Groupe est limitée aux conditions contractuelles liant le Groupe et l'éditeur. La suppression de mention de copyright est interdite.

CONCERNANT LES DATA APPARTENANT A INNOHA :

Les utilisateurs s'engagent à assurer la protection des data du Groupe et notamment :

- Son savoir-faire, par le respect des processus internes de sortie de data (code, produits, documentation, présentation…).
- Ses data, en respectant le fonctionnement et les options des outils ayant pour vocation de protéger les ressources de Innoha.

ARTICLE 3 – REGLES D'UTILISATION PROPORES AUX COMPTES INFORMATIQUES

3.1 Comptes informatiques et mots de passe.

Sauf « comptes de service » (compte attribué à un utilisateur donné de Innoha et pouvant être utilisé par un ou plusieurs utilisateurs dans le cadre du fonctionnement de ce service), l'attribution de comptes informatiques aux utilisateurs est personnelle.

Les utilisateurs doivent appliquer les mesures de protections nécessaires et adéquates afin d'assurer la sécurité des systèmes du Groupe et des données professionnelles, à savoir au minimum :

- Choisir un mot de passe « sûr » et en conserver l'exclusivité.
- Prendre les mesures raisonnables pour protéger ses fichiers et supports (CD, disquettes, impressions, périphériques USB…), par exemple par la mise sous clé ou cryptage des informations
- Outre le mécanisme de verrouillage automatique, les utilisateurs doivent verrouiller leur poste de travail dès qu'ils le quittent.

L'utilisateur est responsable de toute utilisation de son identifiant et de son mot de passe. Toutes connexions et/ou transmissions de données effectuées en utilisant son identifiant et son mot de passe seront réputées avoir été effectuées par l'utilisateur. Il n'est pas recommandé aux utilisateurs de préenregistrer leur mot de passe ; s'ils le font (i) les transmissions seront réputées avoir été faites par eux et (ii) ils engagent leur responsabilité de ce fait.

3.2 En aucun cas un utilisateur n'est en droit d'utiliser sans son accord le compte informatique d'un autre ou de tenter de masquer sa véritable identité. De la même manière, un utilisateur non autorisé ne peut utiliser les comptes informatiques du Groupe.

3.3 Les comptes administrateurs doivent être utilisés exclusivement pour les fonctions d'administration. Les administrateurs se doivent de respecter, le cas échéant, la nature confidentielle des informations qu'ils sont susceptibles de connaître dans le cadre de leurs fonctions.

3.4 L'accès administratif aux machines d'administration et l'action administrative sur les serveurs informatiques sont réservés aux administrateurs eux-mêmes. Seules les personnes autorisées peuvent se connecter à ces ordinateurs. Innoha conserve la traçabilité des accès et actions des administrateurs.

3.5 Fermeture de compte informatique

Le compte informatique d'un utilisateur qui cesse ses fonctions est fermé à la date de fin de son contrat, ce qui permet à l'utilisateur de récupérer ses dossiers et documents personnels jusqu'à cette date. L'accès aux données de son compte ne lui sera plus possible après cette date, étant entendu que les sauvegardes effectuées sont conservées pendant une durée maximale de 3 mois à partir de la date de la sauvegarde.

Innoha pourra toutefois procéder à la fermeture immédiate du compte informatique d'un utilisateur en cas de manquement grave de l'utilisateur aux règlementations applicables et/ou aux règles internes de Innoha et ce conformément à la législation et la jurisprudence en vigueur.

3.6 La prise en main à distance d'un poste utilisateur ne doit pas se faire sans l'accord préalable de l'utilisateur.

ARTICLE 4 – USAGE DES MATERIELS INFORMATIQUES OU ELECTRONIQUES ET OUTILS DE COMMUNICATION

UTILISATION DES MATERIELS INFORMATIQUES OU ELECTRONIQUES ET DES OUTILS DE COMMUNICATION A DES FINS PERSONNELLES

Les matériels informatiques ou électroniques et les outils de communication (différents médias, outils électroniques et numériques) mis par Innoha à la disposition des utilisateurs sont à usage professionnel et visent à améliorer le niveau de productivité et d'efficacité du Groupe.

L'utilisation occasionnelle de ces matériels informatiques ou électroniques et outils de communication à des fins personnelles est tolérée sur le temps et le lieu de travail, mais doit rester raisonnable et ne doit pas aller à l'encontre des intérêts du Groupe (notamment ne pas affecter la sécurité ou le fonctionnement des réseaux) ou nuire à la productivité de Innoha.

Les dossiers ou documents enregistrés sur les matériels électroniques utilisés dans le cadre professionnel sont considérés comme ayant un caractère professionnel, sauf indication expresse dans l'objet du dossier ou le document ou dans le nom du répertoire où il pourrait être archivé par l'utilisateur, qui lui conférerait alors la nature d'une correspondance privée, protégée par le secret des correspondances (sous réserve des dispositions légales ou jurisprudentielles applicables)[2].

Les dossiers et documents électroniques personnels :

- Doivent respecter la législation en vigueur,
- Ne sauraient servir à stocker des contenus contraires à l'ordre public, aux bonnes mœurs (notamment à caractère pornographique ou pédophile) ou au respect des droits des personnes (contenu raciste, diffamatoire, discriminatoire notamment au regard de l'origine nationale, le sexe, la religion, les opinions politiques, les origines sociales, l'âge, la santé ou le handicap) et de la vie privée, et
- Doivent occuper un espace raisonnable sur le matériel électronique sur lesquels ils sont stockés
- Doivent être stockés exclusivement sur le poste de travail de l'utilisateur. Par conséquent, les dossiers et documents électroniques personnels des utilisateurs ne doivent pas être stockés sur les serveurs de Innoha. Ainsi, les dossiers et documents personnels ne doivent pas entrer dans l'objet des sauvegardes effectuées régulièrement par Innoha ; en conséquence, ces dossiers et documents électroniques personnels doivent être enregistrés sur le répertoire « no save » pour les utilisateurs Windows.

Innoha ne prend aucun engagement quant à la conservation et la non-divulgation des dossiers et documents personnels de l'utilisateur. Par conséquent, la responsabilité de Innoha ne pourra être engagée du fait de toute perte, altération ou destruction des dossiers et documents personnels de l'utilisateur intégrés sur le matériel mis à disposition par Innoha.

Les messages électroniques à caractère personnel sont tolérés, dans la limite d'une utilisation raisonnable, à condition de ne pas :

- Perturber le fonctionnement du réseau, interférer avec la productivité de l'utilisateur,
- Empiéter sur l'activité professionnelle,

---

[2] Sous réserve de l'évolution de la jurisprudence française, un message, document ou répertoire sera considéré comme personnel si son intitulé ou son objet :

- Est clair et non équivoque.
- Ne laisse planer aucun doute sur le fait qu'il relève de la vie privée.

Il est précisé que les libellés « personnel », « perso », « privé », « private » et « personal » ne permettent pas de douter du caractère privé d'un message ou répertoire.

Dans le cadre de la messagerie électronique, les messages ou contacts à caractère personnel doivent être archives/enregistrés sur le poste de travail, dans un répertoire d'archive spécifique, afin de ne pas entrer dans l'objet des sauvegardes effectuées régulièrement par Innoha.

REGLES D'UTILISATION DES MATERIELS INFORMATIQUES OU ELECTRONIQUES

4.2.1 L'utilisateur est responsable des conséquences de l'utilisation de matériel informatique ou électronique personnel (clé USB, téléphone portable…) avec les matériels et services de Innoha.

En cas de doute, l'utilisateur contactera le service informatique avant toute utilisation d'un matériel informatique ou électronique personnel.

4.2.2 Les matériels informatiques ou électroniques mis à la disposition des utilisateurs par Innoha sont la propriété de Innoha. Toute intervention sur ces matériels informatiques ou électroniques doit être faite par des utilisateurs de Innoha qui y sont habilités.

4.2.3 En leur qualité de gardien des matériels informatiques mis à leur disposition par Innoha dans le cadre de leur activité, les utilisateurs doivent utiliser les moyens mis à disposition pour protéger les matériels informatiques ou électroniques contre le vol ou contre toute utilisation abusive notamment en mettant le matériel sous clé ou en utilisant le système antivol fourni par Innoha. Hors de Innoha, les utilisateurs s'engagent à exercer une vigilance particulière à l'égard de ces matériels et à prendre toutes les précautions utiles, nécessaires et adéquates afin d'assurer la sécurité desdits matériels.

4.2.4 Les utilisateurs doivent restituer le matériel informatique ou électronique mis à leur disposition par Innoha avant de quitter le Groupe et/ou sur demande de Innoha. La restitution effective du matériel informatique ou électronique fait l'objet d'une mention portée sur la fiche départ de l'utilisateur. L'utilisateur s'il le souhaite recevra une copie dudit document.

4.2.5 Avant de quitter le Groupe et/ou sur demande de Innoha, les utilisateurs s'engagent à restituer à leur manager l'ensemble des données professionnelles en leur possession, notamment une copie de leur messagerie professionnelle et de leurs dossiers et documents professionnels.

REGLES D'UTILISATION PROPRES AUX OUTILS DE COMMUNICATION

4.3.1. Règles communes d'utilisation des outils de communication

Outre l'obligation de respecter les principes posés à l'article 1 de cette Charte et sans porter préjudice à la liberté d'expression ou aux prérogatives législatives ou conventionnelles des Institutions Représentatives du Personnel et des délégués syndicaux, l'utilisateur s'interdit dans le cadre de ses communications professionnelles ou celles réalisées au travers des moyens de communication mis à sa disposition par Innoha :

- D'insérer un lien vers un site web portant atteinte aux droits des tiers ou aux lois et règlements en vigueur ;
- De harceler ou menacer quiconque par quelque moyen que ce soit ;
- De dénigrer des collègues ou des clients, partenaires, concurrents (ou leurs produits), etc. ;
- D'insérer ou partager un contenu à caractère discriminatoire, diffamatoire, injurieux, nuisible, menaçant ou intimidant, malveillant, abusif, vexatoire, tortueux, vulgaire, obscène, calomnieux, constituant une violation de la vie privée d'un tiers, portant atteinte aux règles de protection des données personnelles, aux droits de la personnalité d'un tiers, ou à caractère pornographique, pédophile, racial ou incitant à la haine ou à la discrimination, ou à commettre un délit ou un crime, ou faisant l'apologie des crimes de guerre ou crimes contre l'humanité et plus généralement tout contenu de caractère illicite ;
- De faire de la propagande à caractère syndical, notamment par la diffusion de tout tract ou

publication, hors du cadre législatif institué par l'article L.2142-6 du Code du travail ;

- De faire du prosélytisme politique ou religieux ;
- De véhiculer tout message portant atteinte à l'image la réputation ou la considération de Innoha, de ses utilisateurs, de ses concurrents ou de quiconque.

Il est rappelé que les contenus offensants destinés à nuire intentionnellement à la réputation de quelqu'un ou les contenus susceptibles de contribuer à une détérioration de l'environnement de travail peuvent engager la responsabilité de Innoha selon la loi ou la réglementation en vigueur.

Les informations communiquées doivent être fiables : il est interdit de communiquer sciemment des informations fausses ou trompeuses. En conséquence, outre l'obligation de ne pas dénigrer les produits et offres des concurrents, l'utilisateur qui diffuse du contenu sur les produits et offres de Innoha doit (i) s'efforcer d'être totalement précis et objectif, par exemple en ce qui concerne les fonctionnalités des produits, et (ii) respecter les désignations standards des produits Innoha et, autant que possible, insérer des liens vers les sections correspondantes du site institutionnel de Innoha (www.3ds.com) afin d'éviter tout malentendu ; la divulgation d'une fonctionnalité future ou l'association d'une future fonctionnalité à des dates de livraison peut avoir des conséquences juridiques et financières, c'est pourquoi les utilisateurs doivent veiller à ne pas diffuser de contenus susceptibles de créer une quelconque attente en lien avec un futur produit ou service (en dehors des « roadmaps » officiels).

4.3.2. Messagerie

4.3.2.1. Chaque Utilisateur dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique.

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit. Il peut être encore plus rapidement communiqué à des tiers et constitue un écrit susceptible d'engager la responsabilité de son auteur et de Innoha.

Afin d'éviter tous dysfonctionnements, de limiter l'envoi de messages non sollicités (spams) et de ne pas engager la responsabilité civile ou pénale de Innoha et/ou de l'utilisateur, il est demandé à ces derniers :

- Avant tout envoi, de vérifier l'identité des destinataires du message et leur qualité à recevoir les informations transmises ;
- En cas d'envoi à une pluralité de destinataires, de vérifier que tous les destinataires externes à Innoha ont donné leur consentement préalable à la réception du courrier qui leur est adressé (i.e. l'envoi de messages non sollicités type spams est prohibé par la loi) et d'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 ;
- De veiller au respect des informations à caractère confidentiel et, en cas de doute, demander conseil au Service Informatique ;
- De veiller au respect des lois et règlements, et notamment en matière de protection des droits de propriété intellectuelle et des droits des tiers ;
- De ne pas adresser de correspondances électroniques comportant des éléments illicites, tels que des propos diffamatoires, injurieux et contraires aux bonnes mœurs (notamment à caractère pornographique ou pédophile).

D'une manière générale, l'utilisateur s'engage à ne pas se livrer via la messagerie électronique à une activité susceptible de causer au Client un quelconque préjudice.

Enfin, l'attention des utilisateurs est attirée sur le fait que pour des raisons techniques, le nombre et le type des pièces jointes peuvent être limités par le Service Informatique pour éviter l'engorgement du système de

messagerie. Ainsi en cas d'envoi particulièrement volumineux, il est nécessaire d'en informer au préalable le Service Informatique afin que ce dernier prenne les dispositions nécessaires.

Le Groupe conserve les fichiers journaux (ou logs) de messagerie pour une durée maximale de six mois.

4.3.2.2. Les messages électroniques sont sauvegardés automatiquement pour être conservés pendant une durée de 31 jours.

Innoha a mis en place des outils de contrôle de la messagerie (outils de mesure de la fréquence, de la taille, des messages électroniques ; outils d'analyse des pièces jointes (détection des virus, filtres « anti-spam » destinés à réduire les messages non-sollicités, etc.), pour des raisons de sécurité, de prévention ou de contrôle de l'encombrement du réseau. Tout contrôle sur la messagerie s'exercera conformément à l'article 6 de la présente Charte, ainsi qu'aux dispositions légales et jurisprudentielles.

4.3.2.3. Pour des besoins d'organisation interne, l'utilisateur est informé qu'en son absence, quelle qu'en soit la cause et la durée, les e-mails reçus sur sa boîte de messagerie électronique sont susceptibles d'être redirigés vers la boîte de messagerie électronique d'un autre utilisateur.

En cas d'accès direct d'un utilisateur (« Utilisateur remplaçant ») à la boîte de messagerie électronique d'un autre utilisateur (« Utilisateur absent ») pour des raisons d'organisation interne ou en cas de remplacement ponctuel (vacances, absence longue durée) par une personne externe, l'Utilisateur remplaçant ou la personne externe devra signer chacun des e-mails envoyés de la boîte de messagerie électronique de l'Utilisateur absent avec ses nom et prénom, en utilisant le modèle suivant : M/Mme X au poste de M/Mme Y, M/Mme X étant l'Utilisateur remplaçant ou la personne externe et M/Mme Y étant l'Utilisateur absent.

L'Utilisateur remplaçant ou la personne externe engagée pour un remplacement s'interdit de consulter les messages, documents ou fichiers identifiés comme « personnel » (cf. paragraphe 4.1) par l'Utilisateur absent.

4.3.2.4. En cas de départ d'un utilisateur, son compte de messagerie est désactivé au plus tard dans les 2 mois à compter de la date de son départ. Innoha pourra accéder, dans ce délai, à la messagerie de l'utilisateur et ce aux strictes fins de poursuite de l'activité de Innoha étant précisé que, dans ce cas, Innoha n'accèdera pas aux contenus expressément identifiés comme personnels au sein de ladite messagerie. Toutefois, pour assurer le secret des correspondances privées, il est vivement recommandé aux utilisateurs, dans leur propre intérêt, d'utiliser des services email externes pour leur correspondance électronique privée (Google, Yahoo ou d'autres).

L'utilisateur est invité à fournir à ses contacts personnels toute nouvelle adresse de messagerie à laquelle il souhaite recevoir ses messages.

Les utilisateurs susceptibles d'avoir accès à un compte de messagerie après le départ d'un utilisateur sont informés :

- Qu'ils doivent supprimer sans l'ouvrir tout courriel dont l'objet, tel que décrit par le titre du courriel, est manifestement personnel à l'égard de l'utilisateur initialement destinataire ;
- Qu'ils doivent, sauf demande préalable expresse de l'utilisateur initialement destinataire, supprimer sans (i) poursuivre la lecture ni (ii) procéder à la transmission, à l'impression, à la copie, à la réponse, à l'utilisation ou à l'exploitation, pour quelque raison que ce soit ou à quelque titre que ce soit, de tout courriel dont le titre ne permet pas de déterminer le caractère manifestement personnel à l'égard de l'utilisateur initialement destinataire mais qui, une fois ouvert, révèle un contenu manifestement personnel.

En revanche, l'ensemble des courriels dont ni le titre, ni le contenu ne révèlent un objet manifestement personnel à l'égard de l'utilisateur initialement destinataire pourront être présumés comme étant de nature professionnel et être traités par le destinataire de remplacement.

A l'issue de la période de 2 mois maximum, l'intégralité de la boite de messagerie sera supprimée.

4.3.3. Internet

Innoha a mis en place des dispositifs de filtrage de sites non autorisés (par exemple, les sites à caractère pornographique, pédophile, d'incitation à la haine raciale, révisionniste, etc.).

Le Groupe conserve les fichiers journaux (ou logs) de connexion à internet et de navigation des utilisateurs pendant une durée de six mois ; les logs de connexion et de navigation des autres individus auxquels Innoha fournit un service de connexion à internet (notamment le service Wifi pour les visiteurs) sont conservés pendant une durée d'un an.

Pour des raisons de sécurité, notamment compte tenu des risques de virus, Innoha se réserve le droit de fixer d'autres limites à l'utilisation d'Internet, telle que, par exemple, l'interdiction de se connecter à un forum ou d'utiliser un « chat ».

L'utilisateur s'interdit de consulter des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs (notamment à caractère pornographique ou pédophile) ou au respect des droits des personnes (contenu raciste, diffamatoire, discriminatoire notamment au regard de de l'origine nationale, le sexe, la religion, les opinions politiques, les origines sociales, l'âge, la santé ou le handicap) et de la vie privée.

4.3.4. Utilisation des plateformes collaboratives

Les plateformes collaboratives sont très efficaces et ont une résonnance très large ; ainsi, une fois en ligne, les publications faites sur les plateformes collaboratives sont accessibles par tous, peuvent être transférées à l'infini et sont susceptibles de ne jamais disparaître. C'est pourquoi Innoha recommande à ses utilisateurs d'être extrêmement vigilants et attentifs lors de l'utilisation des plateformes collaboratives, et de mesurer les éventuelles conséquences de toute intervention sur ces plateformes.

B.1 Plateformes collaboratives externes à Innoha

Les principes suivants s'appliquent aux communications professionnelles des utilisateurs sur les plateformes collaboratives externes :

- Les utilisateurs ne sont autorisés à communiquer sur les plateformes collaboratives externes pour le compte de Innoha, sur les produits, l'activité ou tout autre sujet en lien avec l'écosystème de Innoha (les concurrents, partenaires, clients, etc.) que s'ils y ont été préalablement chargés au titre de leur mission et/ou habilités à titre permanent ou temporaire[3]. L'utilisateur s'engage donc à faire valider par sa hiérarchie la possibilité de participer à des discussions sur des plateformes collaboratives lorsqu'il s'exprime à titre professionnel ou au nom de Innoha, et ce préalablement à toute contribution de l'utilisateur sur ces espaces collaboratifs.
- Il est attendu des utilisateurs qu'ils agissent avec transparence sur les plateformes collaboratives : ils doivent mentionner leur statut d'utilisateur de Innoha, utiliser leur véritable nom et spécifier clairement leur fonction.
- Dans l'hypothèse où un autre blogueur dénigrerait un Client, ses produits ou services, ou ferait preuve d'un manque de respect envers les utilisateurs de Innoha, l'utilisateur qui souhaiterait réagir à de telles contributions est invité à contacter son Responsable des Relations Publiques, qui pourra l'aider à déterminer la meilleure réponse à apporter en fonction de la situation.
- Support en ligne : le Support Client étant une activité commerciale qui peut engager la responsabilité de Innoha, les utilisateurs ne sont pas autorisés à fournir de support technique sur les plateformes collaboratives en dehors des outils dédiés du Groupe. Si un utilisateur est consulté en ligne sur un véritable problème de support (à distinguer des questions pratiques auxquelles il peut répondre

[3] Sauf accord exprès et préalable d'un membre du Comité de direction de Innoha (XCOM) et/ou de l'un de ses collaborateurs directs, et sous réserve d'une notification au Responsable des Réseaux Sociaux concerné ou communication@innoha.com ou, les prestataires ou consultants de Innoha ne sont pas autorisés à représenter Innoha sur les plateformes collaboratives. Les revendeurs Innoha ne sont en aucun cas autorisés à représenter Innoha en ligne.

facilement et avec exactitude), il doit conseiller à l'utilisateur de s'adresser à son prestataire de services de support. Si l'utilisateur indique dans ses commentaires qu'il l'a déjà fait et n'a pas reçu de réponse, ou si le prestataire de services de support n'a pas été en mesure de résoudre le problème, l'utilisateur peut contacter contact@innoha.com en précisant les détails de la demande de l'utilisateur.

- L'utilisateur qui souhaite ouvrir un compte Innoha (pour un événement, une marque, une campagne, etc.), doit tout d'abord s'adresser à son Responsable des Réseaux Sociaux ou communication@innoha.com L'ouverture d'un compte Innoha entraîne une responsabilité particulière et implique un engagement à long terme.

En cas de question ou pour obtenir plus d'informations pour une meilleure communication via les plateformes collaboratives, les utilisateurs peuvent contacter leur Responsable des Relations afin obtenir des informations spécifiques à chaque marque et/ou communication@innoha.com.

Lorsqu'ils communiquent sur les plateformes collaboratives en dehors du cadre professionnel, les utilisateurs agissent sous leur propre responsabilité ; il est néanmoins dans leur intérêt de respecter un certain nombre de principes et notamment :

- **De la transparence :** de nombreux utilisateurs pourraient ne pas distinguer si un utilisateur s'exprime en qualité d'utilisateur de Innoha ou à titre personnel, dans le cadre de sa vie privée, de son blog personnel ou compte personnel (en particulier si l'utilisateur intervient sur les plateformes collaboratives à partir des moyens informatiques de Innoha) ; pour éviter le risque de confusion, il est recommandé aux utilisateurs d'insérer un message d'avertissement (par exemple : « les opinions exprimées sur ce site/blog sont personnelles et ne reflètent pas nécessairement celles de mon employeur »), ou tout autre équivalent, de manière suffisamment lisible. Il est rappelé que les propos des utilisateurs peuvent éventuellement engager leur responsabilité et/ou celle de Innoha.
- **Informations confidentielles :** il est rappelé que la divulgation d'une information confidentielle et/ou privilégiée, telles que ces notions sont définies dans le Code de Conduite des Affaires de Innoha peut engager la responsabilité personnelle des utilisateurs.
- **Respect des lois applicables :** tout manquement à la législation, notamment en matière de (i) protection de la propriété intellectuelle (en particulier les brevets, droits d'auteur et marques, notamment lorsque l'utilisateur fait référence aux produits, logos, etc. de l'écosystème Innoha), (ii) protection des données personnelles, (iii) diffamation et (iv) responsabilité délictuelle et/ou contractuelle, peut engager la responsabilité personnelle de l'utilisateur envers des tiers et/ou Innoha.
- **Prudence :** outre le risque mentionné ci-dessus de confusion entre les comptes professionnel et personnel, les utilisateurs doivent être très vigilants sur l'utilisation des plateformes collaboratives externes compte tenu des risques notamment de fraude, d'usurpation d'identité, de piratage de compte, etc.

C.1 Plateformes collaboratives de Innoha

La mise à disposition par Innoha de plateformes collaboratives à ses utilisateurs est réservée à un usage professionnel afin de diffuser et d'échanger des informations dans un esprit de collaboration.

- **Utilisation des plateformes collaboratives de Innoha**

Tout utilisateur utilisant une plateforme collaborative doit respecter les règles communes applicables à l'ensemble des outils de communication. Il ne peut accéder à un espace de la plateforme dont l'accès est restreint qu'après y avoir été autorisé par l'administrateur de cet espace. Il s'interdit en conséquence de tenter d'y accéder par quelque autre moyen que ce soit.
Les utilisateurs s'engagent à utiliser les plateformes collaboratives conformément à leur objet et dans le respect des droits concédés à l'utilisateur tels qu'ils pourront être précisés par Innoha par tout moyen au sein des plateformes collaboratives.

- **Propriété intellectuelle de Innoha**

Sans préjudice des conditions posées à l'article 1 de la présente Charte, tout contenu diffusé sur les plateformes collaboratives de Innoha, y compris les marques, logos, textes, graphiques, images, téléchargements numériques et logiciels, est protégé par les droits de propriété intellectuelle applicables.

Les utilisateurs ayant accès aux plateformes collaboratives de Innoha n'ont qu'un droit de licence individuel, non cessible et non exclusif portant sur l'utilisation de ce contenu aux fins exclusives de le visualiser sur l'écran de leur ordinateur professionnel, de navigation au sein des plateformes collaboratives et d'utilisation des services proposés sur ces plateformes pour les stricts besoins professionnels. Toute autre utilisation, sans le consentement préalable écrit et exprès de Innoha ou, le cas échéant, du titulaire des droits sur le contenu concerné, est strictement interdite.

- **Participation aux espaces collaboratifs proposés sur les plateformes**

1) *Contributions des utilisateurs de Innoha*

Tout utilisateur de Innoha, qui souhaite participer à un des espaces collaboratifs proposés par les plateformes s'engage à ne proposer que des contributions :

- Qui apportent une idée, un point de vue en lien avec la thématique abordée dans l'espace collaboratif concerné ;
- Qui contiennent des informations dont les sources ont été vérifiées afin d'éviter la circulation de données fausses ou inexactes pouvant avoir un impact important ; s'il exprime une opinion qui lui est propre, il doit le mentionner comme tel.
- Qui respectent les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve et devoir de discrétion en usage au sein du Groupe.

Tout utilisateur de Innoha reconnaît qu'il est seul responsable de ses contributions sur les plateformes collaboratives. A ce titre, il garantit qu'il en est bien l'auteur ou qu'il dispose des droits et autorisations nécessaires afin de partager le contenu de cette contribution sur les plateformes.

2) *Droits concédés sur les contributions*

L'utilisateur qui insère un contenu entrant dans le cadre de sa mission et/ou poursuivant un objectif professionnel, transmet tous les droits relatifs audit contenu à Innoha, qui sera ainsi seule propriétaire du contenu.

L'utilisateur qui insère un contenu n'entrant pas dans le cadre de sa mission et/ou ne poursuivant pas un objectif professionnel, concède à Innoha, à titre gratuit, pour le monde entier et pour la durée de la protection dont le contenu pourrait faire l'objet, le droit transférable et sous-licenciable, d'utiliser, de représenter, de reproduire, de modifier, d'adapter et de diffuser, par tout moyen et tout support, existant ou à venir, tout ou partie de la contribution, ainsi que d'associer et/ou d'intégrer ce contenu à un ou plusieurs autres éléments, et ce aux fins de communication et de promotion des activités et/ou des produits de Innoha. A cette fin l'utilisateur garantit qu'il dispose bien de tous les droits relatifs au contenu inséré.

- **Contrôle et modération des plateformes collaboratives de Innoha**

Dans le respect du principe de proportionnalité, les services des plateformes collaboratives de Innoha peuvent donner lieu à contrôle par Innoha à des fins statistiques de traçabilité, d'optimisation, de sécurité ou de détection des abus dans le respect de la réglementation applicable notamment en matière de protection des données personnelles.

Innoha pourra (conformément aux dispositions légales et jurisprudentielles) effectuer toute opération technique de contrôle permettant de vérifier le respect des dispositions légales ou internes de Innoha.

Tout contenu litigieux pourra également être supprimé de la plateforme interactive, et ce sans préavis ou information de l'utilisateur.

Par ailleurs, tout utilisateur de Innoha peut signaler tout contenu contraire aux dispositions légales ou internes de Innoha par l'intermédiaire du lien « Report Abuse/Signaler un Abus » qui figure à côté de chaque article ou commentaire. Tout utilisateur utilisant une plateforme collaborative est autorisé à retirer ou demander la suppression d'une de ses contributions.

4.3.5. Téléphonie

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès au système de téléphonie fixe et mobile de Innoha.

Les appels téléphoniques à caractère personnel sont tolérés, dans la limité d'une utilisation raisonnable, à condition de ne pas :

- Perturber le fonctionnement du système de téléphonie,
- Interférer avec la productivité de l'utilisateur,
- Empiéter sur l'activité professionnelle,
- Engendrer des coûts supplémentaires pour Innoha.

En tout état de cause, l'utilisateur s'engage à utiliser son téléphone conformément aux principes généraux édictés à l'article 1 de la présente Charte.

ARTICLE 5 – SIGNALEMENT DES INCIDENTS

Il est demandé aux utilisateurs de signaler toute disparition (provisoire ou définitive) de support informatique, qu'il avait en sa possession, pouvant contenir des informations relatives à Innoha. Il peut par exemple s'agir d'un vol de matériel, d'un oubli dans un train ou encore de l'ouverture d'un ordinateur portable ou d'accès à des contenus par des autorités douanières.

Innoha dispose de mécanismes permettant d'effacer à distance le contenu des supports informatiques, lesquels peuvent être utilisés en cas de disparition de support informatique (y compris les supports informatiques appartenant aux utilisateurs et qui sont utilisés à des fins professionnelles). Il est donc demandé aux utilisateurs d'effectuer des sauvegardes régulières dans le cadre des mécanismes de sauvegarde mis en place par Innoha, dans la mesure où l'effacement portera sur l'ensemble des contenus du dispositif.

Procédure à suivre en cas de disparition de support informatique :
Il est demandé aux utilisateurs de :

- Dans les meilleurs délais :
  - Demander à l'opérateur de suspendre la ligne si la disparition concerne un téléphone
  - Signaler la disparition au service informatique (Helpdesk) de Innoha, ainsi qu'aux personnes chargées de la sécurité.
- Effectuer dès que possible une déclaration de vol ou de perte auprès des services de police compétents et en transmettre une copie aux personnes chargées de la sécurité.
- Se rendre au service informatique avec une copie de la déclaration de vol ou de perte afin de récupérer un nouveau matériel.

Il pourra être demandé à l'utilisateur victime de cet incident de donner des détails sur les circonstances de la potentielle perte d'informations (cause présumée, contenu impacté, éventuelles mesures prises).

ARTICLE 6 – PROCEDURE D'ALERTE

L'objectif de cette procédure est de fournir des lignes directrices claires et efficaces pour l'identification, l'alerte et la gestion et la résolution des incidents de sécurité de l'information. Elle doit garantir une réponse rapide et appropriée afin de minimiser les risques liés à la sécurité de l'information, assurer la continuité des opérations et réduire l'impact global des incidents

Cette procédure s'applique à tous les employés, partenaires, et prestataires, sous-traitants et autres parties ayant accès aux systèmes d'information de l'organisation. Elle couvre tous les types d'incidents de sécurité, incluant mais ne se limitant pas aux violations de données, attaques informatiques, et comportements malveillants.

Définition des Incidents
Un incident de sécurité de l'information est tout événement susceptible d'affecter la confidentialité, l'intégrité ou la disponibilité des informations. Cela inclut, sans s'y limiter :

- Accès non autorisé aux systèmes ou données sensibles.
- Perte ou vol de données (y compris celles affectées des attaques internes ou externes)
- Attaques par ransomware, phishing, malware, ou tentatives de social engineering.
- Problèmes de conformité liés à la sécurité.
- Dispositifs non sécurisés, vulnérabilités système ou mauvaise gestion des accès.

Classification des Incidents

- Critique : Incidents ayant un impact majeur sur les opérations ou la confidentialité des données, tels qu'une interruption prolongée des services essentiels ou une compromission grave des données sensibles, affectant un grand nombre d'utilisateurs ou des fonctions clés de l'entreprise.
- Majeur : Incidents ayant un impact limité sur les opérations ou la confidentialité des données, tels qu'une perturbation temporaire affectant un nombre restreint d'utilisateurs ou une violation de données non sensibles.
- Mineur : Incidents ayant un impact négligeable sur les opérations ou la confidentialité des données, comme des alertes de sécurité non validées, des défaillances mineures sans conséquence pour les données ou les opérations.

Etapes de la Procédure d'Alerte
1. Signalement de l'Incident

- Toute personne constatant un incident de sécurité doit en avertir immédiatement le responsable de sécurité de l'information en lui envoyant un email à l'adresse dpo@innoha.com ou contacter l'Officier de Sécurité au +33 (0)6 88 01 65 79
- Les informations suivantes doivent être communiquées :
    - Nature de l'incident ;
    - Date et heure de l'incident ;
    - Description détaillée (impact potentiel, utilisateurs affectés, etc.).

2. Enregistrement de l'Incident

- L'incident doit être enregistré dans un registre centralisé (journal des incidents de sécurité) par le responsable de la sécurité de l'information
- Chaque incident comprendra a minima la date, la nature de l'incident, les données affectées et les mesures prises.
- Chaque incident doit être classé selon son niveau de criticité (mineur, majeur, critique).
- Le registre des incidents est lui-même conservé dans un environnement sécurisé accessible uniquement aux personnes autorisées, sous la supervision de la Direction d'Innoha et du responsable de la sécurité de l'information.

3. Analyse préliminaire et confinement

- Identification et qualification de la violation : Déterminer la nature de la violation et évaluer le risque associé.

- Évaluation de l'impact : Analyser les types de données touchées et le nombre de personnes affectées pour comprendre les conséquences potentielles.

4. Notifications des Parties Prenantes
- Selon la gravité de l'incident, les parties prenantes doivent être informées dans les délais spécifiés ci-dessous :
    - Incidents critiques : notification immédiate (dans l'heure suivant la détection de l'incident) à :
        - La direction de l'entreprise
        - Les départements clés : conformité, sécurité, IT, RH, etc. et toute autre unité impactée par l'incident.
        - Les autorités externes : selon les exigences réglementaires, telles que la CNIL, la police ou toute autre autorité compétente, dans les meilleurs délais selon les législations applicables.
    - Incidents majeurs : notification dans les 24h à :
        - La direction de l'entreprise
        - Les départements concernés (conformité, sécurité, IT, RH, etc.) et tout autre unité ayant un lien direct avec l'incident.
        - Les autorités externes si nécessaire et selon les législations applicables, tel que la CNIL si le risque pour les droits et libertés des personnes est avéré.
    - Incidents mineurs : notification dans les 48 à 72h
        - Les départements concernés : conformité, sécurité, IT, RH, etc. en fonction de l'impact de l'incident.
        - La direction à titre de suivi, d'analyse et de prévention des risques futurs.

5. Investigations et Résolution
- Une investigation approfondie doit être menée par les parties prenantes pour identifier la cause de l'incident, son origine (exemples : attaque externe, erreur humaine, défaillance technique...), ainsi que l'étendue de ses effets.
- Le responsable de sécurité de l'information doit coordonner les actions correctives, telles que l'application de patchs de sécurité, la restauration des données affectées, et la mise à jour des systèmes vulnérables.
- Des mesures de prévention devront être mises en place pour éviter la récurrence du problème. Cela peut inclure, selon la nature de l'incident et à titre d'exemple, des actions telles que la mise à jour des politiques de sécurité, l'amélioration des contrôles d'accès, la mise en place de formations de sensibilisation pour les employés, la modification de la configuration des systèmes.

6. Clôture de l'Incident
- Une fois l'incident résolu, il doit être documenté dans le registre des incidents avec un rapport détaillé incluant la nature de l'incident, les actions prises et les résultats obtenus. Un rapport final peut être rédigé pour chaque incident afin de partager des recommandations avec les parties prenantes (direction, équipes opérationnelles, etc.) pour éviter de futurs incidents.
- Le responsable de sécurité de l'information doit donner son approbation pour clore l'incident, si nécessaire après avoir vérifié que toutes les actions correctives ont été mises en œuvre, que les recommandations ont été appliquées, et que les mesures de prévention nécessaires sont en place pour éviter la récurrence de l'incident.

Cette procédure permet d'assurer une réponse appropriée aux incidents de sécurité et de maintenir la sécurité des informations au sein de l'organisation.
À ce titre, les salariés d'Innoha sont engagés à demeurer vigilants et sensibilisés quant à cette procédure et aux bonnes pratiques en matière de cybersécurité.

ARTICLE 7 – CONTROLES ET SANCTIONS

CONTROLES

7.1.1. Contrôles automatisés

L'attention des utilisateurs est attirée sur le fait qu'il est possible de contrôler leur activité et leurs échanges et que des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles de la présente Charte.

Des fichiers journaux (« logs ») créés en grande partie automatiquement par les équipements informatiques et de télécommunication sont stockés sur les postes informatiques et sur le réseau. Ils permettent de détecter les erreurs matérielles ou logicielles et de contrôler l'accès des utilisateurs et des tiers aux différents outils informatiques et de communications.

Dans ce cadre, les données suivantes sont conservées :

- Celles relatives à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;
- Celles relatives aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, aux communications entrantes et sortantes au réseau téléphonique, afin de détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités telles que la consultation de sites web ou le téléchargement de fichiers.

Les utilisateurs sont identifiés par leurs identifiants de connexion au réseau Innoha (Login + mot de passe) pour toute activité réalisée.

Enfin, un dispositif de filtrage des courriers électroniques non sollicités (« spams ») est mis en œuvre afin d'assurer la sécurité du système informatique. Les utilisateurs peuvent s'adresser au Service Informatique (via une demande de support) pour l'interroger sur les messages leur étant destinés et qui auraient été filtrés et/ou pour demander à faire libérer des messages de la quarantaine. Les messages filtrés le sont automatiquement par des serveurs analyseurs et ne sont pas lus par le Service Informatique qui en conserve la trace pendant 30 jours.

Ce système automatique vise à s'assurer que le message ne contient pas de virus, connu ou inconnu, et ne rentre pas dans la catégorie du courrier non sollicité.

7.1.2. Procédure de contrôle ciblé

Innoha se réserve le droit, dans le strict respect de la réglementation et de la jurisprudence applicables, de :

- Procéder à un contrôle ciblé et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs ;
- Prendre connaissance des contenus identifiés par l'utilisateur comme « personnel » (qu'il s'agisse de messages ou fichiers sur le disque dur de l'ordinateur mis à sa disposition), étant entendu que les contenus non expressément identifiés comme « personnel » pourront en revanche être consultés librement[4].

SANCTIONS

Le non-respect des principes développés dans cette Charte constitue une faute passible d'une sanction disciplinaire pouvant aller jusqu'à la rupture du contrat de travail, conformément aux dispositions du règlement intérieur que la présente Charte vient compléter.

[4] Cf. paragraphe 4.1.

En cas de non-respect par l'utilisateur des droits des tiers ou des règles légales et réglementaires en vigueur, Innoha pourra appeler celui-ci en garantie, conformément à la législation et dans le respect des procédures applicables à la suite de toute procédure civile engagée à son encontre. En outre, la responsabilité pénale de l'utilisateur pourra être engagée directement et, en cas de condamnation par les juridictions compétentes, l'utilisateur pourra être amené à réparer tout préjudice causé à un tiers.

ARTICLE 8 – DONNEES PERSONNELLES

Conformément à l'article 32 de la loi « Informatique et Libertés » du 6 janvier 1978, nous vous informons que des données personnelles sont collectées en vue de s'assurer de l'utilisation raisonnable des ressources des systèmes d'information de Innoha. Vous disposez d'un droit d'accès, de rectification et d'opposition au traitement de vos données personnelles auprès de la Division Informatique de Innoha S.A.

ARTICLE 9 – DEPOT, COMMUNICATION ET ENTREE EN VIGUEUR

Il est rappelé que la présente Charte constitue une adjonction au Règlement Intérieur de la société Innoha.

Toute modification ultérieure ou tout retrait d'une ou plusieurs dispositions de la présente Charte serait, conformément au Code du travail, soumis à la même procédure, étant entendu que toute disposition de la présente Charte qui deviendrait contraire aux dispositions légales, règlementaires ou conventionnelles applicables à la société Innoha, serait nulle de plein droit sans préjudice des autres dispositions qui garderont toute leur force et leur portée.

La présente Charte a été soumise pour consultation au CHSCT et au Comité d'entreprise en vue de son intégration au Règlement Intérieur de Innoha.

Elle a été communiquée à la Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi de Saint-Quentin-en-Yvelines et a été déposée au greffe du Conseil de Prud'hommes de Versailles.

La présente Charte entrera en vigueur le 27/02/2016,

Je soussigné(e),

NOM :
PRENOM :
SOCIETE :

Reconnais avoir pris connaissance de cette charte informatique dans le cadre de l'exécution de ma mission au sein de Innoha.

Fait à , le

Signature

C. MESURES DE SECURITE ET DE SAUVEGARDE DE DONNEES

Dans le cadre de notre intervention et avec votre accord, nous aurons recours à nos matériels et systèmes d'informations. Ceci permet de faciliter la mise en œuvre de notre prestation tout en garantissant aisément les niveaux de sécurités requis par votre organisation. Néanmoins, et comme c'est les cas pour certains de nos centres de services, nous sommes en mesure de fonctionner selon les modalités suivantes :

- Environnement de travail Innoha avec un accès direct aux outils Client via un compte d'accès fournisseur (nominatif)
- Environnement de travail Client avec un accès aux outils via un compte d'accès fournisseur (nominatif)
- Equipement physique Innoha, avec un poste de travail virtuel hébergé dans le réseau Client

Dans le cas d'un environnement apporté par Innoha, nous utilisons les configurations suivantes :

- Environnement Microsoft 365 (Office, Sharepoint, Teams)
- Softphonie : Zoiper
- Antivirus Windows
- Bitlocker Activé

Innoha fait appel à un prestataire externe pour l'ensemble des enjeux et support IT : Dryve

HEBERGEMENT DES DONNEES DE NOTRE ENVIRONNEMENT

Les données de la suite d'outils proposée sont hébergées en Europe :

- **Microsoft Office 365 / Microsoft SharePoint Online :** les données des utilisateurs de Microsoft Office 365 / Microsoft SharePoint Online sont **hébergées dans des datacenters Microsoft en France**. https://www.microsoft.com/fr-fr/microsoft-365/microsoft-365-local-datacenter
- **Monday.com :** Monday.com héberge les données de ses clients Européens dans des centres de données Amazon Web Services (AWS) sur un site hébergé en Allemagne. Par ailleurs, monday.com est conforme à la réglementation RGPD.
- **Klaxoon :** les données des utilisateurs Klaxoon sont **hébergées en France**. L'infogérance est également réalisée depuis la France. https://klaxoon.com/fr/securite

TAUX DE DISPONIBILITE, TRAITEMENTS DES INCIDENTS ET ANOMALIES

Les conditions de services standards proposés par nos partenaires permettent de garantir des niveaux de services élevés :

	MICROSOFT OFFICE 365 MICROSOFT SHAREPOINT	MONDAY.COM	KLAXOON
Taux de disponibilité	**99,9 %**	**99,0%**	**99,9%**
Garante de temps de rétablissement	**2 à 8 heures** *Selon la gravité de l'incident*	**6 à 8 heures ouvrées**	**4 heures maximum** *Pendant les heures ouvrables (lundi au vendredi, sauf jours fériés en France, de 8h à 19h, heure de Paris).*

ADMINISTRATION FONCTIONNELLE

L'administration fonctionnelle de la suite d'outils proposée sera opérée par la cellule pilotage et la cellule RH / Administration. Ils auront en charge d'une part le support de niveau 1 pour les collaborateurs de l'Antenne (enregistrement, connexion, navigation) et la formation.

Les fonctionnalités de partage externe des outils permettront aux membres de notre organisation de collaborer avec vos collaborateurs, vos fournisseurs (si nécessaire) et autre.

D. TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Nous nous engageons à offrir le meilleur niveau de sécurité pour les services procurés. En assurant la protection des données personnelles et en apportant simplicité, clarté et transparence, nous traitons les données personnelles avec respect et exemplarité dans le cadre de relations de confiance. Les orientations d'Innoha visent à développer ses services dans un environnement qui connaît des mutations accélérées tant sur le plan technique que réglementaire. La protection des données est ainsi une priorité pour nous. Ayant intégré la constante évolution des menaces et des risques de sécurité, Innoha positionne la sécurité au quotidien au cœur de ses préoccupations. Cette politique s'applique à l'ensemble du Groupe Innoha.

COMMENT COLLECTONS-NOUS LES DONNEES PERSONNELLES ?

Dans le cadre de la réalisation de nos activités, nous collectons et traitons certaines données personnelles. La communication des données personnelles est volontaire et ne constitue en aucun cas une condition obligatoire ou une injonction. Ces données personnelles sont recueillies directement auprès des personnes, ou indirectement.

QUELLES SONT LES DONNEES PERSONNELLES QUE NOUS COLLECTONS ?

Les données que nous collectons en interne et en externe sont, à titre d'exemple :

- Des informations relatives à l'identification : nom, prénom, civilité ;
- Des coordonnées : adresse, téléphone, e-mail ;
- Des informations professionnelles : entreprise, poste ;
- Les informations soumises avec les candidatures ;

S'il apparaît nécessaire pour nous de collecter ou d'utiliser des catégories particulières de données personnelles (« données sensibles »), nous demandons aux personnes concernées d'y consentir expressément.

Nous sommes vigilants à la protection de la vie privée des mineurs. Nous ne collectons pas intentionnellement les données personnelles de personnes mineures.

COMMENT UTILISONS-NOUS LES DONNEES PERSONNELLES ?

Nous n'utilisons les données personnelles que si cette utilisation repose au moins sur une base légale précisée ci-dessous :

- Le respect d'une obligation légale incombant à Innoha ;
- La protection des intérêts légitimes de Innoha ;
- L'exécution d'un contrat conclu ou des mesures précontractuelles prises à la demande de la personne concernée par le traitement ;
- Le consentement donné par la personne concernée par le traitement.

Nous traitons les données personnelles afin de, notamment :

- Répondre à vos demandes d'informations ;
- Gérer des demandes d'inscription à des conférences ou évènements ;
- Évaluer des candidatures et recruter ;
- Distribuer des newsletters, articles, informations et des alertes ;

- Améliorer notre qualité de service ;
- Diffuser des offres commerciales en B2B.

LE TRAITEMENT DE DONNEES PERSONNELLES DANS LE CADRE DE NOS MISSIONS :

Nous sommes également susceptibles de traiter des données personnelles dans le cadre des prestations que nous réalisons pour nos clients, et ce conformément à nos engagements contractuels. Dans ce cas, les données sont exclusivement traitées dans la limite du cadre défini par la mission. Nous mettons en place des mesures organisationnelles et techniques de sécurité afin de limiter l'accès aux données et garantir la confidentialité des informations traitées dans le cadre bien spécifique inhérent à nos prestations.

QUI SONT LES DESTINATAIRES DES DONNEES PERSONNELLES ?

Les données recueillies sont destinées aux services d'Innoha. Elles peuvent également être transmises à des tiers, comme des prestataires auxquels nous pourrions confier la réalisation de certaines activités (par exemple la gestion de la paie…).
Innoha peut être sollicité par les autorités afin de transmettre des données personnelles. Nous nous assurons de disposer (y compris auprès de nos partenaires et prestataires) de garanties suffisantes en matière de protection des données personnelles à chaque transfert de données.

QUI EST RESPONSABLE DES DONNEES PERSONNELLES EN CAS DE LIEN VERS UN SITE TIERS ?

Si lors de la navigation sur notre site internet, Innoha fournit un lien vers un site tiers, les règles et politiques applicables à ce site s'appliqueront.
En aucun cas Innoha ne pourra être tenu responsable du traitement de vos données personnelles par un site tiers.

OU SONT STOCKEES ET TRAITEES LES DONNEES PERSONNELLES ?

La législation en matière de réglementation sur les données n'étant pas équivalente entre les pays, Innoha a fait le choix de privilégier l'hébergement et le traitement des données sur le territoire français, ou le cas échéant un pays de l'Union Européenne, ou de contractualiser avec une entreprise respectant les Clauses Contractuelles Types de la Commission Européenne.

COMBIEN DE TEMPS SONT CONSERVEES LES DONNEES PERSONNELLES ?

Les données concernées par des traitements sont conservées en respectant un ensemble de règles. Nous ne traitons que des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Cela entraîne, notamment, de garantir que la durée de conservation des données soit limitée au strict minimum. Cette durée de conservation est variable et dépend de la nature des données, de leur finalité et des aspects légaux et réglementaires auxquels elles sont soumises.

COMMENT SONT PROTEGEES VOS DONNEES PERSONNELLES ?

Innoha s'assure que les traitements de données personnelles bénéficient du meilleur niveau de sécurité. Nous garantissons la mise en œuvre de « mesures techniques et organisationnelles appropriées », prises en fonction de la nature des données, des finalités du traitement et des risques associés. En cas d'un incident conduisant à une violation des données personnelles, Innoha notifie l'incident à l'autorité de contrôle compétente et informera, si nécessaire, les personnes concernées dans les meilleurs délais.

QUELS SONT LES DROITS DES PERSONNES ?

Conformément à la réglementation applicable en matière de protection des données, toute personnes dont les données personnelles font l'objet d'un traitement de notre part disposent des droits suivants :

- D'UN DROIT D'ACCES ET DE COMMUNICATION SUR LES INFORMATIONS LES CONCERNANT ET LES TRAITEMENTS ASSOCIES ;
- D'UN DROIT DE RECTIFICATION AVEC UNE POSSIBILITE DE COMPLETER ET DE METTRE A JOUR LEURS INFORMATIONS ;
- D'UN DROIT A LA PORTABILITE AFIN DE TRANSMETTRE LES INFORMATIONS CONCERNANT LA PERSONNE EN FAISANT LA DEMANDE A UN TIERS LORSQUE CELA EST TECHNIQUEMENT POSSIBLE, ETANT PRECISE QUE CE DROIT N'EST APPLICABLE QU'AUX DONNEES FOURNIES DIRECTEMENT PAR LA PERSONNE ;
- D'UN DROIT A LA DETERMINATION DU SORT DE LEURS DONNEES EN CAS DE DECES ;
- D'UN DROIT D'EFFACEMENT DES DONNEES ;
- D'UN DROIT A LA LIMITATION DU TRAITEMENT QUI LEUR EST RELATIF ;
- D'UN DROIT D'OPPOSITION AU TRAITEMENT ;
- D'UN DROIT AU RETRAIT DU CONSENTEMENT POUR L'UTILISATION DE LEURS DONNEES.

Nous portons à votre connaissance le fait que lorsque la loi l'impose, dans le cas du respect de ses obligations contractuelles, de l'intérêt public, ou l'intérêt légitime, Innoha se réserve à titre exceptionnel le droit de ne pas honorer certains contenus de demandes (liés à une demande de suppression, de limitation, et d'opposition).

Par ailleurs, dans les cas de demandes manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, Innoha peut soit :

- EXIGER LE PAIEMENT DE FRAIS RAISONNABLES QUI TIENNENT COMPTE DES COUTS ADMINISTRATIFS SUPPORTES POUR FOURNIR LES INFORMATIONS, PROCEDER AUX COMMUNICATIONS OU PRENDRE LES MESURES DEMANDEES ;
- REFUSER DE DONNER SUITE A CES DEMANDES.

Toutefois, il incombe à Innoha de démontrer le caractère manifestement infondé ou excessif de ces demandes.

COMMENT PEUVENT-ELLES EXERCER LEURS DROITS VIS-A-VIS D'INNOHA ?

Toute personne peut exercer ses droits, en joignant à leur demande une copie d'un titre d'identité soit :

- PAR VOIE POSTALE, A L'ADRESSE : INNOHA DPO, 8 RUE DE BERRI, 75008, PARIS, FRANCE
- PAR COURRIER ELECTRONIQUE : CONTACT@INNOHA.COM OU DPO@INNOHA.COM

Innoha dispose d'un délai d'un mois pour y répondre. En cas de demande complexe ou d'un nombre important de demandes, ce délai pourra être porté à trois mois. Le cas échéant, nous informerons les personnes concernées.

Si malgré toute l'attention que Innoha porte au traitement des données personnelles, une personne concernée par ce traitement constate que nous n'apportons pas satisfaction à sa demande, nous l'informons qu'elle peut adresser une réclamation auprès de la CNIL (Commission Nationale de l'Informatique et des Libertés) : www.cnil.fr ; 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07.

E. ENGAGEMENTS ET MOYENS MIS EN ŒUVRE EN MATIERE DE PREVENTION DU RISQUE NUMERIQUE

LES 4 POINTS FORTS DE NOS ENGAGEMENTS PRIS VIS A VIS DE L'ADMINISTRATION

On dit souvent que l'on doit se transformer pour ne pas disparaître, c'est particulièrement vrai en matière de risque numérique ! Parce que demain, l'organisation responsable et génératrice de confiance sera celle qui s'attache à maitriser le risque numérique, nous nous employons, avec nos Clients, à le comprendre pour mettre en œuvre les mesures nécessaires. Nous sommes convaincus que seule une approche holistique permet de progresser dans la maîtrise des risques et la définition de standards pour nos Clients comme pour nous. Plus qu'une contrainte, nous voyons dans l'apparition de ce risque et dans l'ensemble des initiatives prises pour en assurer une certaine maitrise un réel avantage compétitif.

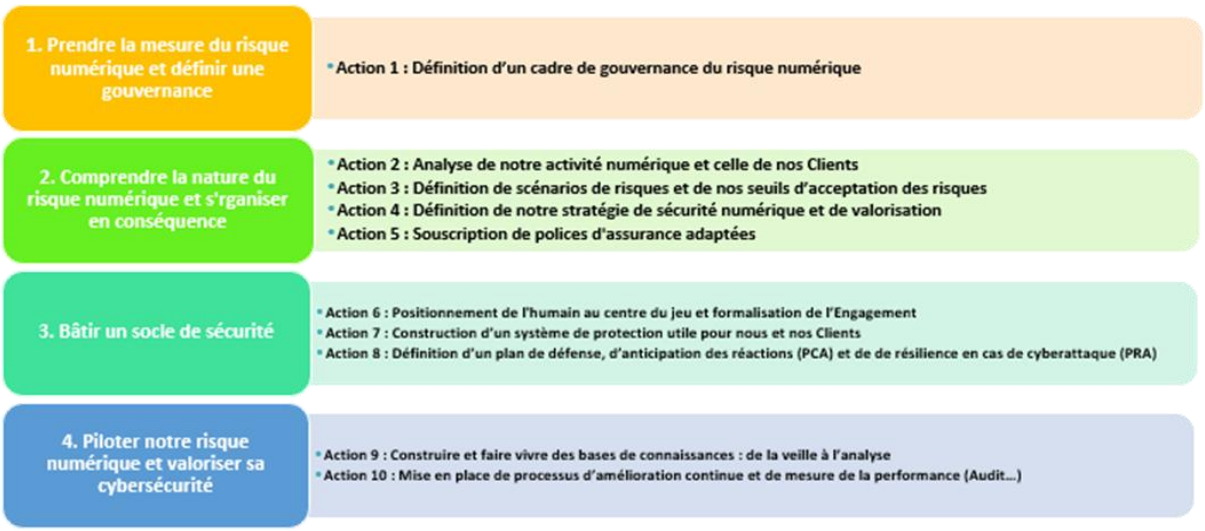
Le risque numérique est vraiment devenu incontournable, mais, comme tout acteur économique, nous nous attachons à le maitriser !
Basée notamment par les recommandations de l'AMRAE et de l'ANSSI ainsi que par nos expériences Clients et de nombreux benchmarks, la démarche que nous mettons en œuvre et qui sous-tend nos engagements permet de :

Cette démarche a été déclinée opérationnellement en 10 actions permettant d'adresser l'ensemble des questions relatives notamment aux points qui vous intéressent plus particulièrement, à savoir :

- La non-conformité par rapport au cadre de cohérence technique
- La dépendance et ses corollaires en matière de propriété intellectuelle, de réversibilité complexe et d'information critique
- La gestion des données relatives aussi bien à la protection des informations ministérielles, à la protection des données personnelles ou à la protection des différents niveaux de secret de la défense nationale
- La sécurité des systèmes d'information que ce soit en matière d'intégration au SI ministériel, de SSI ou de cyber.

MOYENS MIS EN ŒUVRE POUR SATISFAIRE LES OBLIGATIONS EN MATIERE DE PREVENTION DU RISQUE NUMERIQUE

Voici en synthèse les 10 actions mises en œuvre par INNOHA qui sous-tendent nos engagements et permettent de garantir l'accompagnement de l'Administration pour aider à prévenir les risques numériques :



Revenons en détail sur les actions de chaque engagement.

1er point fort : Prendre la mesure du risque numérique et définir une gouvernance

Pour être efficace, une politique de management du risque numérique nécessite d'être comprise et soutenue par l'ensemble des parties prenantes de l'organisation, à commencer par son équipe dirigeante.
L'évolution du risque numérique dans l'organisation engage dorénavant la responsabilité du dirigeant vis-à-vis de sa gestion et de son traitement. Cette responsabilité est accentuée par les réglementations actuelles : Règlement général sur la protection des données (RGPD), Directive européenne Network and Information Security (NIS).

Pour acquérir cette vision holistique des risques et veiller à ce qu'ils soient clairement corrélés aux objectifs de notre organisation, un comité des risques numériques a été mis en place au sein de notre société. Une attention particulière est portée quant à sa capacité à s'affranchir des silos fonctionnels, métiers et opérationnels existants. C'est cette culture et cette expérience que nous transposons de fait chez nos Clients.

Son rôle est de définir la stratégie de sécurité numérique de notre organisation, de s'assurer de sa mise en œuvre, de piloter la performance et de valoriser les investissements réalisés.

Il est présidé par notre Directeur Général et accueille un représentant de chacune de nos trois lignes de défense.

L'objectif du comité est de mettre en œuvre la stratégie de sécurité numérique en s'appuyant sur une connaissance actualisée des risques numériques qui pèsent sur les activités de notre société. Les missions du comité sont de :

- Rédiger et maintenir à jour la Politique de Sécurité des Systèmes d'Information (PSSI) qui régit la gestion du risque numérique.
- Définir la stratégie de sécurité numérique de l'organisation et les investissements nécessaires à sa mise en œuvre.
- Veiller en priorité à la sécurité des services numériques les plus critiques. Ces services ou ces systèmes d'information font l'objet d'une homologation de sécurité.
- Assurer le pilotage de la performance et l'amélioration continue de la gestion du risque numérique.
- Définir une stratégie de valorisation des investissements réalisés dans le champ de la sécurité numérique.

2ème point fort : Comprendre la nature du risque numérique et s'organiser en conséquence

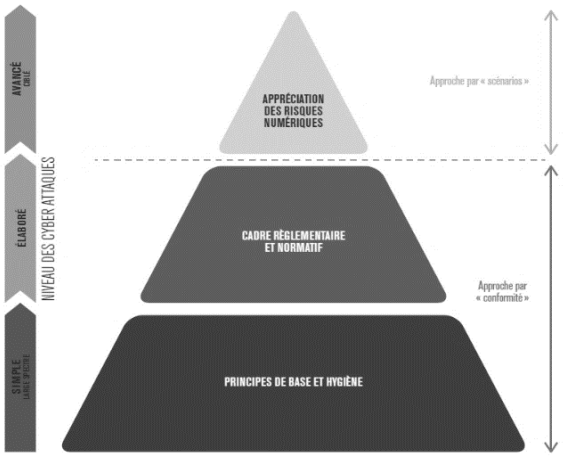
Dans cet objectif, nous avons mené les actions suivantes :

- Cartographier nos activités principales, nos services numériques et nos systèmes d'information les plus essentiels.
- Imaginer des scénarios de risques pour identifier nos services numériques et nos systèmes d'information qui doivent faire l'objet d'une attention spécifique du comité.
- Cartographier notre écosystème Clients afin d'avoir une vision de ses interactions et de ses flux.

Pour les services numériques les moins critiques, les mesures de sécurité qui s'appliquent de manière systématique reposent sur une approche par conformité aux normes et bonnes pratiques et sur la construction d'un socle de sécurité.

3ème point fort : Bâtir un socle de sécurité

Pare-feu Humain : Nos consultants sont à l'origine et au cœur du dispositif. Parce qu'ils sont le plus souvent « sur le terrain » au plus près des Clients, ils sont souvent une cible privilégiée des attaquants. En incluant pleinement le facteur humain dans notre PSSI, nous obtenons de nos collaborateurs une participation active à la sécurité numérique de notre organisation suivie de résultats rapides et significatifs.



Pour y parvenir, nous avons mené des actions de sensibilisation auprès de nos consultants et la conduite d'exercices réalistes sont annuellement organisées avec les membres du siège. L'enjeu est de développer une véritable culture de la sécurité numérique de telle sorte que les collaborateurs INNOHA, appuyés de procédures de sécurité, parviennent à déjouer les pièges les plus courants tendus par les attaquants.

Protéger nos activités et celles de nos Clients passe par la mise en œuvre de mesures de sécurité. Ces mesures se situent au carrefour de considérations organisationnelles, numériques et physiques. Elles sont sélectionnées sur la base d'une approche par conformité vis-à-vis des différents référentiels de sécurité (légal, réglementaire, etc.) s'appliquant à l'organisation (Cf. Pyramide de management du risque numérique – Méthode EBIOS).

Depuis plusieurs années, nos Clients ont entamé leur révolution numérique à travers l'accélération de la collaboration des équipes et la redéfinition des relations avec leurs clients, leurs partenaires et leurs fournisseurs. Dans ce contexte et en tant que prestataire de services, INNOHA a dû s'adapter pour relever des nouveaux défis en matière de prévention du risque numérique, de sécurité et de gouvernance des données, accentués par l'importance stratégique de ces secteurs. En effet, l'usage professionnel et personnel des moyens informatiques (ordinateurs et téléphones mobiles, tablettes, supports amovibles, etc.) mis à disposition de nos Consultants par INNOHA ou nos Clients, les déplacements et l'accès à des réseaux sans-fil dans notre organisation ou en dehors, sont autant de sources de menaces pour notre système d'information et celui de nos Clients.

Mesures de sécurité des équipements communicants et des données : INNOHA a ainsi dû anticiper ces situations pour mettre en œuvre les actions nécessaires ci-dessous afin d'avoir un contrôle total sur ses données et celles de ses Clients, de fournir les garanties de sécurité essentielles à la réussite de ses relations Clients et satisfaire ses obligations en matière de prévention du risque numérique.

Nomination d'un correspondant/référent pour la sécurité informatique d'INNOHA
Rédaction d'une charte informatique
Chiffrement de nos données et de nos échanges d'informations Clients sensibles à l'aide d'un logiciel de chiffrement certifié ANSSI : Solution OODRIVE WORK
Renforcement de la configuration de nos postes et utilisations de solutions de sécurité éprouvées (pare-feu, antivirus)
Analyse par anti-virus des fichiers provenant de supports USB sur nos ordinateurs
Désactivation de l'exécution automatique des supports amovibles depuis nos ordinateurs
Extinction et sécurisation physique des ordinateurs pendant les périodes d'inactivité prolongée (nuit, weekend, vacances)
Surveillance et monitoring de notre système en relation avec notre partenaire Dryve Informatique (en charge de la gestion de notre parc informatique), notamment en utilisant les journaux d'événements, pour réagir aux

événements suspects (connexion d'un utilisateur hors de ses horaires habituels, transfert massif de données vers l'extérieur de l'entreprise, tentatives de connexion sur un compte non actif).

Mesures physiques de protection : La maîtrise du risque numérique passe aussi par la maîtrise de son environnement physique et de ses locaux. Un contrôle d'accès physique à nos locaux et nos systèmes d'information a donc été mis en œuvre et associé à un système de vidéo protection.

Qualifier une cyberattaque consiste à identifier les activités et biens supports affectés par l'attaque et, surtout la gravité de ces impacts. Il s'agit alors de réagir, de traiter et de classer les incidents. Pour ce faire, nous avons défini une procédure d'escalade pour gérer les incidents au juste niveau de responsabilité et décider du déclenchement ou non de la cellule de crise pour répondre aux questions suivantes :

- Que faire lors de la détection d'un incident ?
- Qui alerter ?
- Quelles sont les premières mesures à appliquer ?
- Quelle est l'impact de la cyberattaque sur le fonctionnement de mon organisation ?

Communication de crise : la communication de crise fait également partie intégrante de notre dispositif de gestion de crise. Nous avons mené un travail d'anticipation, tant sur le volet organisationnel (définition d'un dispositif de communication de crise) que sur le volet opérationnel (identification de scénarios types, définition de plans de communication dédiés, préparation d'éléments de réponse clés en main, etc.).

PCA : Notre PCA vise à garantir la survie d'INNOHA à la suite d'une cyberattaque. Il organise le redémarrage de nos activités le plus rapidement possible avec le minimum de perte d'informations, avec ou sans l'assistance de notre prestataire informatique Dryve. Notre PCA prend appui sur l'étude des scénarios de risques identifiés. Il constitue un chapitre essentiel de notre politique de sécurité, est revu et enrichi semestriellement, est testé à intervalles réguliers pour rester efficace.

PRA : L'objectif de notre PRA est de procéder à la reconstruction des systèmes d'information et des données afin de redémarrer les applications et processus métiers le plus rapidement possible en cas de cyberattaque critique. Notre PRA est constitué d'un ensemble de procédures techniques, organisationnelles et de sécurité et s'appuie sur des partenaires et prestataires externes. Notre PRA prend également appui sur l'étude des scénarios de risques identifiés. Intégré à notre politique de sécurité de l'organisation, il est revu, challengé et enrichi semestriellement.

Police d'assurance : Notre police d'assurance souscrite nous permet de bénéficier de ressources juridiques spécifiques supplémentaires pour nous aider à gérer la crise et revenir au plus vite à une situation normale. Selon la couverture d'assurance choisie et la gravité de l'incident, les ressources suivantes peuvent intervenir. Elle doit également nous permettre de faire face aux frais potentiels engendrés pour compenser les dommages causés à nos tiers du fait de l'incident survenu. C'est pour nous un aspect essentiel pour préserver notre réputation et notre crédibilité vis-à-vis de de nos parties prenantes.

Prévention contractuelle : Pour maîtrise notre exposition à des poursuites de la part de partenaires, qui pourraient engager la responsabilité de notre dirigeant et impacter notre réputation nous sommes particulièrement attentifs à la qualité :

- Des contrats établis avec nos tiers et notamment nos sous-traitants (la juridiction applicable des éléments contractuels, la responsabilité civile professionnelle, les annexes de sécurité) ;
- Du « plan d'assurance sécurité ».

4ème point fort : Piloter notre risque numérique et valoriser sa cybersécurité

Veille : Notre comité des risques numériques s'assure de la mise en place d'une démarche de veille de l'information continue et itérative. Cette stratégie de veille a pour objectif :

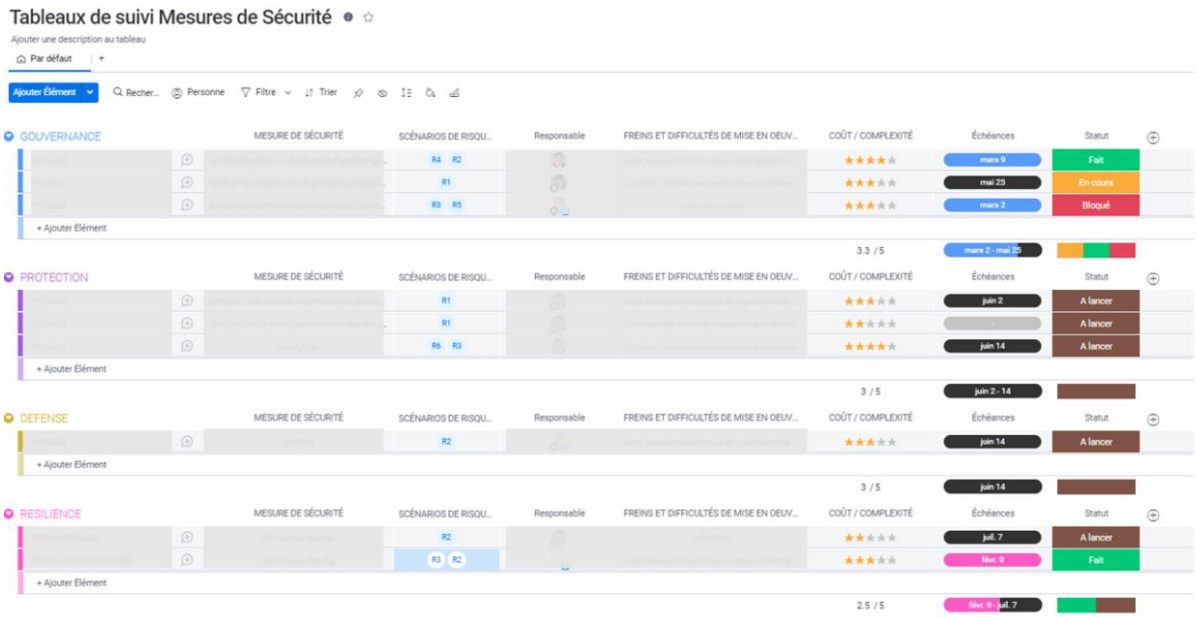
- De maintenir à jour des connaissances de notre organisation vis-à-vis de notre écosystème (concurrence, e-réputation, aspects juridiques, capacité technologique, développement numérique, etc.), des sources de menace et méthodes d'attaques.
- D'aider le comité des risques numériques dans sa prise de décision face à de nouvelles menaces, vulnérabilités ou contraintes légales et réglementaires.
- De communiquer les résultats (informations économiques, politiques, enjeux de sécurités, pertes financières, etc.) de cette veille auprès de nos collaborateurs, clients et autres parties prenantes.
- De maintenir les compétences de nos collaborateurs dans le temps.

Audit : Les audits et contrôles portent sur la conformité de nos mesures organisationnelles, numériques ou physiques. Ils mettent en évidence les points de vigilance et de non-conformité à l'égard des référentiels. Notre stratégie d'audit et de contrôle est revue semestriellement pour y intégrer les éventuelles évolutions de l'organisation et de notre environnement.

Démarche itérative d'amélioration continue : En inscrivant notre stratégie de gestion du risque numérique dans cette démarche, notre organisation s'adapte aux nouvelles menaces, renforce son socle de sécurité et maitrise ses investissements. Elle est portée par le comité des risques numériques et s'appuie sur :

- La stratégie de veille de l'information ;
- Son outil Monday pour piloter la performance (indicateurs, tableaux de suivis et tableau de bord) ;
- Les résultats des actions de contrôle et d'audit.
- Le PACS qui documente l'ensemble des mesures de traitement

En intégrant la connaissance des nouvelles menaces, les objectifs de la stratégie de sécurité numérique et la correction des non-conformités d'audits, INNOHA est en mesure d'adapter de manière dynamique sa stratégie de gestion du risque et donc d'accompagner également ses Clients sur ce sujet. INNOHA est ainsi en capacité de faire évoluer son organisation de manière agile, d'anticiper le risque numérique et ses impacts.



Pour permettre au comité des risques numériques de piloter ce risque, nous l'avons doté d'outils de mesure prenant la forme d'indicateurs (stratégiques, de pilotage, opérationnels, organisationnels ou techniques). Pour

être pleinement exploitables, ces données sont intégrées dans des tableaux de bord dynamiques via notre Work OS Monday (Cf. exemple ci-dessous avec notre Tableau de suivi des Mesures de Sécurité – anonymisé) pour disposer d'une représentation visuelle de l'atteinte des objectifs et ainsi faire émerger les tendances ou les dérives.

MOYENS MIS EN ŒUVRE POUR SATISFAIRE LES OBLIGATIONS EN MATIERE DE PROTECTION DU SECRET DE LA DEFENSE NATIONALE

Le pilotage et la mise en œuvre de la protection du secret de la défense nationale repose sur plusieurs acteurs institutionnels. Leurs relations forment une « chaîne » dite de protection du secret. INNOHA s'inscrit dans cette chaîne de protection. En effet, en tant qu'organisme privé dont le personnel a et/ou aura accès à des informations protégées, INNOHA dispose d'un officier de sécurité (OS).

Ce dernier aura dans le cadre de l'exécution de nos prestations un rôle clé puisqu'il aura en charge :

- La gestion des habilitations ;
- La sensibilisation les personnels concernés aux mesures de protections ;
- La validation de l'effectivité du contrôle de l'accès aux zones réglementées ainsi que du respect des dispositions réglementaires applicables ;
- La conformité de la manipulation, de la conservation, de la reproduction, du transport et, le cas échéant, de la destruction des informations ou supports classifiées ;
- La sécurité des systèmes d'information classifiés en s'appuyant sur l'officier de sécurité des systèmes d'information.

Dans le cas exceptionnel où nous serions amenés à traiter des informations classifiées sur notre système d'information, notre officier de sécurité des systèmes d'information (OSSI) jouera un rôle prépondérant puisqu'il sera responsable de :

- La mise en œuvre du management de la sécurité de nos systèmes d'information
- La définition des exigences de sécurité et en contrôle l'application
- La sensibilisation les personnels aux mesures de protection liées à l'utilisation de ces systèmes.