ANNEXES

1- Formulaire de déclaration d'intérêts
2- Charte de bonnes pratiques professionnelles
3- Modèle de délégation de signature
4- Charte informatique à destination des salariés
5- Charte informatique à destination des élus
6- Modèle de délégation de pouvoir
7- Modèle de convocation à une réunion du Conseil
8- Modèle de lettre de démission d'office

Annexe 1 : Formulaire de déclaration d'intérêts

Déclaration d'intérêts de l'élu ordinal

(Déclaration à adresser au Président du Conseil national de l'ordre des infirmiers 228 rue du Faubourg Saint-Martin, 75010 PARIS)

Je soussigné (e)
Nom :
Prénoms :
Numéro ordinal et/ou RPPS :

1- Activités professionnelles

☐ Activité libérale

☐ Exercice dans l'une des trois Fonctions publiques (hospitalière, territoriale ou de l'Etat)

☐ Exercice dans le secteur privé

Autres situations

☐ Bénévole

☐ Retraité(e) sans activité

☐ Retraité(e) avec une activité

☐ Réserve sanitaire

2- Mandats ordinaux (préciser de la durée du mandat)

☐ Elu (e) au conseil départemental/interdépartemental de :

☐ Elu (e) au conseil régional/interrégional de :

☐ Elu (e) au conseil national de l'ordre des infirmiers

3- Fonctions d'assesseurs d'une chambre disciplinaire ou de la section des assurances sociales

☐ Elu (e) assesseur à la chambre disciplinaire de 1ère instance de :

☐ Elu (e) assesseur à la chambre disciplinaire nationale

☐ Désigné (e) assesseur à la section des assurances sociales de 1ère instance de :

☐ Nommé (e) assesseur à la section des assurances sociales nationale

4- Fonctions au sein d'un syndicat infirmiers

☐ Elu (e) président du syndicat :

☐ Elu (e) vice-président du syndicat :

☐ Elu (e) Secrétaire général du syndicat :

☐ Elu (e) trésorier du syndicat :

☐ Autre – Préciser le cadre

5- Autres fonctions électives

Préciser la nature et la durée du ou des mandats et le nom de la ou des organisations :

6- Autres activités à l'exclusion des missions de service public

Je déclare avoir perçu pendant les cinq années écoulées des revenus provenant d'activités (ou des parts) dans des organismes et/ou sociétés commercialisant des produits ou services en lien avec la santé et/ou des sociétés prestataires (Préciser le nom et l'objet social de ou des organisme(s) ou société(s) ou le nombre de parts, la fonction occupée et/ou l'objet de la mission).

Organisme / société / service…	Fonction occupée	Rémunération	Début (mois/ année)	Fin (mois/année)
		☐ Aucune ☐ Au déclarant ☐ A un organisme dont vous êtes membre ou salarié (préciser)		
		☐ Aucune ☐ Au déclarant ☐ A un organisme dont vous êtes membre ou salarié (préciser)		

7- Autre lien (parents ou proches)

Je déclare avoir un lien de parenté ou d'alliance avec une ou de(s) personne(s) salariée(s) et/ou possédant des intérêts financiers dans des organismes et/ou sociétés commercialisant des produits ou services en lien avec la santé et/ou de sociétés prestataires de services de l'Ordre (Préciser le degré de parenté et l'objet social de ou des organisme(s) ou société(s), la fonction occupée).

Organisme / société / service…	Fonction occupée	Lien de parenté

Je soussigné (e), certifie l'exactitude des renseignements fournis dans la présente déclaration. Je m'engage à actualiser ma déclaration d'intérêts chaque fois que ces informations sont caduques et/ou doivent être complétées. Cette déclaration ne me décharge pas de mon obligation de me récuser ou de me désister, si j'estime que j'ai des liens susceptibles d'être considérés comme pouvant porter atteinte à mon indépendance, à l'occasion d'une mission ou d'une délibération du conseil.

Fait à ……..le……

Signature obligatoire

Conformément à la loi du 6 janvier 1978 modifiée, vous disposez d'un droit d'accès et de rectification de données vous concernant. Vous pouvez exercer ce droit auprès du Conseil national.

Annexe 2 : Charte des bonnes pratiques professionnelles

Bonnes pratiques professionnelles

Cette charte regroupe les attitudes et les objectifs que l'Ordre souhaite voir adopter par l'ensemble de ses ressources humaines, **relations entre collaborateurs et relations entre collaborateurs et élus ordinaux**, afin de créer un environnement de travail sain, harmonieux et stimulant.

1. Adopter une attitude relationnelle respectueuse

De fait, pour que cette charte génère les résultats escomptés, l'adhésion de chacun et son engagement à la respecter et le promouvoir quotidiennement dans le cadre de son activité (salariée ou ordinale) sont essentiels.
Au-delà des tâches à accomplir, ce sont la qualité des relations interpersonnelles et la façon dont chacun collabore avec les autres qui influencent le climat au sein de notre institution.

Vis-à-vis des autres, je m'engage à faire preuve de :

1.1 Respect

- Respect des autres, de leur travail et de leurs valeurs : compréhension et acceptation des différences de chacun ;
- Respecter les décisions fixées par les instances de l'Ordre National des Infirmiers, représentant les infirmiers ;
- Respecter la profession d'infirmier ;
- Respecter la hiérarchie ;
- Respect des règles élémentaires de civilité : « bonjour, merci, s'il vous plait » doivent faire partie du vocabulaire quotidien ;
- Respect de l'équilibre « vie au travail – vie privée » choisi par un collègue/collaborateur/manager ;
    - Les sollicitations le week-end, le soir et durant les congés doivent relever de l'exceptionnel ;
    - Les sollicitations sur le téléphone personnel doivent relever de l'exceptionnel ;
    - Etre attentif à ne pas transférer ses urgences sur les autres : savoir définir conjointement les objectifs prioritaires, hiérarchiser les actions ;
    - Intégrer des délais réalistes de réalisation, planifier les demandes et ne pas céder au tout urgent.

1.2 Engagement

- S'impliquer et inscrire son travail dans une démarche collective et dans les missions de l'institution ;
- Participer au développement d'un esprit d'équipe et savoir travailler ensemble en bonne intelligence ;
- Privilégier le dialogue et l'échange verbal ;
- Être capable de maitriser ses émotions, de comprendre celles des autres pour éclaircir les malentendus et résoudre les conflits ;
- Faire son possible pour ne pas pénaliser l'avancée d'un projet, s'engager à informer de difficultés face à une demande à laquelle on ne pourrait pas répondre, s'engager à trouver des solutions alternatives face aux difficultés ;
- Accepter des solutions alternatives.

2. Résister à une utilisation abusive et inappropriée du « @ »

2.1. Considération :

- Acceptation du droit à l'erreur ;
- Être à l'écoute de chacun pour pouvoir détecter des signes de mal-être de chacun ;
- Encouragement et reconnaissance du travail accompli ;
- Confiance, encouragement de l'autonomie et de l'initiative ;
- Coopération et valorisation de la participation et du travail d'équipe.

2.2. Privilégier la rencontre en direct :

- Elle génère conversation et compréhension ;
- Elle entraîne plus facilement confiance et par la suite modération des propos écrits.

2.3. Rester courtois dans sa communication électronique :

- Ecrire intelligiblement :
  - Soigner la rédaction et préciser l'objet du message ;
  - Faire des phrases courtes : sujet, verbe, complément ;
  - En cas de transfert de mail, penser à rédiger quelques mots d'explications dans le message
  - Éviter les mots tout en majuscules ou gras. Une telle utilisation peut être mal perçue par le destinataire ;
  - Un nouveau sujet = un nouveau courriel ;
- Ne pas oublier de mettre un message automatique en cas d'absence pour prévenir de son absence et réorienter vers un autre interlocuteur ;
- Ne pas croire qu'un conflit peut se régler rapidement et efficacement par mail. Privilégier l'oral ou le face à face ;
- Eviter le principe abusif de protection et ne mettre en copie que les personnes vraiment concernées et directement impliquées par le sujet ;
  - Les destinataires des mails sont les acteurs, ils sont donc en nombre limité ;
  - Les personnes en copie des mails le sont pour information.

2.4. Ne pas céder à l'instantanéité de la messagerie :

- Gérer les priorités et ne pas répondre immédiatement à chaque mail reçu ;
- Une demande faite par mail devra respecter un délai de traitement raisonnable ; ne constitue pas un délai raisonnable un mail envoyé à 20 h pour un retour le lendemain 9 h ;
- Ne pas lire ses mails en réunion.

3. Respecter des règles communes de rythme de travail

3.1. Se conformer au rythme de travail :

- Respecter les périodes de pause, les horaires et les jours de travail des salariés ;
- Les périodes d'absence doivent être respectées par tous (ne pas solliciter un collaborateur pendant ses congés ou arrêt de travail) ;
- L'ensemble des jours de congés doivent être posés dans l'année.

4. Avoir connaissance des comportements proscrits par la loi

4.1. Le harcèlement moral

Rappel du cadre législatif :

« *Aucun salarié ne doit subir les agissements répétés de harcèlement moral qui ont pour objet ou pour effet une dégradation de ses conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel.* » Article L. 1152-2 du Code du travail.
« *Le **fait de harceler autrui** par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel, **est puni de deux ans d'emprisonnement et de 30 000 € d'amende*** ». Article 222 -33-2 du Code pénal.

- **Il peut prendre des formes variées tels que :**
    - Dénigrement systématique du travail accompli ;
    - Insultes, menaces, propos dégradants ou chantage, rétrogradation sans justification ;
    - Mise à l'écart répétée, volonté manifeste d'ignorer ;
    - Obligation d'accomplir des tâches humiliantes ou sans aucun rapport avec le poste occupé ;
    - Isolement, interdiction d'entretenir des relations sociales avec d'autres collaborateurs.

- **Ne pas confondre avec**
    - **Harcèlement moral et exercice légitime du pouvoir de direction** : confier une tâche et exiger des résultats dans le cadre de travaux habituels, demander à un salarié de justifier ses absences ou un non-respect des horaires de travail, prendre des mesures disciplinaires à l'égard d'un collaborateur fautif ;
    - **Harcèlement moral et comportement inapproprié :** un incident isolé ou un comportement inapproprié occasionnel ne constitue pas un harcèlement.

Pour caractériser un harcèlement, il faut que ce mode de comportement s'inscrive dans le temps. Pour savoir si un comportement est inapproprié, vous pouvez vous poser la question suivante :
« *Accepterai-je d'être traité ainsi par un supérieur hiérarchique direct ? »*

4.2. Le harcèlement sexuel

Rappel du cadre législatif :

« Aucun salarié ne doit subir des faits :
1° Soit de harcèlement sexuel, constitué par des propos ou comportements à connotation sexuelle répétés qui soit portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante ; 2° Soit assimilés au harcèlement sexuel, consistant en toute forme de pression grave, même non répétée, exercée dans le but réel ou apparent d'obtenir un acte de nature sexuelle, que celui-ci soit recherché au profit de l'auteur des faits ou au profit d'un tiers. » Article L. 1153-1 du Code du travail

« I. - Le harcèlement sexuel est le fait d'imposer à une personne, de façon répétée, des propos ou comportements à connotation sexuelle ou sexiste qui soit portent atteinte à sa dignité en raison de leur caractère dégradant ou humiliant, soit créent à son encontre une situation intimidante, hostile ou offensante.

L'infraction est également constituée :

1° Lorsque ces propos ou comportements sont imposés à une même victime par plusieurs personnes, de manière concertée ou à l'instigation de l'une d'elles, alors même que chacune de ces personnes n'a pas agi de façon répétée ;

2° Lorsque ces propos ou comportements sont imposés à une même victime, successivement, par plusieurs personnes qui, même en l'absence de concertation, savent que ces propos ou comportements caractérisent une répétition.

II. - Est assimilé au harcèlement sexuel le fait, même non répété, d'user de toute forme de pression grave dans le but réel ou apparent d'obtenir un acte de nature sexuelle, que celui-ci soit recherché au profit de l'auteur des faits ou au profit d'un tiers.

III. - Les faits mentionnés aux I et II sont punis de deux ans d'emprisonnement et de 30 000 € d'amende.

Ces peines sont portées à trois ans d'emprisonnement et 45 000 € d'amende lorsque les faits sont commis :

1° Par une personne qui abuse de l'autorité que lui confèrent ses fonctions ;

2° Sur un mineur de quinze ans ;

3° Sur une personne dont la particulière vulnérabilité, due à son âge, à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse, est apparente ou connue de leur auteur ;

4° Sur une personne dont la particulière vulnérabilité ou dépendance résultant de la précarité de sa situation économique ou sociale est apparente ou connue de leur auteur ;

5° Par plusieurs personnes agissant en qualité d'auteur ou de complice ;

6° Par l'utilisation d'un service de communication au public en ligne ou par le biais d'un support numérique ou électronique ;

7° Alors qu'un mineur était présent et y a assisté ;

8° Par un ascendant ou par toute autre personne ayant sur la victime une autorité de droit ou de fait. »

Article 222-33 du Code pénal

- **Les comportements suivants peuvent constituer des faits de harcèlement sexuel :**
    - Promesse de récompense (augmentation, embauche…) en échange de l'acceptation de demandes à caractère sexuel, ou menaces de représailles en cas de refus de telles demandes ;
    - Répétition de propos grossiers, suggestifs ou d'insinuations à caractère sexuel : utilisation d'un langage cru ou de gestes obscènes ;
    - Contacts physiques (prise de main insistante, embrassade appuyée, frôlements…) non souhaités ;
    - Voyeurisme, exhibitionnisme, envoi de matériel informatique ;
    - Commentaires répétés sur l'aspect physique ou les tenues vestimentaires ; compliments répétés et exagérés.

Le harcèlement sexuel est puni de deux ans d'emprisonnement et de 30 000 € d'amende. Ces peines sont **portées à trois ans et 45 000 € d'amende en cas de circonstances aggravantes**, notamment lorsqu'ils sont commis par une personne qui abuse de l'autorité que lui confère sa fonction ou lorsqu'ils sont commis sur une victime particulièrement vulnérable (femme enceinte, personne dont la précarité économique est connue de l'auteur des faits...).

4.3. Les agissements sexistes

Rappel du cadre législatif :

« Nul ne doit subir d'agissement sexiste, défini comme tout agissement lié au sexe d'une personne, ayant pour objet ou pour effet de porter atteinte à sa dignité ou de créer un environnement intimidant, hostile, dégradant, humiliant ou offensant. » Article L. 1142-2-1 du Code du travail

Les comportements suivants peuvent constituer des agissements sexistes :

- Critiquer l'apparence ou la tenue vestimentaire d'un collaborateur parce qu'elle ne correspond pas à ce qu'on attend d'un homme ou d'une femme ;
- Montrer de l'hostilité ou du mépris envers une personne en raison de son sexe ou envers toutes les personnes de ce sexe ;
- Ne pas prendre les compétences d'un collaborateur au sérieux en raison de son sexe ;
- Imposer à un collaborateur le fait d'écouter des plaisanteries sexistes ;
- Insinuer qu'un collaborateur doit son recrutement/ sa réussite professionnelle/ sa rémunération/ le bon aboutissement d'un dossier à son sexe ;
- Entretenir un climat sexiste qui empêche un collaborateur de façon sereine.

Les agissements sexistes ne constituent pas directement une infraction pénale mais ils peuvent entrer en ligne de compte dans le cadre de poursuites pour discrimination fondée sur le sexe. Ce type de discrimination est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.

4.4. La discrimination

Rappel du cadre législatif :

« Aucune personne ne peut être écartée d'une procédure de recrutement ou de nomination ou de l'accès à un stage ou à une période de formation en entreprise, aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, telle que définie à l'article 1er de la loi n°2008-496 du 27 mai 2008 portant diverses dispositions d'adaptation au droit communautaire dans le

domaine de la lutte contre les discriminations, notamment en matière de rémunération, au sens de l'article L. 3221-3, de mesures d'intéressement ou de distribution d'actions, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, d'horaires de travail, d'évaluation de la performance, de mutation ou de renouvellement de contrat en raison de son origine, de son sexe, de ses mœurs, de son orientation sexuelle, de son identité de genre, de son âge, de sa situation de famille ou de sa grossesse, de ses caractéristiques génétiques, de la particulière vulnérabilité résultant de sa situation économique, apparente ou connue de son auteur, de son appartenance ou de sa non-appartenance, vraie ou supposée, à une ethnie, une nation ou une prétendue race, de ses opinions politiques, de ses activités syndicales ou mutualistes, de son exercice d'un mandat électif, de ses convictions religieuses, de son apparence physique, de son nom de famille, de son lieu de résidence ou de sa domiciliation bancaire, ou en raison de son état de santé, de sa perte d'autonomie ou de son handicap, de sa capacité à s'exprimer dans une langue autre que le français, de sa qualité de lanceur d'alerte, de facilitateur ou de personne en lien avec un lanceur d'alerte, au sens, respectivement, du I de l'article 6 et des 1° et 2° de l'article 6-1 de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique. » Article L. 1132-1 du Code du travail

« Constitue une discrimination toute distinction opérée entre les personnes physiques sur le fondement de leur origine, de leur sexe, de leur situation de famille, de leur grossesse, de leur apparence physique, de la particulière vulnérabilité résultant de leur situation économique, apparente ou connue de son auteur, de leur patronyme, de leur lieu de résidence, de leur état de santé, de leur perte d'autonomie, de leur handicap, de leurs caractéristiques génétiques, de leurs mœurs, de leur orientation sexuelle, de leur identité de genre, de leur âge, de leurs opinions politiques, de leurs activités syndicales, de leur qualité de lanceur d'alerte, de facilitateur ou de personne en lien avec un lanceur d'alerte au sens, respectivement, du I de l'article 6 et des 1° et2° de l'article 6-1 de la loi n°2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, de leur capacité à s'exprimer dans une langue autre que le français, de leur appartenance ou de leur non-appartenance, vraie ou supposée, à une ethnie, une Nation, une prétendue race ou une religion déterminée.

Constitue également une discrimination toute distinction opérée entre les personnes morales sur le fondement de l'origine, du sexe, de la situation de famille, de la grossesse, de l'apparence physique, de la particulière vulnérabilité résultant de la situation économique, apparente ou connue de son auteur, du patronyme, du lieu de résidence, de l'état de santé, de la perte d'autonomie, du handicap, des caractéristiques génétiques, des mœurs, de l'orientation sexuelle, de l'identité de genre, de l'âge, des opinions politiques, des activités syndicales, de la qualité de lanceur d'alerte, de facilitateur ou de personne en lien avec un lanceur d'alerte, au sens, respectivement, du I de l'article 6 et des 1° et 2° de l'article 6-1 de la loi n° 2016-1691 du 9 décembre 2016 précitée, de la capacité à s'exprimer dans une langue autre que le français, de l'appartenance ou de la non-appartenance, vraie ou supposée, à une ethnie, une Nation, une prétendue race ou une religion déterminée des membres ou de certains membres de ces personnes morales. » Article 225-1 du Code pénal

« La discrimination définie à l'article 225-1, commise à l'égard d'une personne physique ou morale, est punie de deux ans d'emprisonnement et de 200 000 F d'amende lorsqu'elle consiste :

1° A refuser la fourniture d'un bien ou d'un service ;

2° A entraver l'exercice normal d'une activité économique quelconque ;

3° A refuser d'embaucher, à sanctionner ou à licencier une personne ;

4° A subordonner la fourniture d'un bien ou d'un service à une condition fondée sur l'un des éléments visés à l'article 225-1 ;

5° A subordonner une offre d'emploi à une condition fondée sur l'un des éléments visés à l'article 225-1. »
Article 225-2 du Code pénal

Le principe de non-discrimination est basé sur le principe d'égalité**.**

Constitue une discrimination directe la situation dans laquelle, sur le fondement d'un critère mentionné par la loi (l'origine, l'état de santé, le handicap, l'âge, le nom de famille etc.), une personne est traitée de manière moins favorable qu'une autre ne l'est dans une situation comparable.

La discrimination peut être indirecte lorsque des mesures apparemment neutres défavorisent, de fait, de façon importante, une catégorie de personnes.

Tout salarié victime de discrimination au travail peut signaler les faits aux représentants du personnel.

Toute discrimination est passible de 3 ans de prison et de 45 000 € d'amende.

Annexe 3 : Modèle de délégation de signature

LOGO DU CDOI/CIDOI

Modèle de délégation de signature

Je soussigné, Prénom Nom, agissant en qualité de président du conseil départemental/régional de l'Ordre des infirmiers de ……., donne par la présente pouvoir à M/Mme Prénom Nom, en sa qualité de ……..

…… ……., afin qu'il ou qu'elle puisse signer pour moi et en mon nom, dans la stricte limite de l'exercice de ses fonctions les documents suivants (**liste non exhaustive**) :

- Autorisation de remplacement
- Attestation d'inscription
- Attestation de radiation
- Attestation de changement de département
- Courriers liés à l'instruction des demandes d'inscription
- Courriers liés à l'instruction des plaintes dans le cadre de l'organisation des conciliations
- Courriers liés l'instruction des demandes de médiation

Ce pouvoir de signature est confié par M/Mme Prénom Nom (déléguant jusqu'à la fin de son mandat. Le délégant restant toutefois libre, à tout moment et sans préavis, de supprimer la présente délégation de signature ou d'en modifier le périmètre et/ou les modalités, sans autre formalité qu'une notification écrite informant le délégataire.

Les documents signés en application de la présente délégation de signature comportent la mention « Pour le Président, par délégation ».

Il est précisé que M/Mme Prénom Nom n'est pas autorisé à subdéléguer la présente délégation de signature.

Fait à..... , le xx/xx/xxxx, en 2 exemplaires originaux

Signature du délégant	**Signature du délégataire**
Prénom Nom	**Prénom Nom**
Qualité	**Qualité**

Annexe 4 : Charte informatique à destination des salariés

Charte informatique de l'Ordre national des infirmiers

Adoptée par le Conseil national du 22 janvier 2021

Table des matières

1 Préambule

L'entreprise met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment

- un réseau informatique
- Un réseau téléphonique
- Une flotte mobile.
- Des applications SAS
- Un bureau virtuel

Les salariés et les élus de l'Ordre, dans l'exercice de leurs fonctions respectives, sont conduits à utiliser les outils informatiques et téléphoniques mis à leur disposition et à accéder aux services de communication de l'entreprise.

L'utilisation du système d'information et de communication doit se faire exclusivement à des fins professionnelles pour les salariés et dans le respect de leur mandat électif pour les élus, sauf exception prévue dans la présente 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, la présente charte pose les règles relatives à l'utilisation de ces ressources. Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation mise en place, non seulement pour la bonne exécution du contrat de travail pour les salariés, dans le cadre des mandats électifs pour les élus (en respect de leurs attributions visées par le code de la santé publique), mais aussi dans le cadre de la responsabilité pénale et civile du CNOI. Elle dispose d'un aspect réglementaire et est annexée au règlement intérieur de l'entreprise. Elle ne remplace en aucun cas les lois en vigueur que chacun est censé connaître.

2 Champ d'application

2.1 Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de l'entreprise, quel que soit leur statut, y compris les

- mandataires sociaux,
- salarié(e)s,
- intérimaires,
- stagiaires,
- employé(e)s de sociétés prestataires,
- visiteurs occasionnels,
- Elu(e)s

Elle sera annexée aux contrats de prestations.

Les salariés et les élus veillent à faire accepter valablement les règles posées dans la présente 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

Le système d'information et de communication de l'entreprise 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,
- smartphones,
- tablettes
- clés 3G,
- logiciels,
- fichiers,
- données et bases de données,
- système de messagerie,
- connexion internet,
- intranet,
- extranet,
- abonnements à des services interactifs.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des salariés et des élus connecté au réseau de l'entreprise, ou contenant des informations à caractère professionnel concernant l'entreprise.

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

La présente charte ne préjuge pas des accords particuliers pouvant porter sur l'utilisation du système d'information et de communication par les institutions représentatives, l'organisation d'élections par voie électronique ou la mise en télétravail de salariés.

3 Confidentialité

3.1 Paramètres d'accès

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

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs. Ils ne doivent être communiqués à personne. Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par la direction ou la direction informatique afin de recommander les bonnes pratiques en la matière.

Aucun utilisateur ne doit se servir pour accéder au système d'information de l'entreprise 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.

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 la direction 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 d'outils informatiques, personnels ou appartenant à l'entreprise, dans des lieux autres que ceux de l'entreprise (hôtels, lieux publics…).

4 Sécurité

4.1 Rôle de l'entreprise

L'entreprise 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. La direction informatique est responsable de la mise en œuvre et du contrôle du bon fonctionnement du système d'information et de communication. Elle doit prévoir un plan de sécurité et de continuité du service, en particulier en cas de défaut matériel. Elle veille à l'application des règles de la présente charte. Elle est assujettie à une obligation de confidentialité sur les informations qu'elle est amenée à connaître.

4.2 Responsabilité 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 des dites 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. Sauf autorisation expresse de la direction, l'accès au système d'information avec du matériel n'appartenant pas à l'entreprise (assistants personnels, supports amovibles…) est interdit.

Dans le cas où il a été autorisé, il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité. De même, la sortie de matériel appartenant à l'entreprise 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 la direction 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 de la direction 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 de l'entreprise. 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 dans l'entreprise. Il doit dans tous les cas en alerter la direction informatique.

L'utilisateur s'oblige en toutes circonstances à 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 de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication.

5 Internet

5.1 Accès aux sites

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par la direction informatique qui est habilitée à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites.

Seule la consultation de sites ayant un rapport avec l'activité professionnelle ou ordinale est autorisée. En particulier, l'utilisation de l'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 créer ou mettre à jour au moyen de l'infrastructure de l'entreprise tout site Internet, notamment des pages personnelles.

Bien sûr, il est interdit de se connecter à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'entreprise, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information de l'entreprise ou engageant financièrement celle-ci.

5.2 Autres utilisations

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, chats, blogs n'est autorisée qu'à titre professionnel et sur autorisation expresse de la hiérarchie pour les salariés ou dans le cadre de leur mandat électif et en respect du code de la santé publique pour les élus. La direction informatique devra en être informée sans délai.

De même, tout téléchargement de fichier, en particulier de fichier média, est prohibé, sauf justification professionnelle dûment validée par la hiérarchie ou dans le cadre de leur mandat électif et en respect du code de la santé publique pour les élus.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte aux intérêts de l'entreprise.

Ils sont informés que la direction 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 de l'entreprise.

5.3 Communication externe

En ce qui concerne l'utilisation des réseaux sociaux ou de création de site internet par les élus comme les salariés, il est impératif de ne pas porter préjudice à l'Ordre et à ses missions par des publications sortant des missions de la personne et de l'instance concernées ou par des propos allant à l'encontre de l'institution ordinale ou de ses représentant.

Il ne doit pas non plus être fait usage de ces outils pour une propagande syndicale, personnelle ou visant à dénigrer une personne ou une institution.

La stratégie de communication de toute instance doit être en accord avec la stratégie de communication fixé par le CNOI.

Seul les logos officiels de l'Ordre sont autorisés dans ces communications.

6 Messagerie électronique

Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique normalisée attribuée par la direction informatique.

Chaque élu dispose, pour l'exercice de son activité ordinale, d'une adresse de messagerie électronique normalisée attribuée par la direction informatique.

Les messages électroniques reçus sur la messagerie professionnelle ou ordinale font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés sont invités à informer la direction informatique des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

L'utilisation de cette messagerie ne peut être faite que dans le cadre de son activité professionnelle pour les salariés ou en respect des missions dévolues par son mandat ordinal pour les élus.

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, 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 son supérieur.

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

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'informations à caractère confidentiel, ces vérifications doivent être renforcées ; en cas de besoin, un cryptage des messages pourra être aussi proposé par la direction informatique.

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 d'en vérifier les modalités d'abonnement, de contrôler la liste des abonnés et de prévoir l'accessibilité aux archives. 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 être envoyés avec un accusé de réception ou signés électroniquement.

Pour les salariés, tout mail à un ensemble du personnel (RAR, directeurs ou ensemble du personnel) doit d'abord avoir été validé soit en CODIR ou en cas d'urgence par son directeur de référence.

Pour les salariés, tout mail adressé à l'ensemble des Président de départements, de régions où aux élus en général part de la boite mail du président, une fois cet envoi validé par ce dernier ou par son représentant.

Pour les salariés, tout envoi de mail à des instances publiques comme, notamment, des ministères, des députés, des sénateurs, des autorités administratives doivent obligatoirement être validé par le Président de l'Ordre National des infirmiers ou son représentant quand ce mail concerne une prise de décision ou une remontée d'information officielle. En cas de doute, le salarié consulte le directeur ou son représentant.

Tout envoi de mail par un élu doit se faire dans le cadre de son mandat électif tout en respectant les règles du RGPD.

Les mails 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.

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

En cas d'absence supérieure à 3 jours, le salarié doit mettre en place un répondeur automatique.

Seuls les logos officiels de l'Ordre peuvent être utilisés dans le cadre des communications internes comme externes.

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 la direction informatique. Cette limite est susceptible d'être levée temporairement ou définitivement sur demande adressée à la direction informatique, qui est aussi chargée de l'ouverture des listes de diffusion qui pourraient s'avérer nécessaires.

De même, la direction informatique peut limiter la taille, le nombre et le type des pièces jointes pour éviter l'engorgement du système de messagerie. Pour des raisons de capacité mémoire, les messages électroniques sont conservés sur le serveur de messagerie pendant une durée maximale d'un an. Passé ce délai, ils sont automatiquement supprimés. Si le salarié souhaite conserver des messages au-delà de ce délai, il lui appartient d'en faire des sauvegardes avec l'aide de la direction informatique si nécessaire. Il est aussi tenu de supprimer lui-même dès que possible tous les messages inutiles.

6.3 Utilisation personnelle de la messagerie

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte. Les messages envoyés doivent être signalés par la mention "Privé" ou "Perso" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon. Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Perso".

En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'entreprise.

Ces mails doivent respecter la législation en vigueur notamment ne pas inciter à des actes prohibés.

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 être signalés et classés de la même manière que les messages à caractère personnel, mais en utilisant la mention "Délégué" dans leur objet à l'émission et dans le dossier où ils doivent être classés.

7 Téléphonie

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un poste fixe et 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 mêmes règles rappelées plus haut.

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

7.1 Utilisation personnelle de la téléphonie

L'utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, à condition qu'elle reste dans des limites raisonnables en termes tant de temps passé que de quantité d'appels. Les surcoûts pour l'entreprise engendrés par l'utilisation de la téléphonie à des fins personnelles devront être 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 la direction informatique enregistre leur activité téléphonique, aussi bien sur les postes fixes que sur les mobiles. Ces traces 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 Données personnelles

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, définit les conditions dans lesquelles des traitements de données personnels peuvent être opérés. Elle institue au profit des personnes concernées par les traitements des droits que la présente invite à respecter, tant à l'égard des utilisateurs que des tiers.

Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle, prévus dans la présente 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 et ces données ne seront conservées que sur une période maximale de 1 an. 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 ou ordinal, des traitements relevant de ladite loi sont invités à prendre contact avec la direction informatique avant d'y procéder.

Depuis 2018, l'ensemble de nos données ainsi que des traitements de celle-ci, sont régis par le RGPD. La DSI mets à disposition un ensemble d'outils permettant à l'ensemble des salariés, élus et utilisateurs de ses données de travailler dans les meilleures conditions. Chaque extraction de données doit être validé par le DPO, a défaut le responsable de la sécurité informatique désigné, ainsi que le directeur des systèmes d'informations. Un documents à remplir par le responsable du traitement sera examiné et validé pour que l'extraction soit effectuée.

9 Contrôle des activités

9.1 Contrôlesautomatisés

Le système d'information et de communication s'appuie sur des fichiers journaux ("logs"), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, 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.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;

- aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour 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 ou le téléchargement de fichiers ;

- aux appels téléphoniques émis ou reçus à partir des postes fixes ou mobiles pour surveiller le volume d'activités et détecter des dysfonctionnements.

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.

9.2 Procédure de contrôle manuel

En cas de dysfonctionnement constaté par la direction 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 de l'entreprise, ou sur sa messagerie. Alors, 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 présente charte, qu'en présence de l'utilisateur ou celui-ci dûment appelé et

éventuellement représenté par un délégué du personnel pour un salarié ou d'un autre élu pour un élu ordinal.

10 Information et sanctions

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié et à chaque élu par voie électronique.

La direction informatique est à la disposition des salariés et des élus pour leur fournir toute information concernant l'utilisation du système d'information, 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 ainsi que sur les menaces susceptibles de peser sur sa sécurité. Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par la direction informatique dans le cadre de la présente charte.

En cas de besoin, les salariés ou les élus pourront être formés par la direction informatique pour appliquer les règles d'utilisation du système d'information et de communication prévues.

Le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre, pour les salariés, des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés. Dans ce dernier cas, les procédures prévues dans le règlement intérieur et dans le Code du travail seront appliquées. Pour les élus, peut être prononcé une suspension d'utiliser tout ou partie du système d'information et de communication ou, après passage en CNOI, un renvoi en chambre disciplinaire si le nom respect de cette charte a engendré un manquement déontolog ique.

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

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

11 Entrée en vigueur

La présente charte est applicable à compter du 1er février 2021

Ordre National des Infirmiers

Charte d'utilisation des systèmes d'information

Charte informatique ONI (mise à jour 2022) à destination des ELUS

Table des matières

1 Préambule

L'ORDRE NATIONAL DES INFIRMIERS (ci-dessous dénommé « ONI ») met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment :

- Un réseau informatique ;
- Un réseau téléphonique ;
- Des outils mobiles (bureau virtuel, smartphones, etc.) ;
- Des applications ;
- Du matériel (ordinateur, smartphone, etc.) en fonction du profil de l'Utilisateur.

Les Utilisateurs (élus infirmiers), dans l'exercice de leurs fonctions, sont conduits à utiliser les outils informatiques et téléphoniques mis à leur disposition et à accéder aux services de communication de l'ONI.

L'utilisation du système d'information et de communication doit se faire exclusivement à des fins ordinales, sauf exception prévue dans la présente 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, la présente charte pose les règles relatives à l'utilisation de ces ressources. Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation mise en place, mais aussi le cadre de la responsabilité pénale et civile. Elle dispose d'un aspect réglementaire et est annexée au règlement intérieur de l'ONI. Elle ne remplace en aucun cas les lois en vigueur que chacun est censé connaître.

2 Champ d'application

2.1 Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique aux :

- Mandataires sociaux ;
- Elu(e)s de l'Ordre.

Elle sera annexée aux contrats de prestations.

Les Utilisateurs veillent à faire accepter valablement les règles posées dans la présente 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

Le système d'information et de communication de l'ONI est notamment constitué des éléments suivants (liste non exhaustive) :

- Ordinateurs (fixes ou portables) ;
- Périphériques y compris clés USB ;
- Assistants personnels ;
- Réseau informatique (serveurs, routeurs et connectique) ;
- Photocopieurs ;
- Télécopieurs ;
- Téléphones ;
- Smartphones ;
- Tablettes ;
- Clés 3G / 4G / 5G ;
- Logiciels ;

- Fichiers ;
- Données et bases de données ;
- Système de messagerie ;
- Connexion internet ;
- Intranet ;
- Extranet ;
- Abonnements à des services interactifs.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des Utilisateurs connectés au réseau de l'ONI, ou contenant des informations à caractère professionnel concernant l'ONI.

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

La présente charte ne préjuge pas des accords particuliers pouvant porter sur l'utilisation du système d'information et de communication par les institutions représentatives, l'organisation d'élections par voie électronique ou la mise en télétravail de salariés.

3 Confidentialité

3.1 Paramètres d'accès

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

S'agissant des mots de passe, et afin de garantir la sécurité et la confidentialité des données personnelles auxquelles l'utilisateur a accès, il lui est rappelé qu'il est dangereux de réutiliser un même mot de passe pour plusieurs comptes et que pour des raisons de sécurité chaque compte doit disposer d'un mot de passe unique.

Ces paramètres sont personnels à l'Utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des Utilisateurs. Ils ne doivent être communiqués à personne, ni responsable hiérarchique, ni informatique. Dans la mesure du possible, ces paramètres doivent être mémorisés par l'Utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'Utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

Lorsqu'ils sont choisis par l'Utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par la direction ou la direction informatique afin de recommander les bonnes pratiques en la matière.

Aucun Utilisateur ne doit se servir pour accéder au système d'information de l'ONI 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.

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 la direction 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 d'outils informatiques, personnels ou appartenant à l'ONI, dans des lieux autres que ceux de l'ONI (hôtels, trains, lieux publics, espace de coworking, etc.).

L'élu ordinal s'engage, conformément à l'article 1.14 du RI à garantir la confidentialité des informations auxquelles il a accès au cours de son mandant et à prendre toutes les précautions pour préserver la sécurité des données personnelles.

Aussi, l'utilisateur :

- N'utilisera les données personnelles auxquelles il a accès que dans le strict cadre prévu par ses missions et des traitements de données personnelles préalablement définis conformément au RGPD et à la loi informatique et libertés
- N'accédera pas, ne tentera pas d'accéder ou de supprimer des informations si cela ne relève pas des missions qui lui sont attribuées
- Ne fera pas de copie de données personnelles auxquelles il a accès pour un usage personnel
- Ne communiquera pas les données auxquelles il a accès à des personnes non autorisées
- Verrouillera ou éteindra son ordinateur dès qu'il quitte son poste de travail
- restituera le matériel prêté par l'Ordre lors de la cessation de ses fonctions ordinales

4 Sécurité

4.1 Rôle de l'ONI

L'ONI 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. La direction informatique est responsable de la mise en œuvre et du contrôle du bon fonctionnement du système d'information et de communication. Elle doit prévoir un plan de sécurité et de continuité du service, en particulier en cas de défaut matériel. Elle veille à l'application des règles de la présente charte. Elle est assujettie à une obligation de confidentialité sur les informations qu'elle est amenée à connaître.

4.2 Responsabilité 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 des dites ressources, en faisant preuve de prudence et de vigilance.

Notification des incidents et des violations à la direction informatique :

Toute violation de données personnelles susceptible d'engendrer un risque pour les droits et libertés des personnes devant être notifiée auprès de la commission nationale de l'informatique et des libertés (CNIL) dans les meilleurs délais et au plus tard 72 heures après en avoir pris connaissance, l'utilisateur doit signaler dans les meilleurs délais à la direction informatique toute violation ou tentative de violation de l'intégrité de ces ressources et des données personnelles auxquelles il a accès, et, de manière générale tout dysfonctionnement, incident ou anomalie.

Sauf pour les Utilisateurs ne disposant pas du matériel fourni par l'ONI ou sur autorisation expresse de la direction, l'accès au système d'information avec du matériel n'appartenant pas à l'ONI (assistants personnels, supports amovibles…) est interdit.

Dans le cas où il a été autorisé, il appartient à l'Utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité. De même, la sortie de matériel appartenant à l'ONI 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 utiliser dans la mesure du possible les outils de partage de fichiers fournis par l'ONI (exemples suite bureautique Office 365 avec la solution OneDrive, GED) : ces outils permettent une sauvegarde automatique des fichiers. 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 de la direction informatique.

Les Utilisateurs ayant le mandat permettant de bénéficier d'un matériel fourni par l'ONI doivent obligatoirement et exclusivement utiliser ce matériel (ordinateur comme smartphone) pour se connecter au système d'information. L'Utilisateur ne doit pas installer ou supprimer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein de l'ONI. 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 dans l'ONI. Il doit dans tous les cas en alerter la direction informatique.

Pour les Utilisateurs ne disposant pas du matériel fourni par l'ONI, il est recommandé d'utiliser du matériel régulièrement mis à jour (antivirus, système d'exploitation, etc.).

La politique de sécurité évoluant en fonction notamment du contexte interne comme externe à l'ONI, l'Utilisateur doit se conformer aux directives liées à l'authentification sur les outils mis à disposition de l'ONI (exemple authentification enforcée MFA).

L'Utilisateur s'oblige en toutes circonstances à 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 de l'ONI ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication. Pour cela, l'utilisation d'une messagerie non ordinale (ie non fournie par l'ONI) est proscrite (inclus les transferts d'un courriel de la messagerie ordinale vers une messagerie non ordinale).

5 Internet

5.1 Accès aux sites

Dans le cadre de leur activité, les Utilisateurs peuvent avoir accès à Internet depuis le réseau de l'ONI. Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par

la direction informatique qui est habilitée à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites.

Seule la consultation de sites ayant un rapport avec l'activité professionnelle est autorisée. En particulier, l'utilisation de l'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 créer ou mettre à jour au moyen de l'infrastructure de l'ONI tout site Internet, notamment des pages personnelles.

Bien sûr, il est interdit de se connecter à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'ONI, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information de l'ONI ou engageant financièrement celle-ci.

5.2 Autres utilisations

La contribution des Utilisateurs à des forums de discussion, systèmes de discussion instantanée, chats, blogs n'est autorisée qu'à titre professionnel et sur autorisation expresse de la hiérarchie qui devra en informer la direction informatique.

De même, tout téléchargement de fichier, en particulier de fichier média, est prohibé, sauf justification professionnelle dûment validée par la hiérarchie.

Il est rappelé que les Utilisateurs ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte aux intérêts de l'ONI.

Ils sont informés que la direction 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 de l'ONI.

5.3 Communication externe

En ce qui concerne l'utilisation des réseaux sociaux ou de création de site internet par les Utilisateurs, il est impératif de ne pas porter préjudice à l'Ordre et à ses missions par des publications sortant des missions de la personne et de l'instance concernées ou par des propos allant à l'encontre de l'institution ordinale ou de ses représentant.

Il ne doit pas non plus être fait usage de ces outils pour une propagande syndicale, personnelle ou visant à dénigrer une personne ou une institution.

Il est rappelé que conformément aux articles L.4312-1 et L.4312-2 du code de la santé publique les missions de l'Ordre sont notamment les suivantes :

- L'ordre national des infirmiers veille à maintenir les principes éthiques et à développer la compétence, indispensables à l'exercice de la profession. Il contribue à promouvoir la santé publique et la qualité des soins.
- L'ordre national des infirmiers assure la défense de l'honneur et de l'indépendance de la profession d'infirmier. Il en assure la promotion.

La stratégie de communication de toute instance doit être en accord avec la stratégie de communication fixé par le CNOI.

Seuls les logos officiels de l'Ordre sont autorisés dans ces communications.

L'adresse courriel associée à un compte créé sur un réseau social doit être une adresse courriel ordinale.

6 Messagerie électronique

Chaque Utilisateur dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique normalisée attribuée par la direction informatique.

Les messages électroniques reçus sur la messagerie ordinale font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les Utilisateurs sont invités à informer la direction 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, en particulier en matière d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer aux instances de l'ONI.

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

Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'informations à caractère confidentiel, ces vérifications doivent être renforcées ; en cas de besoin, un chiffrement des messages pourra être aussi proposé par la direction informatique.

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 d'en vérifier les modalités d'abonnement, de contrôler la liste des abonnés et de prévoir l'accessibilité aux archives. 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 être envoyés avec un accusé de réception ou signés électroniquement.

Tout courriel à un ensemble du personnel e(/ou élus (RAR, directeurs ou ensemble du personnel) doit d'abord avoir été validé soit en CODIR ou en cas d'urgence par son directeur de référence.

Les échanges entre les Utilisateurs et les salariés ou les infirmiers doivent obligatoirement être effectués depuis une messagerie ordinale.

Tout envoi de courriel à des instances publiques comme, notamment, des ministères, des députés, des sénateurs, des autorités administratives doivent obligatoirement être validé par le Président de l'Ordre National des infirmiers ou son représentant quand ce mail concerne une prise de décision ou une remontée d'information officielle. En cas de doute, l'Utilisateur consulte le directeur ou son représentant.

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.

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

En cas d'absence supérieure à 24 heures, l'Utilisateur doit mettre en place un répondeur automatique.

Seul le logo officiel de l'Ordre peut être utilisé dans le cadre des communications internes comme externes.

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 la direction informatique. Cette limite est susceptible d'être levée temporairement ou définitivement sur demande adressée à la direction informatique, qui est aussi chargée de l'ouverture des listes de diffusion qui pourraient s'avérer nécessaires.

De même, la direction informatique peut limiter la taille, le nombre et le type des pièces jointes pour éviter l'engorgement du système de messagerie. L'Utilisateur est tenu de supprimer lui-même dès que possible tous les messages inutiles.

L'Utilisateur doit utiliser exclusivement l'outil de campagne communication mis à disposition par la direction informatique. L'usage de cet outil doit rester limité à un usage défini dans le cadre des missions de l'ONI.

6.3 Utilisation personnelle de la messagerie

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte. Les messages envoyés doivent être signalés par la mention « Personnel et confidentiel » dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon. Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé « Personnel et confidentiel ».

En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Toutefois, les Utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'ONI.

6.4 Utilisation des messageries partagés

Seuls les Utilisateurs habilités à accéder à une messagerie partagée peuvent utiliser cette messagerie.

Sauf accord du manager de région (RAR), un Utilisateur ne doit pas accéder au contenu d'une messagerie ordinale d'un salarié.

7 Téléphonie

En fonction du mandat et de l'évolution de la politique nationale de mise à disposition du matériel, les Utilisateurs peuvent disposer d'un poste fixe dans les locaux de l'ONI et/ou d'un terminal mobile,

smartphone, tablette ou clé 3G / 4G / 5G. 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 mêmes règles rappelées plus haut.

Enfin, les connexions depuis l'étranger (hors régions outre-mer) sont strictement interdites sauf autorisation exceptionnelle de la hiérarchie en cas d'urgence professionnelle.

7.1 Utilisation personnelle de la téléphonie

L'utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, à condition qu'elle reste dans des limites raisonnables en termes tant de temps passé que de quantité d'appels. Les surcoûts pour l'ONI engendrés par l'utilisation de la téléphonie à des fins personnelles devront être 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 la direction informatique enregistre leur activité téléphonique, aussi bien sur les postes fixes que sur les mobiles. Ces traces 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 Déplacements dans le cadre des missions ordinales

L'usage des équipements nomades facilite les déplacements professionnels mais fait peser des menaces sur des informations sensibles dont le vol ou la perte auraient des conséquences importantes sur les activités de l'ONI.

Avant de partir en déplacement :

- N'utiliser que du matériel (ordinateur, supports amovibles, téléphone) dédié à la mission et ne contenant que les données nécessaires ;
- Emporter un filtre de protection pour son ordinateur si l'Utilisateur compte profiter des trajets pour travailler ;
- Vérifier que ses mots de passe ne sont pas à la portée d'un tiers (exemple carnet ou pense-bête sur l'écran).
-

Pendant le déplacement :

- Garder ses appareils, supports et fichiers avec soi, pendant son voyage comme pendant le séjour (ne pas les laisser dans un bureau ou un coffre d'hôtel) ;
- Vérifier que le matériel est soit éteint soit avec une session verrouillée ;
- Informer l'ONI en cas d'inspection ou de saisie de son matériel par des autorités étrangères ;
- Ne pas utiliser les équipements offerts à l'Utilisateur s'il ne peut pas les faire vérifier par un service de sécurité de confiance ;
- Eviter d'utiliser de passer un un Wi-Fi public
- De ne pas exposer son écran à des regards indiscrets
- D'avertir dans les plus brefs délais l'ONI en cas de vol du matériel ordinal
- L'ordinateur devra être verrouillé ou éteint dès que l'utilisateur quitte son poste de travail

- Refuser la connexion d'équipements appartenant à des tiers à ses propres équipements (exemple : Smartphone, clé USB).

Après la mission :

- Ne jamais utiliser les clés USB qui peuvent avoir été offertes lors de ses déplacements (salons, réunions, voyages…) : elles sont susceptibles de contenir des programmes malveillants.

Ces mesures s'appliquent également au sein des sites de l'ONI.

9 Protection des données à caractère personnel

Le Règlement n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et communément appelé Règlement Général sur la Protection des Données (RGPD) est entré en vigueur le 25 mai 2018. Le RGPD, complété par la nouvelle Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa version consolidée du 14 juin 2018, précise les conditions dans lesquelles des traitements de données à caractère personnel peuvent être réalisés, les obligations incombant aux organismes publics et privés qui traitent ces données personnelles es droits et les personnes de décider et de contrôler les usages qui sont faits des données à caractère personnel.

Cette réglementation ouvre aux personnes concernées par les traitements un droit d'information, d'accès, de rectification, d'effacement, de portabilité et d'opposition sur leurs données personnelles lorsqu'elles sont collectées et traités par des organismes publics ou privés.

l'ONI a désigné un Délégué à la Protection des Données à caractère personnel (DPO). Ce dernier a pour mission de veiller au respect des dispositions du RGPD Il a pour rôle de s'assurer de la conformité juridique des traitements.

Le DPO est le point de contact pour l'exercice des droits et peut également être consulté pour toute question ou renseignement sur les traitements de données personnelles.

Il est obligatoirement consulté par le responsable de traitement préalablement à la création d'un fichier. Le « Responsable de Traitement » est celui qui détermine les finalités et les moyens du traitement, c'est celui qui a pris l'initiative du traitement. A ce titre, l'ONI est Responsable de Traitement.

Il recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de l'ONI au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande. Elle est également diffusée sur l'intranet de l'ONI.

En cas de difficultés rencontrées lors de l'exercice de des droits auprès du responsable de traitement, les personnes concernées peuvent introduire une réclamation auprès de la Commission nationale de l'Informatique et des Libertés https://www.cnil.fr/

10 Contrôle des activités

10.1 Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux ("logs"), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces

fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'ONI, 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.

Les Utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- A l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;
- Aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour 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 ou le téléchargement de fichiers ;
- Aux appels téléphoniques émis ou reçus à partir des postes fixes ou mobiles pour surveiller le volume d'activités et détecter des dysfonctionnements.

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.

10.2 Procédure de contrôle manuel

En cas de dysfonctionnement constaté par la direction 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 de l'ONI, ou sur sa messagerie. Alors, 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 présente charte, qu'en présence de l'Utilisateur ou celui-ci dûment appelé et éventuellement représenté par un délégué du personnel.

11 Information et sanctions

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque Utilisateur par voie électronique.

La direction est à la disposition des Utilisateurs pour leur fournir toute information concernant l'utilisation du système d'information, 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 ainsi que sur les menaces susceptibles de peser sur sa sécurité. Chaque Utilisateur doit se conformer aux procédures et règles de sécurité édictées par la direction informatique dans le cadre de la présente charte.

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

Le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'Utilisateur (articles 226-13 et 226-16 à 226-24 du code pénal notamment) et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées à la gravité des faits concernés. 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 de l'ONI donnera également lieu à remboursement de la part de l'Utilisateur concerné.

Le Représentant de l'ONI 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.

12 Entrée en vigueur de la charte

La présente charte a été adoptée après information et consultation du Comité Social Économique, transmise à l'inspection du travail et déposée au greffe.

Elle est applicable après validation de ces enregistrements.

Annexe 6 : Modèle de délégation de pouvoir

LOGO DU CDOI/CIDOI

POUVOIR

REUNION PLENIERE DU CDOI/CIDOI----------

Je soussigné(e)----------**[Indiquez vos nom et prénom]**, demeurant à ----------, membre du CDOI/CIDOI, domicilié ----------,

Donne, par la présente, pouvoir à Mme/M ----------**[Indiquez les nom et prénom de votre représentant]**, membre du CDOI/CIDOI----------, aux fins de me représenter à ---------- du CDOI/CIDOI---------- qui se tiendra le ---------- à ---------- heure, à l'effet de prendre part aux délibérations et voter les résolutions visées à l'ordre du jour.

Fait à ----------

Le ----------

Signature

Annexe 7 : Modèle de convocation à une réunion du conseil

Mme/M. xxxxxxx
Adresse
Code postal Ville

« Lieu », le …… 2021

Objet : Convocation

Chère consœur / Cher confrère,

J'ai le plaisir de vous convier à la prochaine réunion du Conseil interdépartemental XXX, qui se déroulera :

Le ../.. 2021 de xxh à xxh

Adresse

L'ordre du jour sera le suivant :

1. xx
2. xx
3. xx
4. xx
5. xx

Comptant sur votre présence, je vous prie d'agréer, chère consœur / cher confrère, l'expression de mes cordiales salutations.

Le Président
signature

Article L4125-3 du Code de la Santé Publique : « Tout conseiller départemental, territorial, régional, interrégional ou national de l'ordre qui, sans motif valable, n'a pas siégé durant trois séances consécutives peut, sur proposition du conseil intéressé, être déclaré démissionnaire par le conseil national.
Les employeurs ou, pour les agents publics, l'autorité hiérarchique, sont tenus de laisser à leurs salariés ou agents, membres d'un conseil de l'ordre, le temps nécessaire pour se rendre et participer aux séances de ces conseils, de ses commissions ou de ses chambres disciplinaires. Le salarié doit informer, selon le cas, l'employeur ou l'autorité hiérarchique de la séance dès qu'il en a connaissance. Le temps passé hors du cadre du travail pendant les heures de travail à l'exercice des fonctions ordinales est assimilé à une durée de travail effectif pour la détermination de la durée des congés payés, du droit aux prestations d'assurances sociales et aux prestations familiales ainsi qu'au regard de tous les droits que le salarié ou agent public tient du fait de son ancienneté dans l'entreprise. Ces absences, justifiées par l'exercice de leurs fonctions, n'entraînent aucune diminution de leurs rémunérations et des avantages y afférents. »

Annexe 8 : Modèle de lettre de démission d'office

LOGO DU CDOI/CIDOI

Objet : perte de la qualité de conseiller ordinal

Lettre recommandée AR

Cher Confrère/Chère Consœur,

Vous avez été élu(e) le XX/XX/XXXX membre de notre Conseil ordinal, au sein du collège des XXXX.

(Selon la situation :)

Cas 1 (applicable en cas de transfert géographique)	J'observe que vous n'êtes plus inscrit(e) au tableau au double titre de la circonscription et du collège qui étaient les vôtres au moment de votre élection précitée. Dans ces conditions, conformément aux dispositions des articles R.4125-3 et R.4125-30 du CSP (voir ci-joint), je suis amené à vous notifier par la présente votre démission d'office. En vous remerciant vivement de la contribution que vous avez apportée jusqu'ici à nos travaux,
Cas 2	J'observe que vous n'êtes pas à jour du règlement de votre cotisation ordinale. Cette situation, si elle se poursuivait, entraînerait votre inéligibilité, et donc votre démission d'office immédiate de tout mandat ordinal, conformément aux dispositions de l'article R.4125-3 du CSP (voir ci-joint). Pour éviter une telle conséquence, je vous invite instamment à régulariser votre situation et à m'en informer dans un délai maximal de deux semaines. Dans l'attente de votre réponse,

Cas 3	J'observe que vous n'avez pas siégé durant trois sessions consécutives de notre Conseil, les ……, ……..et ……... Cette situation, à défaut de motifs valables, peut conduire le Conseil national de l'Ordre à déclarer votre démission, sur proposition de notre instance, conformément aux dispositions de l'article L.4125-3 du CSP (voir ci-joint). Je vous invite donc instamment à me faire connaître les motifs de vos absences. A défaut de réponse de votre part dans un délai maximal de deux semaines, ou en l'absence de motifs reconnus valables, je serai amené à demander à notre Conseil de proposer au Conseil national de déclarer votre démission. Pour éviter les délais et les inconvénients de toute nature liés à cette procédure, je vous précise que vous pouvez, bien entendu, si vous le souhaitez, me présenter votre démission à tout moment, par lettre recommandée avec demande d'avis de réception. Dans l'attente de votre réponse,
Cas 4	J'observe qu'une peine disciplinaire devenue définitive a été prononcée à votre encontre le XX/XX/XXXX par la chambre disciplinaire… (du Conseil régional de……./ du Conseil national). Une telle mesure entraine, conformément aux dispositions de l'article L. 4124-6 du code de la santé publique et L.145-5-3 du code de la sécurité sociale (voir ci-joints), la privation du droit de faire partie d'un conseil ordinal. Dans ces conditions, je suis amené à vous notifier votre démission d'office. Avec mes regrets,

Je vous prie de recevoir, Cher Confrère/Chère Consœur, l'assurance de mes sentiments confraternels et dévoués.

P. J. :
articles du code
de la santé publique