



CHARTRE DU BON USAGE DES RESSOURCES INFORMATIQUES, ELECTRONIQUES ET NUMERIQUES

Version du 07 Septembre 2016

1. DEFINITIONS

Enes : la régie municipale d'électricité de Hombourg-Haut

Equipements informatiques : ordinateur de bureau et portable, serveurs, logiciels, systèmes de bases de données relationnelles et tout système et logiciel permettant de traiter des informations de façon numérique

Moyens de communication : outils de messagerie interpersonnelle, accès internet, assistants personnels numériques, téléphone portable, ...

Informations et données : tout document numérique ou alphanumérique représentant des voix, données ou images dans le domaine numérique

Utilisateur : est considéré comme "Utilisateur" toute personne, quel que soit son statut (salarié, personnel intérimaire, stagiaire, apprenti, CDD, ...), qui est amenée à créer, consulter et mettre en œuvre des Ressources Informatiques depuis le site d'Enes ou à distance via les outils mis à sa disposition par Enes.

Administrateur système : personne responsable du bon fonctionnement des ressources informatiques ; ce rôle est notamment dévolu aux équipes du service informatique d'Enes.

Ressources informatiques : sont notamment constitutifs de Ressources Informatiques, les serveurs, stations de travail, postes de consultation, les réseaux internes et externes d'Enes, les micro-ordinateurs des services, ainsi que l'ensemble du parc logiciel, des bases de données, des produits multimédias ou des périphériques affectés au fonctionnement des éléments décrits.

Services Internet : la mise à disposition par des serveurs locaux ou distants de moyens d'échanges et d'information diverses : Web, messagerie, forum, réseaux sociaux,...

Compte : association d'un utilisateur, d'un identifiant (nom de « login »), et d'un droit d'accès à une ou plusieurs ressources informatiques. A un compte est associée une méthode d'authentification, par exemple un mot de passe, un certificat électronique, ...

Données personnelles ou nominatives : correspondent aux nom, prénoms, adresses (physique et électronique), numéro de téléphone, lieu et date de naissance, numéro de sécurité sociale, numéro de carte de paiement, plaque d'immatriculation d'un véhicule, photo, empreinte digitale, ADN, ... relatives à une personne. Certaines de ces données, dont en particulier le numéro de sécurité sociale ou le NIR, ainsi que les données biométriques (empreinte digitale, échantillon ADN, etc.), sont particulièrement sensibles, car elles fonctionnent en tant qu'« identifiants universels », qui permettent de rapprocher une personne à un fait ou un objet.

2. INTRODUCTION : POUR UNE UTILISATION RESPONSABLE

Enes met à la disposition de tout « utilisateur » des équipements informatiques, des moyens de communication ainsi que des informations et données.

Ces « Ressources Informatiques » sont nécessaires à l'accomplissement de sa mission.

Cependant, compte-tenu de la rapidité des évolutions technologiques et de la capacité des réseaux, le présent document peut ne pas être exhaustif. Il est donc indispensable que

chacun tienne compte, dans l'utilisation qu'il fait des Ressources Informatiques mises à disposition, des principes et de l'esprit décrits dans le présent document.

Celles-ci font partie du patrimoine d'Enes et leur utilisation doit être uniquement professionnelle, tournée vers la performance d'Enes et la satisfaction de ses clients.

A cet égard, toute information conçue, émise, reçue ou stockée sur le poste de travail et les moyens de communication mis à sa disposition, est et demeure la propriété d'Enes.

Toutefois une utilisation ponctuelle des Ressources Informatiques pour un motif personnel, syndical, et social est autorisée, à la condition qu'elle reste dans des limites raisonnables.

La présente charte ne fait pas obstacle à ce que des dispositions spécifiques soient définies par Enes en vue d'une utilisation des Ressources Informatiques, électroniques et numériques par les représentants du personnel.

Chaque utilisateur doit être conscient que, d'une part, l'usage de ces ressources obéit à des règles qui s'inscrivent dans le respect de la loi et du code de déontologie d'Enes, dans le respect de la sécurité d'Enes et de bonnes pratiques, gages d'efficacité opérationnelle, et que, d'autre part, sa négligence ou la mauvaise utilisation de celles-ci fait encourir des risques à Enes, et donc à lui-même.

Chacun est responsable de l'usage qu'il fait des outils, données et moyens de communication.

3. DROITS ET DEVOIRS

3.1. Champ d'application de la charte

La présente Charte a pour objet de définir les principales règles d'utilisation et obligations s'appliquant à tout Utilisateur des Ressources Informatiques d'Enes ainsi que des Ressources Informatiques extérieures accessibles via les réseaux informatiques d'Enes. Elle informe des précautions que tout Utilisateur doit respecter, et mettre en œuvre.

Les contrats entre Enes et tout tiers donnant accès aux données, aux programmes informatiques ou autres Ressources Informatiques d'Enes, devront stipuler que les utilisateurs extérieurs s'engagent à respecter la Charte Prestataire

3.2. Application de la charte

Le droit d'accès aux Ressources Informatiques d'Enes est subordonné à la signature de la présente charte. Ce droit est personnel et incessible, et disparaît lorsque les raisons de cet accès disparaissent.

Ce droit est limité à des activités conformes aux missions d'Enes.

En qualité d'utilisateur des ressources d'Enes, chaque utilisateur s'engage à connaître, à appliquer, faire appliquer le cas échéant l'ensemble des dispositions de la présente Charte.

Les agents d'ENES doivent agir en utilisateurs responsables et avertis.

Enes s'engage, pour sa part, à mettre en œuvre tous les moyens pertinents, compte tenu de l'état de l'art des techniques, afin de garantir la meilleure sécurité possible des installations, des personnes, des données et des informations qu'elle gère.

3.3. Sanctions applicables

Tout Utilisateur n'ayant pas respecté la présente Charte, c'est-à-dire les règles et obligations qui s'y trouvent définies, et qu'il a librement acceptées, comme ses obligations purement légales, sera susceptible :

- d'être sanctionné en application du règlement intérieur d'Enes (Article 14),
- de faire l'objet le cas échéant d'une plainte et de poursuites judiciaires mêmes pénales.

4. ROLE DES ADMINISTRATEURS DU SYSTEME D'INFORMATION

Les Ressources Informatiques d'Enes sont gérées par des « Administrateurs » missionnés par Enes qui s'engagent à prendre toute disposition utile pour permettre le bon fonctionnement des Ressources Informatiques communes.

Les Administrateurs ont pour missions de :

- proposer au Directeur le cadre de la politique de sécurité des systèmes d'Information,
- de mettre en œuvre les décisions en matière de sécurité des systèmes d'information,
- d'administrer et gérer au quotidien les outils mis en œuvre.

De ce fait, ils

- autorisent les accès aux Ressources Informatiques.
- attribuent les comptes et les mots de passe ou tout autre dispositif permettant l'accès aux Ressources Informatiques conformément à la politique d'Enes,
- assurent le fonctionnement et la disponibilité normale des Ressources Informatiques,
- définissent et mettent en œuvre les moyens appropriés, en l'état de la technique, pour protéger les utilisateurs et pour protéger les ressources mises à leur disposition contre tout risque de destruction ou d'altération.

L'administrateur système est chargé, de gérer, de garantir l'intégrité des données, le bon fonctionnement ainsi que la sécurité du système informatique.

Il a donc connaissance de toutes les données collectées ainsi que l'utilisation des différents services proposés avec l'obligation de confidentialité y afférant.

L'administrateur ne doit faire aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des applications des informations des réseaux et systèmes.

Un administrateur n'est pas en droit d'accéder à des ressources protégées par un mot de passe personnel d'un utilisateur à son insu. Exceptionnellement, en cas d'absence d'un utilisateur, et à des fins de bon fonctionnement de l'activité, l'employeur peut demander à un administrateur de forcer l'accès en écrasant un mot de passe personnel.

5. RESPECTS DE LA VIE PRIVEE

Enes respecte le principe de protection de l'intimité de la vie privée de ses collaborateurs sur son lieu de travail et donc du secret des correspondances et des fichiers relevant des activités personnelles, syndicales ou sociales. Ces messages et ces fichiers doivent être placés par les utilisateurs dans des dossiers dont les noms sont explicites : personnel,

syndical (ou le nom du syndicat), social, ... Aucun autre utilisateur que le propriétaire n'est autorisé à accéder au contenu de ces dossiers.

6. REGLES D'UTILISATION DES RESSOURCES : ADOPTER LES BONS REFLEXES

6.1. Règles Générales

L'utilisateur est responsable de l'usage qu'il fait des Ressources Informatiques d'Enes dans l'exercice de sa fonction au sein d'Enes.

Il doit en réserver l'usage au cadre de son activité professionnelle sauf exception visée au chapitre 5 de la présente charte.

Par conséquent, il ne doit en aucune circonstance charger, stocker, publier, diffuser ou distribuer, au moyen des Ressources Informatique d'Enes, des documents, informations, images, vidéos, etc. :

- à caractère violent, pornographique ou contraire aux bonnes mœurs, ou susceptibles de porter atteinte au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs,
- de caractère diffamatoire et de manière générale illicite,
- portant atteinte aux Ressources Informatique d'Enes et plus particulièrement à l'intégrité et à la conservation des données d'Enes,
- portant atteinte à l'image de marque interne et externe d'Enes.

Il est interdit d'accéder à des serveurs Web traitant de ces sujets avec le risque de voir l'adresse e-mail de l'utilisateur reprise dans un courrier de masse comportant des pièces jointes illicites. Si l'utilisateur est amené à recevoir, à son insu, de tels éléments, il est tenu de les détruire aussitôt.

L'utilisateur doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents sous forme d'informations, d'images, de vidéos, de fichiers, etc.

Il est interdit

- d'utiliser les Ressources Informatique d'Enes à des fins de harcèlement, menace ou d'injure et de manière générale de violer des lois en vigueur,
- de charger, stocker ou transmettre des fichiers contenant des «données personnelles» protégés par les lois sur les données personnelles, sauf à posséder les autorisations nécessaires,
- de charger, stocker ou transmettre des fichiers contenant des éléments protégés par les lois sur la propriété intellectuelle, sauf à posséder les autorisations nécessaires. L'utilisateur s'interdit de solliciter l'envoi par des tiers, en pièces jointes, de tels fichiers,
- de charger, stocker, utiliser ou transmettre des programmes, logiciels, progiciels, etc., qui sont protégés par les lois sur la propriété intellectuelle, autres que ceux qui sont expressément autorisés par Enes. L'utilisateur s'interdit de solliciter l'envoi par des tiers, en pièces jointes, de tels programmes, logiciels, progiciels, etc..
- d'utiliser les matériels, programmes, logiciels, progiciels, etc., mis à sa disposition par Enes, en violation des lois sur la propriété intellectuelle, des règles techniques et des prescriptions définies par Enes,

- de charger ou transmettre, sciemment, des fichiers contenant des virus ou des données altérées,
- de falsifier la source d'éléments contenus dans le référentiel des données géré par Enes.
- d'envoyer des messages en masse (plus de 20 destinataires, hors diffusion sur des listes d'Enes pour raisons de service) ou en chaîne (messages reçus individuellement dans le cadre d'une diffusion collective avec invitation à le renvoyer également collectivement),
- d'utiliser les Ressources Informatiques d'Enes de manière à gêner l'accès des autres utilisateurs.

Chacun doit veiller, par des règles à paramétrer en cas d'absence, à s'assurer de la bonne continuité du fonctionnement du service

Pour rappel, certaines des activités énoncées ci-dessus peuvent constituer des infractions de nature à faire l'objet de poursuite pénale y compris par d'autres entités qu'Enes.

Enes se réserve la possibilité d'effectuer des vérifications et contrôles réguliers, dans les limites et conditions prévues par la loi.

Par ailleurs, l'usage de certains services accessibles en ligne à des particuliers peut faire l'objet de contrats commerciaux si ces services sont utilisés à des fins professionnelles (géolocalisation, API Google, ...). Dans le doute, les utilisateurs devront se rapprocher du service informatique.

Enes étant distributeur de contenus de communications électroniques et audiovisuelles, ainsi qu'éditeur de programmes de télévision, les utilisateurs ont un devoir d'exemplarité dans le respect des droits des éditeurs de contenus qu'ils nous ont confiés, et dans l'application et le respect des lois encadrant les règles énoncées ci-dessus.

6.2. Mesures de sécurité

Afin de permettre la mise en œuvre par Enes d'une parade de premier niveau, l'utilisateur doit respecter au minimum les prescriptions suivantes :

- | | |
|-----------------|---|
| Prescription 1 | Mettre toujours un mot de passe quand il lui est demandé |
| Prescription 2 | Changer de mot de passe régulièrement, en mélangeant majuscules, minuscules et chiffres |
| Prescription 3 | Ne jamais prêter son identifiant/mot de passe |
| Prescription 4 | Protéger en déposant ses fichiers Enes sur les disques réseaux mis à disposition afin de disposer d'une sauvegarde |
| Prescription 5 | Ne pas répondre, ni être le relais aux messages en masse |
| Prescription 6 | Ne pas installer de logiciels même Freeware sans accord du service informatique |
| Prescription 7 | Ne pas laisser des intervenants extérieurs prendre le contrôle de son poste, ni intervenir sur son poste, en son absence, |
| Prescription 8 | Ne jamais quitter son poste de travail sans avoir verrouillé sa session en cours |
| Prescription 9 | En quittant Enes, quitter ses applications en cours et éteindre son poste, de préférence par arrêt logiciel et non par l'interrupteur pour terminer proprement ses sessions (hors cas de blocage technique) |
| Prescription 10 | Ne pas laisser à disposition des supports informatiques (Clé USB, CDRom, disque dur externe...) contenant des données confidentielles, dans un bureau ouvert |
| Prescription 11 | Ne pas oublier de récupérer, sur les fax, imprimantes ou photocopieurs, les documents sensibles que l'on envoie, imprime ou photocopie. |

L'absence de respect des prescriptions ci-dessus ne pourra être sanctionnée, conformément à l'article 3.3 de la présente charte, que si les manquements observés ont nui ou sont susceptibles de nuire à Enes ou aux personnes qui s'y trouvent, ou ont été réitérés en dépit de mises en garde.

6.3. Matériels, programmes, logiciels, etc

Enes met à la disposition de l'utilisateur des ressources (PC, stations, serveurs « assistants personnels numériques », téléphones multifonctions, fax, etc.) pour exercer son activité professionnelle conformes aux règles juridiques et techniques applicables et aux prescriptions définies par Enes (standards). L'utilisateur s'interdit par conséquent de modifier ces standards, notamment par l'ajout de logiciels hors standards pour lesquels Enes pourrait être accusée de piratage, en dehors d'incompatibilités potentielles. A des fins de précaution, certaines configurations peuvent être verrouillées par Enes (poste de travail, etc.).

Le disque dur du poste de travail de l'utilisateur ne doit pas contenir de programmes, logiciels, documents, fichiers, informations ou données, tels que rappelés ci-dessus, et notamment des fichiers à caractère pornographique, nazi ou raciste ainsi que tout autre fichier prohibé par la loi.

6.4. Ordinateurs portables et périphériques externes

Les utilisateurs de postes portables s'engagent, quel que soit l'endroit où ils se trouvent, à sécuriser leur matériel et l'accès aux données qu'il contient. L'utilisateur ne doit jamais transporter l'intégralité de fichiers qui auraient une valeur stratégique ou confidentielle pour Enes. Nous préconisons le cryptage des informations et données sensibles stockées sur le disque dur de son poste portable. Un outil de cryptage est mis à la disposition des utilisateurs à cet effet.

Il en est de même pour les périphériques externes : clés usb, disque dur, ...

Les ressources mises à la disposition de tout utilisateur, et notamment les disques durs externes, clés usb,..., pourront faire l'objet de vérifications et de contrôles par Enes, dans les limites prévues par la loi.

6.5. Accès distant, VPN, smartphone, clients de messageries et WebMail

L'utilisateur s'engage à agir pour que les Ressources Informatiques qu'il utilise afin d'accéder à celles d'Enes ne deviennent pas un point d'accès pour des personnes non autorisées. A ce titre l'utilisateur doit être vigilant sur les conditions extérieures et le lieu à partir duquel il effectue un accès distant aux Ressources Informatiques d'Enes. En aucun cas il ne doit laisser une session active, même pour un temps très court, en dehors de sa présence. Le verrouillage ou la déconnexion sont impératifs.

6.6. Virus Informatiques

Le poste de travail (station, micros, portable, etc.) de chaque utilisateur est en règle générale équipé d'un logiciel anti-virus.

Cependant, l'utilisation des applications communicantes (internet, messagerie, etc.) et des supports de stockage (disque dur externe, clé USB, CD-Rom,...), peut, malgré les précautions prises, provoquer la transmission et l'installation sur le poste de travail de l'utilisateur, à l'insu de ce dernier, de programmes ou fichiers, qui altèrent ou pillent les données et logiciels qu'il contient.

En cas d'anomalie, l'utilisateur doit stopper toute transaction et prévenir immédiatement le service informatique.

6.7. Messagerie électronique et autres moyens de communications écrits

6.7.1. Conseils généraux

L'utilisation des outils de messagerie électronique est réservée à un usage strictement professionnel sauf exception visée à l'article 5 de la présente charte.

Toute utilisation à des fins promotionnelles est interdite.

L'utilisateur doit respecter le secret de la correspondance échangée (usage du contenu d'un mail ou à l'insu de son émetteur).

L'utilisateur ne peut engager la responsabilité d'ENES au travers de ses propos ou du contenu de ses messages électroniques que s'il en a explicitement l'autorisation dans le cadre de ses activités professionnelles.

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. 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/ou de l'utilisateur.

L'envoi de messages électroniques à des tiers obéit aux mêmes règles que l'envoi de correspondances postales, en particulier en termes d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient de référer à l'autorité hiérarchique.

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

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,

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel. Les messages doivent, dans ce cas, être cryptés, conformément aux recommandations du service informatique.

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, le cas échéant, être doublés par des envois postaux.

6.7.2. Limites techniques

La taille, le nombre et le type des pièces jointes peuvent être limités pour éviter l'engorgement du système de messagerie.

Les messages électroniques sont conservés indéfiniment.

Toutefois, Il appartient au salarié de classer les messages professionnels qu'il envoie et reçoit dans le cadre d'un plan de classement compréhensible. Il lui est également demandé de faire une copie des messages importants dans les dossiers des fichiers relatifs à la question posée, comme il le ferait avec une télécopie classée dans le dossier papier concerné.

6.7.3. 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 « Message Privé » dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé «Message Privé».

Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé «Message Privé ».

A défaut, les messages sont présumés être à caractère professionnel.

6.8. Publications sur Internet

Publier sur un réseau social est équivalent à publier dans un média traditionnel (presse, télévision, radio).

Il est strictement interdit à un utilisateur de publier sur les réseaux sociaux dans le cadre de son exercice ou dans le cadre privé toute information qu'il détiendrait relative à Enes, ses clients et ses partenaires.

Tout manquement à cette règle entraînerait des sanctions telles que décrites à l'article 3.3 de la présente charte.

6.9. Internet

L'Internet est un outil qui est mis à la disposition de l'utilisateur à titre professionnel sauf exception visée à l'article 5 de la présente charte. Il doit donc en faire un usage approprié.

L'accès à Internet est attribué individuellement à chaque utilisateur, afin de lui permettre de visiter, à des fins professionnelles, des sites du monde entier sous le nom d'Enes. Toutefois, lorsqu'il «navigue» sur le Web, l'identifiant de l'utilisateur ainsi que les sites visités sont enregistrés dans les limites prévues par la loi. D'autre part, la direction d'Enes se réserve le droit de filtrer certains sites dont l'accès n'est pas jugé nécessaire par elle dans le cadre d'une mission strictement professionnelle.

En outre, chaque site internet pouvant être régi par des règles juridiques autres que le droit français, toutes précautions doivent être prises à cet égard par l'utilisateur.

Par ailleurs, toutes les activités de l'utilisateur ainsi que les données concernant l'utilisateur (sites consultés, messages échangés, données fournies à travers des formulaires, données collectées à l'insu de l'utilisateur, etc.) peuvent être enregistrées par des tiers, analysées pour en déduire ses centres d'intérêt, les préoccupations d'Enes, ..., et utilisées à des fins commerciales ou autres. Toutes précautions doivent également être prises par l'utilisateur à cet égard.

A des fins de statistiques, de qualité de service et de sécurité, le trafic Internet est sujet à une supervision et à des vérifications et audits réguliers par Enes, dans les limites prévues par la loi.

6.10. Suppression des comptes

En cas de départ définitif d'un salarié, ses comptes d'accès et les droits associés seront supprimés immédiatement.

Son compte de messagerie sera placé sur répondeur pendant une durée de deux mois. Passé ce délai, le compte de messagerie sera supprimé. L'entreprise se réserve le droit de consulter les messages à caractère professionnel avant la suppression du compte.

6.11. Données et informations d'Enes

Enes est responsable de :

- la mise à disposition de Ressources Informatiques sécurisées conformes aux règles juridiques et techniques applicables et aux prescriptions définies par Enes,
- la maintenance technique des Ressources Informatiques, de leur sécurisation et de leur sauvegarde ou archivage. Il est à noter que l'espace de stockage One Drive dont bénéficient certains ordinateurs n'est pas sauvegardé par Enes. Les utilisateurs feront leur affaire de copier et sauvegarder les contenus sur leur espace One Drive sur le serveur de fichier d'Enes.

Toute perte, divulgation ou altération est susceptible de causer un préjudice important à Enes ou à des tiers. Chaque utilisateur doit veiller à respecter Enes, ses salariés et ses clients et réserver l'usage d'informations stratégiques et/ou confidentielles au strict cadre professionnel dans le cadre des missions qui lui sont explicitement confiées à ce sujet.

Par défaut les informations sont professionnelles et doivent être accessibles par la hiérarchie et les nécessités de service sauf si figurent les mentions personnel et confidentiel.

La recopie ou duplication d'informations professionnelles à des fins autres que professionnelles est interdite en particulier en cas d'accès distant ou en dehors de locaux d'Enes.

L'utilisateur est responsable de l'usage qu'il fait de la pérennité de ses fichiers, données, informations, etc., ainsi que des accès de lecture et de modification qu'il peut donner à d'autres personnes ou Utilisateurs.

L'utilisateur ayant accès à des données personnelles des clients ne doit en faire usage que dans le cadre de son travail et en préserver la confidentialité. Toute diffusion ou utilisation est interdite.

6.12. Vigilance et information

Il est demandé à chaque utilisateur de signaler toute tentative de violation de son poste de travail ou de ses fichiers ou données, dès qu'il en a connaissance, auprès du Responsable du Service Informatique d'Enes afin de pouvoir apprécier l'imputabilité personnelle des incidents qui pourraient survenir.

De façon générale, il est demandé à chaque utilisateur d'alerter en cas de panne, dysfonctionnement, ou erreur le responsable du service informatique d'Enes.

Les utilisateurs qui perdent des données stockées sur un support amovible par mégarde ou par vol comme des identifiants de connexion, des données propres aux clients, doivent immédiatement en informer le service informatique.

6.13. Prestataires et sous-traitants

Il est demandé à chaque Utilisateur de faire signer la Charte Prestataire avant l'intervention d'un utilisateur externe et de veiller aux respects de celle-ci.

7. ENTREE EN VIGUEUR

La présente charte a été soumise à l'avis de la commission secondaire du personnel d'Enes, qui a été informée et consultée conformément aux articles L122-36 et L. 432-2-1 alinéa 3 du Code du Travail. Elle s'applique, les formalités requises achevées, à la date du 14 novembre 2016.

8. ANNEXES

8.1. Textes de loi référents

Pour mémoire les principaux textes permettant de respecter la législation française et en particulier les aspects liés à la sécurité informatique sont :

- loi du 6/1/1978 dite "Informatique et Libertés"
- législation relative à la fraude informatique, article 323-1 à 323-7 du code pénal
- loi du 10/7/1991 relative au secret des correspondances émises par voie de télécommunication
- législation relative à la propriété intellectuelle dans son article n°L122-6-1
- législation applicable en matière de cryptologie, notamment l'article 28 de la loi du 29/12/1990 sur la réglementation des télécommunications
- législations sur l'audiovisuel et les télécommunications en ce qui concerne les grands principes applicables aux communications publiques et privées
- loi du 6/01/1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6/8/2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel
- décret n°2006-358 du 24/3/2006 relatif à la conservation des communications électroniques (journal officiel n°73 du 26/3/2006)
- loi n°2006-64 du 24/1/2006 relative à la lutte contre le terrorisme et portant dispositions diverses relative à la sécurité et aux contrôle frontaliers (journal officiel n°20 du 24/1/2004)
- loi n°85-660 du 3/1/1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle

8.2. Sites internet utiles

<http://www.ssi.gouv.fr/fr/bonnes-pratiques/principes-generaux/>

Hombourg-Haut, le 22 septembre 2016

Le Directeur
S. DIDIERJEAN.



Signature des agents :

BAILLY Stéphanie



DAUVERGNE Aurélie



GAMEL Stéphanie



HOY Christiane



KUS Jérémy



MERLE Benjamin



MULLER Frédéric



PARTICELLI Yann



PEIFFER Nadine



PETIT Christian



PICHON Fabien



ROTHENMACHER Daniel



THIL Denis



