CHARTE INFORMATIQUE

Sécurité du Système d'Information

Conditions d'utilisation de "pléiade"

Version : 2017

Commune d'Yvré le Pôlin

Visa du responsable fonctionnelle du SI	Visa des représentants du personnel (CTD, Syndicats)	Visa du responsable juridique de l'entitée couverte par le SI
Date :	Date :	Date :

HISTORIQUE DE VERSIONS

Indice	Date	Rédacteur	Création/Modification	Page(s)
1.0	14/08/17	JF.Bellanger	Création	Toutes

SOMMAIRE

DÉFINITION

Le bon fonctionnement du système d'information implique le respect des dispositions législatives et réglementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.

L'association "antiskwat" hébergé dans les locaux de la maison des jeunes

se dote d'une charte qui régit l'usage du système d'information par les utilisateurs, et définit les règles d'usage et de sécurité que l'institution et l'utilisateur s'engagent à respecter ainsi que les droits et devoirs de chacun.

Pour accéder au système d'information, les utilisateurs doivent s'engager à respecter les termes de la présente charte.

La charte a valeur de règlement intérieur pour ce qui concerne l'usage du système d'information. Adoptée par les représentants du personnel du 01 juillet 2017, la charte entre en vigueur pour tous les utilisateurs à compter du 01 septembre 2017.

Par «institution» il faut entendre tout service de

l'association et partenaire intervenant pour l'association "antiskwat".

Le "système d'information" recouvre l'ensemble des ressources matérielles et logicielles, les applications, les bases de données et les réseaux de télécommunications pouvant être mis à disposition par l'institution. L'informatique nomade (assistants personnels, ordinateurs portables, tablettes, téléphones portables, etc.) est également un des éléments constitutifs du système d'information dès lors qu'il est mis à disposition par l'institution ou qu'il est connecté quand il est personnel.

Le terme d'«utilisateur» recouvre tout personnel (employés ou bénévoles) ayant accès, dans le cadre de l'exercice de son activité professionnelle ou associatif, au système d'information quel que soit son statut.
Il s'agit notamment de :
- tout agent titulaire ou non titulaire concourant à l'exécution des missions du service;
- tout bénévole ou volontaire intervenant pour et au nom de l'association ;
- tout prestataire ayant contracté avec l'institution, avec une collectivité territoriale ou une association ayant une compétence partagée avec l'état.

La présente charte définit les règles d'usage et de sécurité que l'institution et l'utilisateur s'engagent à respecter.
Elle précise les droits et devoirs de chacun. À ce titre l'institution doit la communiquer à l'utilisateur qui en prend connaissance.

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'institution ainsi qu'à l'ensemble des utilisateurs du système d'information (y compris les intervenants extérieurs à l'institution) !

DROITS ET OBLIGATIONS BILATÉRALES

DROITS ET OBLIGATIONS DE L'INSTITUTION :

L'institution met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs et de leurs données.

L'institution facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'institution est tenue de respecter l'utilisation résiduelle du système d'information à titre privé comme le prévoit la Commission Nationale Informatique et Libertés.

L'institution délivrera à l'utilisateur un identifiant et un mot de passe temporaire que ce dernier devra changer lors de la première utilisation.

L'institution fournie un compte utilisateur profilé pour les besoins strictement nécessaires de l'utilisateur.

L'institution s'engage à signaler à l'utilisateur toutes tentatives ou compromission de son système d'information et s'oblige à mettre en place un système de remédiation.

DROITS ET OBLIGATIONS DE L'UTILISATEUR

L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès. Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des lois en vigueur ainsi que des règles d'éthique professionnelle et de déontologie.

À ce titre, il s'interdit toute utilisation des ressources informatiques et d'Internet à des fins commerciales, personnelles (forum de discussion, réseaux sociaux, …), ou à des fins ludiques (jeux multimédias « en réseau » ou autres) sans lien avec son activité professionnelle.

Chaque utilisateur s'engage à avoir une utilisation loyale du réseau et à respecter le matériel et les locaux informatiques, mis à sa disposition.

L'utilisateur signalera toute tentative de violation de son compte (identifiant…).

En cas de non-respect, la responsabilité de l'utilisateur pourra être engagée. Tout abus de l'utilisation des ressources mises à disposition à des fins extra professionnelles peut être de nature à enclencher une procédure disciplinaire à son encontre.

Par ailleurs le responsable hiérarchique pourra, sans préjuger des poursuites ou procédures pouvant être engagées, limiter les usages par mesure conservatoire.

En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

1 CONDITIONS D'UTILISATION DES SYSTÈMES D'INFORMATION

RAPPEL

L'institution propose à l'utilisateur un système d'information lui permettant de travailler dans un environnement professionnel et sécurisé.
- la mise à disposition d'un poste de travail, individuel ou partagé, fixe ou mobile ;
- la mise à disposition d'un espace de stockage de ses données ;
- la sauvegarde et la restauration de ses données ;
- un service d'impression.

Dans le cadre d'une compétence partagée, cette offre de services est à mettre en œuvre en partenariat avec la collectivité, l'association ou l'entreprise de rattachement.

1.1 UTILISATION PROFESSIONNELLE ET PRIVÉE

Les systèmes d'information (notamment messagerie, internet, imprimante …) sont des outils de travail mis à disposition pour des usages professionnels.
Ils peuvent également constituer le support d'une communication privée dans les conditions décrites ci-dessous.

L'utilisation du système d'information à titre privé doit être résiduelle, tant dans sa fréquence que dans sa durée, et non lucrative. Les conséquences, dont en particulier le surcoût qui en résulte, doivent demeurer négligeables au regard du fonctionnement et du coût global d'exploitation.

Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur et au bon fonctionnement du service.
Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.

Ainsi il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données dénommé explicitement *(Par exemple, cet espace pourrait être dénommé "privé")* ou en mentionnant le caractère privé sur la ressource *(Par exemple, "privé – nom objet" : l'objet pouvant être un message, un fichier ou toute autre ressource numérique)*.
La sauvegarde régulière des données à caractère privé incombera à l'utilisateur qui est responsable de son espace de données à caractère privé.

Les espaces de partage fournis par l'institution ne doivent pas servir à cet usage privé.
Lors de son départ définitif du service ou de l'établissement, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'administration ne pouvant être engagée quant à la conservation de cet espace.

L'utilisation des systèmes d'information à titre privé doit respecter la législation en vigueur et s'inscrire dans le cadre du respect des obligations et de la déontologie propres aux fonctionnaires rappelés dans la loi n°83-634 du 13 juillet 1983 relative aux droits et obligations des fonctionnaires.

1.2 GESTION DES ABSCENCES ET DES DEPARTS

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités permettant l'accès aux ressources mises spécifiquement à sa disposition lors de son départ définitif (si besoin).

En cas d'absence prolongée (supérieure à 30 jours consécutifs), l'utilisateur devra le faire savoir au service informatique qui suspendra temporairement l'usage du compte.

En cas de départ définitif, l'utilisateur préviendra au moins 15 jours avant son départ le service informatique qui supprimera son compte la date venue.

Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'institution.

Si du matériel a été prêté à l'utilisateur ou un partenaire associatif, l'usager s'assurera de le conserver en lieu sûr, à l'abri de personne n'ayant pas l'approbation de l'institution ou de l'utilisateur pour y accéder.

L'utilisateur s'interdit de chercher à affaiblir la sécurité ou de laisser à disposition les instructions d'accès au matériel de l'institution en son absence.

2 MESURE DE CONTRÔLE DE LA SÉCURITÉ

RAPPEL

L'institution est dans l'obligation légale de mettre en place un système de journalisation *(Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur)* des accès Internet et des données échangées.

Préalablement à cette mise en place, l'institution a procédé, auprès du Correspondant Informatique et Libertés *(CIL)*, à une déclaration qui mentionnera notamment la durée de conservation des traces et la durée de connexion, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n° 78-17 du 6 janvier 1978 modifiée.

Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions. Dès lors que ces informations sont couvertes par le secret des correspondances ou identifiées comme telles, elles relèvent de la vie privée de l'utilisateur.

En revanche l'article 40 alinéas 2 du code de procédure pénale impose à tout fonctionnaire ou agent public d'informer sans délai le procureur de la République de tout crime ou délit dont il a connaissance dans l'exercice de ses fonctions.

2.1 L'UTILISATEUR

L'utilisateur est informé que :

- pour effectuer la maintenance corrective, curative ou évolutive, l'institution se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- une maintenance à distance est précédée d'une information de l'utilisateur ;
- toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée; le cas échéant supprimée ;
- le système d'information est l'objet d'une surveillance et d'un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions :

- s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'institution des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés et/ou ne provenant pas de sites dignes de confiance ;
- se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques

par programmes informatiques ;
- avertir dans les meilleurs délais sa hiérarchie qui en réfère au Responsable de la Sécurité des Systèmes d'Information via la gestion des incidents mise à sa disposition, de tout dysfonctionnement constaté ou de toute anomalie découverte (par exemple une intrusion dans le système d'information ou un accès non autorisé à une ressource sensible ou confidentielle).
- respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ;
- garder strictement confidentiel(s) son (ou ses) code(s) d'accès et ne pas le(s) dévoiler à un tiers ;
- ne pas conserver le mot de passe par défaut ;
- respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître.

2.2 L'INSTITUTION

La sécurité des systèmes d'information que l'institution met à disposition lui impose de:

Mettre en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition de l'utilisateur.

D'informer l'utilisateur que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel. Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est conférée.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions:

- porter à la connaissance de l'utilisateur de manière explicite ses habilitations ;
- contrôler et mettre à jour les habilitations ;
- veiller à ce que les ressources sensibles ou confidentielles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie ;
- porter à la connaissance de l'utilisateur les éléments susceptibles de lui permettre de sécuriser l'usage du système d'information, dont le matériel personnel à usage professionnel.

3 COMMUNICATION ÉLECTRONIQUE

RAPPEL

L'institution déploie des dispositifs « anti-virus » et « anti-spam » qui contribuent à éviter la propagation des virus et bloquent (au mieux des possibilités qu'offre la technique) les messages non sollicités.
L'utilisation de la communication électronique constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'échange de l'information au sein de l'institution.

3.1 ÉMISSION ET RÉCEPTION DE MESSAGES

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé ou s'il est stocké dans un espace privé de données.

Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés et portés à la connaissance de l'utilisateur par le fournisseur de service de messagerie.

À partir du réseau de l'institution, sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques…).

Le réseau de l'institution ne saurait être un vecteur de provocation et à ce titre, l'utilisateur agit dans le respect de l'ordre public et s'interdit notamment toute provocation à un acte malveillant de quelle que nature que ce soit (trouble à l'ordre public, incitation au racisme, au terrorisme, au suicide …) ou toute diffusion de message à caractère violent de nature à porter atteinte à la dignité humaine.

De manière générale, l'utilisateur veille au respect de la personnalité, de l'intimité et de la vie privée d'autrui, y compris de ces collègues en s'interdisant par un procédé quelconque et notamment par la transmission sans son consentement de son image ou de ses écrits diffusés à titre confidentiel ou privé.

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages.
Il doit veiller, comme l'institution, à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile du réseau de consultation ainsi qu'une dégradation du service.

Il veille également à ne pas émettre d'informations sensibles ou confidentielles. En cas de nécessité liée à ses fonctions, il devra alors s'assurer, avant toute émission, que l'institution a mis à sa disposition les modalités de sécurité adaptées au niveau de sécurité de l'information traitée.

3.2 STATUT ET VALEURS JURIDIQUE DES MESSAGES

Quel que soit le lieu, le mode d'accès et le moyen de communication électronique ou le prestataire, les règles prévues par la présente charte s'appliquent intégralement. Les messages électroniques échangés avec des tiers peuvent revêtir une forme juridique, sous réserve du respect des conditions fixées par les articles 1125 à 1125-6 du code civil.L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

4 UTILISATION DU RÉSEAU INTERNET

RAPPEL

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'institution. Internet est un outil de travail ouvert à des usages professionnels.
Si une utilisation résiduelle privée, telle que définie en section 1.1 (page 5), peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'administration sont présumées avoir un caractère professionnel. L'administration peut les rechercher aux fins de les identifier.

4.1 PUBLICATION SUR LE RÉSEAU INTERNET

Toute publication de pages d'information sur les sites internet ou intranet de l'institution doit être validée par un responsable de site ou un responsable de publication nommément désigné.

Aucune publication de pages d'information à caractère privé sur les ressources du système d'information de l'institution n'est autorisée, sauf disposition particulière précisée dans un guide d'utilisation établi par le service ou l'établissement.

Aucune publication de pages d'information à caractère professionnel sur les ressources du système d'information de l'institution n'est autorisée, sans l'accord écrit du responsable de la sécurité du système d'information établi par le service ou l'institution.

4.2 SÉCURISATION DES USAGES SUR LE RÉSEAU INTERNET

L'Institution se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.
Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'institution.
Des règles de sécurité spécifiques peuvent être précisées, s'il y a lieu, dans un guide d'utilisation établi par le service ou l'institution.
L'utilisateur est informé des risques et des limites inhérents à l'utilisation d'Internet par le biais d'actions de formation ou de campagnes de sensibilisation.

4.3 TÉLÉCHARGEMENT DE CONTENU SUR LE RÉSEAU INTERNET

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définit le chapitre 5.1 (page 13).
L'institution se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'institution, codes malveillants, programmes espions …).

5 ENGAGEMENT MORAL

RAPPEL

Les données diffusées sur Internet ou intranet doivent avoir été obtenues licitement et ne pas porter atteinte au droit des tiers.
L'utilisateur des ressources informatiques et d'Internet doit veiller au respect du droit de propriété d'autrui.

5.1 RESPECT DE LA PROPRIÉTÉ INTELLECTUELLE

L'institution rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires liés par convention ou contrat et plus généralement, de tous tiers titulaires de tels droits.
En conséquence, chaque utilisateur doit :
- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

5.2 RESPECT DE LA LOI INFORMATIQUES ET LIBERTÉS

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 dite «Informatique et Libertés» modifiée, en particulier lors de la création de fichiers, auxquelles l'institution elle-même a l'obligation de se conformer.
Les données à caractère personnel sont des informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.
Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'Information.
Sauf mention particulière, ce droit s'exerce auprès du CIL sans préjudice des contestations portées directement à la CNIL.

5.3 LES RESPECT DE LA CONFIDENTIALITÉ

L'utilisateur respecte les contenus à caractère confidentiel, et s'engage particulièrement :
- A ne pas lire, copier, divulguer ou modifier les fichiers d'un autre utilisateur sans y avoir été explicitement autorisé par son propriétaire et/ou son auteur.
- A ne pas intercepter les communications entre tiers.

L'utilisateur qui enfreint une des règles énoncées dans la présente charte encourt d'éventuelles sanctions disciplinaires et/ou la suppression de son accès au réseau. Par ailleurs, il peut faire l'objet de poursuites pénales.

6 ORGANIGRAMME STRUCTUREL

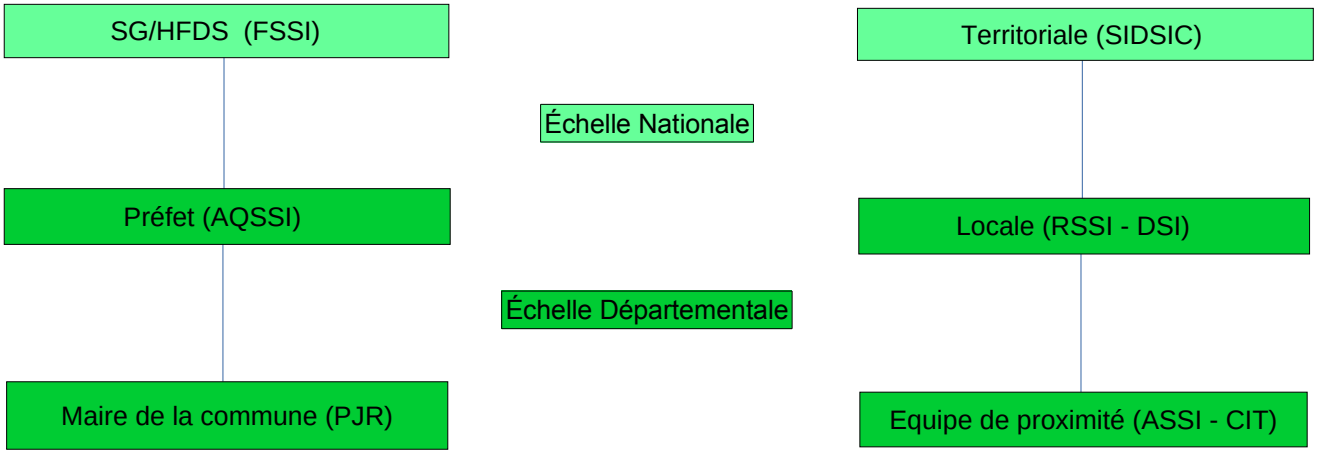
RAPPEL

L'organisation du système d'information est composé de 2 chaînes de responsabilités (la chaîne fonctionnelle et la chaîne organisationnelle & technique) ainsi que 2 niveaux décisionnelles (échelle nationale et échelle départementale).

6.1 LES ACTEURS DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION

CHAÎNE FONCTIONNELLE

CHAÎNE ORGANISATIONNELLE - TECHNIQUE



La charte a valeur de règlement intérieur pour ce qui concerne l'usage du système d'information.
Adoptée par les représentants du personnel le 1 septembre 2017 , elle entre en vigueur dans toute l'institution et pour tous les utilisateurs à compter de sa publication.

fait à : le :

Signature de l'utilisateur habilité :

Signature du gestionnaire d'habilitation :