Schéma Informatique Ministériel

Groupe Chartes d'usage des TIC

Charte d'usage des TIC

Introduction

Le développement et la diffusion au sein du MINEFI des nouveaux moyens de communication et d'information a connu ces dernières années un effet d'accélération important. L'ensemble des agents est ainsi conduit à utiliser, quotidiennement ou non, selon leurs fonctions, des outils de travail devenus de plus en plus puissants et dotés de capacités de diffusion immédiate et massive. Or, l'apparente facilité technique, la nouveauté de l'utilisation, le manque de repères peuvent susciter des questions, ou entraîner des risques méconnus, voire mal appréciés.

Dans ce nouveau contexte, il convient d'assurer à la fois, la qualité et la sécurité des systèmes d'information, la protection des données recueillies notamment auprès des usagers et de fournir les garanties que sont en droit d'attendre les agents du Ministère, au regard de leur vie privée.

Par la recherche d'un juste équilibre entre les droits et les obligations des utilisateurs, la présente Charte ministérielle a pour objectif de prévenir les situations de conflit et de favoriser la réalisation de prestations de qualité.

Les principes généraux énoncés dans le présent document concernent tous les utilisateurs du MINEFI. Enrichis des annexes spécifiques à chaque direction, ils seront déclinés en « chartes directionnelles », applicables aux seuls utilisateurs de ces entités et seront éventuellement complétés de documents utiles propres à chaque direction (chartes déontologique, de confiance, règles d'usage de la messagerie…).

L'appropriation de ces règles d'usage se fera par des actions d'information, de formation et de communication permettant à la fois une bonne compréhension par chaque agent des principes généraux de la charte et des annexes propres à sa direction, ainsi que leur utilisation effective et continue.

L'utilisation des nouveaux outils de communication et de gestion de l'information ne fait pas disparaître les règles de déontologie et de fonctionnement existant actuellement au sein du MINEFI. La diffusion des données obéit ainsi aux mêmes principes et règles en vigueur dans la fonction publique, quel que soit le support utilisé (papier ou dématérialisé). Les règles administratives (validation, compte-rendu hiérarchique, compétence, etc…) continuent de s'appliquer nonobstant la facilité nouvelle d'échanges et de communication.

N.B. - Certaines des situations évoquées dans la charte le sont à titre démonstratif ou préventif.

I - Domaine d'application

Les présentes règles s'imposent à toutes les personnes qui utilisent les ressources informatiques partagées et les services de communication mis à disposition par le Ministère (internet et intranet, messagerie, forum, etc…).
Elles s'adressent donc aux personnes travaillant au Ministère ou pour le Ministère, de façon permanente ou occasionnelle (agents, prestataires, stagiaires…).

Les modalités d'accès aux ressources par les organisations syndicales et leurs correspondants ainsi que leur utilisation au profit des agents font l'objet de dispositions figurant dans un protocole spécifique, publié sur l'intranet ALIZE.

II - Bonnes pratiques

a) Une utilisation raisonnée des ressources.

Dans le cadre des travaux initiaux du PAGSI et du développement de l'e-ministère, l'administration a eu la volonté d'offrir à chacun des outils et des ressources adaptés et fiables.

Chaque utilisateur veillera cependant à un emploi mesuré de ces ressources partagées afin de permettre une bonne qualité de service au plus grand nombre.

A titre d'illustration, des règles simples doivent être appliquées par tous :

Pour la messagerie, l'utilisateur veillera à adapter et limiter aux besoins ses messages, tant en contenu qu'en nombre de destinataires, et utilisera tous les moyens techniques mis à sa disposition pour en réduire la taille, tels que la compression éventuelle des pièces jointes, l'insertion de liens hypertexte, l'utilisation appropriée des listes de diffusion, etc…

Pour l'internet, une vigilance particulière est demandée dans la mise en œuvre de certains services, notamment pour les téléchargements de fichiers volumineux. Certains usages, fortement consommateurs de ressources réseau peuvent faire l'objet de restriction, voire d'interdiction.

Ces dispositions seront détaillées par chaque direction **(annexe 1).**

b) Un respect des procédures administratives et techniques fixées par le service.

Les procédures administratives portent notamment sur le respect des processus de circulation, de validation et de mise à disposition des informations, définis par la direction pour les échanges internes et externes.

Il s'agit par exemple des règles :

- d'utilisation des boites aux lettres fonctionnelles et personnelles,
- d'échanges entre les services déconcentrés et l'administration centrale, entre le ministère et l'extérieur (administrations, entreprises et particuliers),
- de conservation des documents et de publication des données, etc…

Les procédures techniques portent sur le respect des règles définies pour l'accès aux ressources et le paramétrage des logiciels de communication.
Il s'agit par exemple de n'utiliser que les modes d'accès internet autorisés.
Ces dispositions seront détaillées par chaque direction **(annexes 2 et 3)** et donneront lieu à des actions de formation et de communication.

III - Règles de Sécurité

L'ouverture d'un réseau informatique constitue toujours un risque pour la sécurité. Tout utilisateur contribue donc à la sécurité générale du système informatique; il est responsable de l'usage qu'il fait des ressources informatiques et du réseau auxquels il a accès.

Il convient donc de rappeler quelques règles de sécurité qui s'imposent à l'utilisateur :

a) Respecter la configuration du poste de travail

Sauf s'il y est autorisé, l'utilisateur ne doit pas modifier les périphériques et les logiciels de communication qui lui sont fournis ou installer de nouveaux équipements non agréés, notamment des modems.

b) Respecter les droits d'accès

Les droits d'accès sont attribués nommément à un utilisateur et n'ont pas vocation à être cédés. Ils sont protégés soit par un dispositif d'authentification forte (telle la carte à puce), soit par un mot de passe, afin de préserver l'accès aux ressources contre des tiers non autorisés. Dans ce dernier cas, le mot de passe doit être personnel, secret, complexe et changé périodiquement.

L'utilisateur ne doit pas masquer son identité ou tenter d'usurper celle d'un autre et, d'une manière générale, il ne doit pas utiliser des ressources autres que celles auxquelles il a légitimement accès.

Toute tentative d'intrusion ou toute anomalie constatée doit être signalée sans attendre, au responsable sécurité désigné par la direction de l'utilisateur.

c) Assurer la confidentialité

En l'absence de dispositifs de cryptage et de certification dans les échanges d'informations, la confidentialité et l'intégrité des messages et documents transitant sur l'internet ne peuvent pas être garanties. Chaque utilisateur s'engage à respecter les règles d'utilisation de la messagerie définies par sa direction, en fonction du degré de confidentialité des informations qu'il traite.
L'accès des utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, et à ceux qui sont publics ou partagés. Sauf mesures particulières prévues pour des nécessités de service, il est interdit de prendre connaissance et d'utiliser des informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

Les documents partagés ou publics disponibles dans les systèmes d'information ne peuvent être communiqués à des tiers qu'en application de règles définies par chaque unité ou d'autorisations spécifiques.

Ces dispositions seront détaillées par chaque direction **(annexe 4).**

d) Contribuer à lutter contre les malveillances

L'utilisateur doit respecter toutes les mesures visant à ne pas introduire et diffuser de virus dans les systèmes informatiques. Il appliquera les prescriptions de sa direction concernant l'activation et la mise à jour de son logiciel anti-virus ; celles-ci sont fonction de la configuration matérielle et logicielle dont il dispose (poste fixe, portable…). Toute attaque doit être signalée immédiatement aux responsables de la sécurité.

L'utilisateur doit veiller à ne pas donner suite aux demandes de rediffusion de messages alarmistes ou de suppression des fichiers.
Ces dispositions seront détaillées par chaque direction **(annexe 5).**

e) Sauvegarder ses données

Il appartient à l'utilisateur de protéger ses données en utilisant régulièrement les différents moyens de sauvegarde mis à sa disposition.

f) Sécuriser les portables

L'usage d'un portable, posant des problèmes spécifiques (vol, connexion aux ressources), son utilisateur se conformera aux règles spécifiques édictées par sa direction (**annexe 6**).

IV - Règles déontologiques

a) Utilisation des ressources

Les ressources sont mises à disposition pour un **usage professionnel**.
L'utilisation de ces ressources pour la création à des fins privées de services de communication n'est pas admise.

Toutefois, l'usage à titre privé des services web et de la messagerie est admis à condition que ce soit dans des limites raisonnables et qu'il n'affecte pas le trafic normal professionnel.
Cet usage doit être conforme aux obligations (de réserve, discrétion et neutralité) des fonctionnaires. Il ne doit pas être contraire à l'ordre public et aux bonnes mœurs. Il ne doit pas mettre en cause l'intérêt et la réputation de l'administration en accédant à des forums publics, des sites pornographiques, de jeux, etc…

Cet usage privé peut être restreint pour des raisons particulières (sécurité, performance…).
Ces dispositions seront précisées par chaque direction **(annexe 7).**

Il doit être considéré qu'un message reçu ou envoyé depuis le poste de travail mis à disposition par l'administration revêt un caractère professionnel. Toutefois sont considérés comme messages privés les messages comportant dans leur objet la mention « privé » ou classés dans un répertoire privé, ainsi que les échanges non professionnels avec les organisations syndicales, les services sociaux, les services médicaux **…**

b) Protection de la confidentialité des données de l'administration.

L'utilisateur est tenu de respecter la confidentialité des informations auxquelles il a accès ou qu'il gère, conformément aux obligations de secret professionnel et de discrétion.
Cette règle s'applique tant pour le traitement des informations que pour leur communication interne et externe. En particulier, pour toute information disponible sur un intranet, l'utilisateur doit s'assurer de la possibilité de diffusion avant toute communication à l'extérieur.

c) Protection du service

Tout message électronique comportant dans l'adresse de l'expéditeur l'identification de l'administration émettrice, engage, si ce n'est la responsabilité de celle-ci, du moins son image.

En conséquence, l'utilisateur doit respecter les règles de validation et le formalisme fixés par l'autorité hiérarchique dont il dépend.
L'utilisateur veille à respecter son devoir de réserve lorsqu'il s'exprime par l'intermédiaire des nouveaux outils de communication mis à sa disposition. Ainsi, lorsque l'utilisateur s'exprime à titre personnel, doit-il l'indiquer de manière explicite.

d) Forme des échanges

L'utilisateur doit s'exprimer avec prudence et courtoisie.
Il ne doit jamais écrire un message électronique qu'il s'interdirait d'exprimer oralement ou par un autre moyen.

Toute communication électronique peut en effet être conservée et considérée comme un élément de preuve.

e) Respect des lois et textes réglementaires

L'utilisateur s'interdit de produire, de collecter ou de transmettre des données, messages ou oeuvres en infraction avec la législation en vigueur, notamment les messages contraires à l'ordre public, diffamatoires, racistes, xénophobes, portant atteinte à la décence ou constituant une diffusion de fausses nouvelles.

L'utilisateur s'engage à prendre toutes dispositions pour consulter ou reproduire de manière licite les données ou œuvres protégées par des droits d'auteur, sous quelque forme que ce soit, notamment les logiciels, les œuvres audiovisuelles et littéraires.

NB : Certains sites Internet pouvant être régis par des règles juridiques autres que de droit français, toutes précautions doivent être prises à cet égard par l'utilisateur.

De la même façon, les agents en mission ou en poste à l'étranger, doivent se conformer aux règles édictées par leur direction pour cette situation.

V Traitement de contrôle

Tout utilisateur a droit au respect de ses données privées. Toutefois, il doit être conscient que les systèmes informatiques enregistrent et peuvent mémoriser les transactions et les informations de connexion.

a) Accès aux traces

Seuls les administrateurs techniques et les personnels habilités au titre de la sécurité disposent d'outils d'analyse, de surveillance et de contrôle.

Tenus au secret professionnel, ils ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni les intérêts de l'administration. Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens.

b) Traitements automatisés

Tout traitement automatisé d'informations nominatives dont l'objet est la sécurité du système d'information, le suivi, le contrôle de l'utilisation des ressources informatiques et des services internet doit faire l'objet d'une déclaration à la CNIL et être soumis à son contrôle.

Dans le cadre de ce traitement et suivant la gravité de l'anomalie constatée, seule l'autorité hiérarchique d'un niveau suffisant, déterminé dans chacune des directions, peut donner son accord préalable à un contrôle individuel détaillé. L'utilisateur concerné est immédiatement informé par écrit du contrôle.

Ces dispositions seront détaillées par chaque direction. (annexe 8)

VI Application de la charte

a) Mise en œuvre de la charte

Chaque direction devra définir les conditions de diffusion de la présente charte ; en outre, la publication sur les intranets directionnels et ministériel concernés permettra de garantir que tout utilisateur a le texte à sa disposition.

Elle devra veiller à expliquer le contenu du document, notamment à travers des actions de formation.
Elle devra publier les dispositions spécifiques qui dépendent des ressources dont elle a la charge.
Ces dispositions seront détaillées par chaque direction **(annexe 9)**

b) Respect des obligations de la charte

La mise en œuvre de cette charte répond aussi bien aux besoins de l'administration qu'à ceux des utilisateurs.
Les manquements qui seraient regardés comme des fautes professionnelles sont susceptibles d'entraîner pour l'utilisateur des sanctions disciplinaires sans préjudice d'éventuelles actions pénales ou civiles à son encontre.

c) Suivi et révision de la charte

Le suivi annuel et la révision de la présente charte feront l'objet d'une procédure concertée avec les représentants du personnel.

Liste des annexes

Principaux textes législatifs applicables

- Code civil, art. 9 (respect dû à la vie privée)
- Code pénal, notamment art. 226-13 à 226-14 (atteintes au secret professionnel), 226-15 (atteinte au secret des correspondances), 226-16 à 226-24 (atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques), 323-1 à 323-7 (atteinte aux systèmes de traitement automatisés de données)
- Code de la propriété intellectuelle
- Loi du 29 juillet 1881 sur la liberté de la presse, notamment le chapitre IV
- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et les actes réglementaires pris en application de son article 15 pour autoriser la mise en œuvre de traitements informatiques
- Loi n° 83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires, notamment art. 6 (liberté d'opinion), 8 (droit syndical) et 26 (obligations de discrétion et de secret professionnels, auxquelles sont rattachées les obligations de réserve et de neutralité)
- Loi n° 84-16 du 11 janvier 1984 modifiée portant obligations statutaires relatives à la fonction publique de l'Etat

1. Une consommation raisonnée des ressources de la direction

Objectif :
Prendre en compte les spécificités des systèmes des directions
Contenu :
Contraintes imposées sur les volumes, l'utilisation des média en fonction des volumes…

2. Le respect des procédures administratives fixées par la direction

Objectif :
Prendre en compte l'organisation particulière des directions

Contenu
Utilisation des boites aux lettres fonctionnelles ou d'unité ,
Circulation du courrier officiel
Règles d'archivage….

3. Le respect des procédures techniques fixées par la direction

Objectif :
Prendre en compte les potentialités des systèmes

Contenu :
Pour Internet : les modalités d'accès,

Pour la messagerie : le contenu des messages, l'identification de l'auteur, l'utilisation des accusés de réception, les messages d'absence….

Guide d'utilisation

4. Assurer la confidentialité

Objectif :

Préciser les règles d'utilisation des outils

Contenu :
La certification, le cryptage
Processus d'accès en cas d'absence

5. Lutter contre les malveillances

Objectif :
Règles de prévention des risques de virus

Contenu :
Antivirus, mise à jour

6. Sécurisation des portables

Protection particulière des données stockées ou accessibles.

7. Restriction à l'usage privé

Pour des raisons de sécurité ou de performance

8. Traitements automatisés à caractère personnel

Déclaration à la CNIL

9. Règles de mise en œuvre de la charte

Diffusion, formation, mise à jour