



CHARTE INFORMATIQUE

IRA de Metz

N°2022-01
Octobre 2022

Table des matières

Introduction	2
II. Domaine d'application	2
III. Bonnes pratiques	2
A. Une utilisation raisonnée des ressources	2
B. Un respect des procédures administratives et techniques fixées par l'IRA de METZ	3
IV. Règles de Sécurité.....	3
A. Respecter la configuration du poste de travail.....	3
B. Respecter les droits d'accès	3
C. Assurer la confidentialité	4
D. Contribuer à lutter contre les malveillances.....	4
E. Sauvegarder ses données	4
F. Sécuriser les portables.....	4
V. Règles déontologiques.....	5
A . Utilisation des ressources	5
B . Protection de la confidentialité des données de l'administration	5
C. Protection du service	5
D. Forme des échanges	5
E. Respect des lois et textes réglementaires	5
VI. Traitement de contrôle.....	6
A. Accès aux traces.....	6
B. Traitements automatisés	6
VII. Application de la charte	6
A. Mise en œuvre de la charte	6
B. Respect des obligations de la charte	6
C. Suivi et révision de la charte	7
VIII. Contenus illicites.....	7
IX. Cadre légal	7

Introduction

Le développement et la diffusion au sein de l'IRA 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 ainsi que la protection des données recueillies.

Par la recherche d'un juste équilibre entre les droits et les obligations des utilisateurs, la présente charte informatique 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 de l'IRA de METZ.

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 de l'IRA. 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.

II. 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 l'IRA de METZ (internet et intranet, messagerie, forum, applications, etc...).

Elles s'adressent donc aux personnes travaillant à l'IRA de METZ ou pour l'IRA de METZ, de façon permanente ou occasionnelle (agents, intervenants, stagiaires, prestataires, ...).

III. Bonnes pratiques

A. Une utilisation raisonnée des ressources

L'IRA de METZ 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.

Accès aux différents postes de travail :

Seuls les agents de l'IRA et assimilés, les attachés stagiaires, les élèves Classe Prépa Talents, la Prépa concours, le dispositif Passerelle et les intervenants sont autorisés à utiliser le matériel informatique de l'IRA.

Les stagiaires de formation continue, si leur stage le nécessite, peuvent être autorisés à utiliser du matériel informatique de l'IRA après une demande explicite auprès du ou de la directeur.trice de la formation continue ou du ou de la responsable des systèmes d'information.

Toute autre personne ne peut en aucun cas utiliser du matériel informatique de l'IRA. L'ensemble du personnel de l'IRA doit veiller particulièrement à cette règle d'accès.

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.

B. Un respect des procédures administratives et techniques fixées par l'IRA de Metz

Les procédures administratives portent notamment sur le respect des processus de circulation, de validation et de mise à disposition des informations, définis par l'IRA de Metz pour les échanges internes et externes. Il s'agit par exemple des règles :

- d'utilisation des boîtes aux lettres fonctionnelles et personnelles ;
- d'échanges avec des services de l'État 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 ;
- d'utiliser uniquement les modes d'accès internet autorisés.

IV. 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 ni modifier les périphériques et les logiciels de communication qui lui sont fournis ni installer de nouveaux équipements non agréés, notamment des modems ou tout autre moyen de connexion à un réseau extérieur ou intérieur.

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 (tel un certificat, une 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. Un mot de passe, une carte d'accès ou tout autre dispositif de sécurité ne doit en aucun cas être diffusé, prêté ou utilisé par une autre personne que son titulaire.

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 des systèmes d'information ou à la directrice de l'IRA de Metz.

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 l'IRA de Metz, 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 service ou d'autorisations spécifiques.

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 l'IRA de METZ concernant l'activation et la mise à jour de son logiciel anti-virus ; celles-ci sont fonctions de la configuration matérielle et logicielle dont il dispose (poste fixe, portable...). Toute attaque doit être signalée immédiatement aux Responsables des systèmes d'information.

L'utilisateur doit veiller à ne pas donner suite aux demandes de rediffusion de messages alarmistes ou de suppression des fichiers. Il ne doit pas répondre à une demande « d'ordre improbable ».

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, pose des problèmes spécifiques (vol, connexion aux ressources), son utilisateur se conformera aux règles spécifiques édictées par le responsable des systèmes d'information :

- l'utilisation d'un gestionnaire de mot de passe est obligatoire ;
- aucun mot de passe ne doit être enregistré sur les navigateurs web ;
- tout agent et assimilé est doté d'une clé usb professionnelle, si l'ordinateur fournit n'est pas verrouillé par un mot de passe, l'intégralité des données professionnelles doivent se trouver sur la clé USB chiffrée à l'aide de l'outil Bitlocker ;
- tout poste de travail ou moyen d'accès à des données professionnelles doit être sécurisé par l'emploi d'un mot de passe de 12 caractères alphanumériques minimum comprenant majuscules, minuscules, chiffres et caractère spéciaux (@+, »\$*).
- chaque agent dispose d'un espace de stockage individuel sur réseau local ou espace collaboratif pour assurer la conservation de ses données en cas de perte de la clé USB.

V. 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...).

Il est 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 », « personnel » ou « perso » ou ceux qui sont 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. Les informations à destination du site internet de l'institut doivent suivre le protocole de validation avant diffusion.

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, il doit 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

Interdiction de produire, collecter ou transmettre des données, messages ou œuvres en infraction avec la législation en vigueur (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. Il prend les précautions nécessaires pour certains sites Internet pouvant être régis par des règles juridiques autres que de droit français.

VI. Traitement de contrôle

Tout utilisateur a droit au respect de ses données privées. Toutefois, il doit être conscient que les systèmes informatiques 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 le directeur.trice de l'IRA de Metz peut donner son accord préalable à un contrôle individuel détaillé. L'utilisateur concerné est immédiatement informé par écrit du contrôle.

VII. Application de la charte

A. Mise en œuvre de la charte

La présente charte sera affichée et sera diffusée sur l'intranet de l'IRA, ce qui permettra de garantir que tout utilisateur a le texte à sa disposition. L'ensemble des agents de l'IRA de Metz, les attachés stagiaires, les élèves CPI, ainsi que toute personne devant avoir accès à une ressource informatique seront informés de l'existence de cette charte. Le (la) responsable des systèmes d'information devra veiller à expliquer le contenu du document, notamment à travers des actions de formation.

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

La révision éventuelle de la présente charte fera l'objet d'une information auprès des utilisateurs.

VIII. Contenus illicites

Tout agent et assimilé est tenu de signaler tous contenus illicites impliquant : injures, diffamation, incitation à la haine raciale ou à la discrimination, atteintes aux mineurs, ..., les utilisateurs peuvent être les témoins ou les victimes d'infractions. Ces contenus doivent être signalés à la plate-forme PHAROS (<https://www.internet-signalement.gouv.fr/PharosS1/etape/contenu>).

IX. Cadre légal

L'agent et assimilé, élève, personnel civil en relation avec l'établissement, s'engage, conformément aux articles 121 et 122 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de ses attributions afin de protéger la confidentialité des informations auxquelles il a accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Toute violation de confidentialité inhérente à l'emploi, formation de l'agent et assimilé, élève, personnel civil en relation avec l'établissement, s'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Fait à Metz, le 15 septembre 2022

Le directeur,



Dominique Bemer