MINISTÈRE
DE LA CULTURE

Liberté
Égalité
Fraternité

CHARTE D'UTILISATION DES MOYENS INFORMATIQUES

du ministère de la culture

CHARTE D'UTILISATION DES MOYENS INFORMATIQUES

du ministère de la culture

Cette charte a été soumise pour avis en comité d'hygiène, de sécurité et des conditions de travail ministériel du du 2 mars 2017 et adoptée au comité technique ministériel du 18 avril 2017.

SOMMAIRE

1. OBJET DE LA CHARTE

Les équipements informatiques et les moyens de communication électronique du ministère de la Culture sont une ressource commune dont la sécurité et la disponibilité dépendent de leur bon usage par chaque utilisateur.
L'objet de la présente charte est de fixer des règles d'utilisation afin d'assurer le bon fonctionnement et la sécurité du système d'information dans le cadre de la politique de sécurité des systèmes d'information de l'État[1] et le respect des réglementations en vigueur rappelées en annexe 1. L'utilisation des technologies de l'information et de la communication par les organisations syndicales est quant à elle définie par la décision ministérielle du 26 avril 2017.

2. DOMAINES D'APPLICATION

Ces règles de bon usage s'appliquent à toute personne, quel que soit son statut (titulaire, non titulaire, salarié.e de droit privé, prestataire, intervenant.e externe, stagiaire, apprenti.e…), ci-après dénommée « utilisateur », utilisant les moyens informatiques mis à sa disposition par le ministère dans ses différentes composantes (administration centrale, services déconcentrés, services à compétence nationale, établissements publics administratifs et associations sous tutelle du ministère de la Culture).
Pour chaque service et établissement public du ministère, les modalités d'application de la charte pourront être précisées par décision de l'autorité concernée après avis du comité technique compétent. En particulier, les étudiant.e.s poursuivant des études dans les écoles du ministère ne relevant pas du droit du travail, il convient d'adapter la présente charte autant que de besoin.

Dans ce qui suit, on désigne :
- le ministère dans ses différentes composantes définies ci-avant sous le terme « ministère » ;
- collectivement les moyens informatiques sous le terme de système d'information (SI).

L'annexe 2 définit les mesures techniques spécifiques s'appliquant aux utilisateurs dont les adresses de messagerie professionnelles relèvent du domaine « culture.gouv.fr ».

3. RÈGLES GÉNÉRALES D'UTILISATION

3.1. Droits d'accès aux comptes utilisateurs

L'autorisation d'accès est accordée par l'autorité hiérarchique compétente puis mise en place par la sous-direction des systèmes d'information (SDSI) du ministère ou le service informatique compétent[2] L'autorisation d'accès se traduit notamment par :

- une dotation en équipements informatiques pour les utilisateurs disposant d'une station de travail personnelle appartenant à l'administration et restant sous sa responsabilité ;
- l'attribution à l'utilisateur de moyens d'identification et d'authentification (exemple : identifiant, mot de passe et carte à puce) et de droits d'accès ;
- une formation adaptée et/ou une documentation lui permettant d'utiliser correctement le SI.

Le droit d'accès au SI est personnel. Cet accès est limité aux activités autorisées par le ministère. Une utilisation à titre personnel est tolérée dans les limites raisonnables et dans la mesure où elle est compatible avec l'activité du service. Il est interdit à tout utilisateur de se servir des ressources du ministère pour des activités contraires à la loi.

Dans ce cadre, dans le respect de la réglementation relative à l'informatique, aux fichiers et aux libertés, les services informatiques compétents enregistrent et peuvent analyser les traces de connexions au SI. Ces traces sont conservées pendant douze mois courant à compter de leur enregistrement avant d'être détruites, conformément à la réglementation en vigueur.

Les tentatives répétées de connexion à des sites internet interdits sont identifiées et signalées à l'utilisateur par les services informatiques compétents. Après cet avertissement, et dans le cas où l'utilisateur réitère ses tentatives de connexion interdites, l'administration peut décider la fermeture de l'accès à internet de l'utilisateur, pour une durée qu'il lui appartient de déterminer.

3.2. Sensibilité des informations manipulées

L'utilisateur est avisé que les documents et informations qu'il produit ou consulte sous forme numérique peuvent être sensibles. Ce caractère est lié soit à la confidentialité des informations (données personnelles par exemple), mais aussi au fait qu'elles peuvent nécessiter des précautions pour ne pas être perdues ou simplement altérées (archives à valeur probantes par exemple).

1 - La Politique de Sécurité des Systèmes d'Information de l'État (PSSIE) est consultable sur le site de l'ANSSI.
2 - Tout service qui a des responsabilités sur une partie du système d'information d'une entité du ministère.

3.3. Conditions de confidentialité

Il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs sans leur accord, quand bien même ceux-ci ne les auraient pas explicitement protégées par une mention « personnel » ou « privé ». Les administrateurs systèmes et réseaux, qui, par la nature de leurs missions, sont susceptibles d'avoir accès à des informations d'autres utilisateurs, sont soumis au secret professionnel, dans le respect des textes en vigueurs, notamment des articles du code pénal visés en annexe 1.

Afin que la continuité du service public puisse être assurée, en références à la Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés et à l'arrêt de la cour de cassation n°843 F-D, Union mutuelle solidarité c/ Clain, du 18 mars 2003, l'accès au poste informatique d'un utilisateur absent est autorisé dans les conditions suivantes :

3.3.1 Cas où l'utilisateur absent a donné son mot de passe à un « tiers de confiance »

L'utilisateur désigne lui-même, s'il le souhaite, un tiers de confiance et en informe sa hiérarchie par écrit. Dans ce cas, seul le tiers de confiance pourra avoir accès au poste informatique de l'utilisateur absent.

3.3.2 Cas où l'utilisateur absent n'a pas donné son mot de passe à un « tiers de confiance » ou que le « tiers de confiance » n'est pas joignable.

Les informations détenues par l'utilisateur ne peuvent être obtenues que par l'accès physique au poste informatique. Si l'utilisateur absent n'est pas joignable, une personne du support informatique peut alors accéder au poste informatique de l'utilisateur absent, en présence et sur ordre écrit d'une personne du service ayant autorité sur l'utilisateur absent.

Dans tous les cas, il est rappelé que les informations enregistrées sur le poste informatique d'un utilisateur sont supposées être des données de nature professionnelle, sauf si celles-ci portent clairement la mention « personnel » ou « privé ». Dans ce dernier cas, les informations ne sauraient être portées à la connaissance du ministère en l'absence de l'intéressé.

Il est rappelé que les personnes en charge du support informatique ont l'interdiction de communiquer les identifiants et mots de passe des autres utilisateurs.

3.4. Traitements automatisés de données à caractère personnel

Si, dans l'accomplissement de ses missions, l'utilisateur est amené à constituer un traitement automatisé de données à caractère personnel au

sens de l'article 2 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, il doit au préalable déterminer, en fonction de la nature des données, à quel régime d'autorisation auprès de la CNIL ce traitement est soumis. Pour ce faire, il peut solliciter un avis juridique auprès de la sous-direction des affaires juridiques du ministère ou du service juridique dont il relève.

3.5. Préservation de l'intégrité des informations

L'utilisateur ne doit pas :

- modifier ou détruire d'autres informations que celles dont il est gestionnaire. En particulier, il lui est interdit de modifier le ou les fichiers contenant des informations comptables ou d'identification ;
- faire disparaître ni altérer les informations dont il est gestionnaire et dont la suppression ou la modification pourrait avoir des conséquences dommageables pour le ministère.

L'utilisateur doit :

- veiller à la sécurité des supports amovibles (clés USB, disques externes fournis par l'administration…), notamment en les conservant en lieu sûr ;
- sauvegarder régulièrement les informations dont il est gestionnaire ;
- privilégier le stockage de ses documents sur des espaces réseau (« ressources partagées », « espaces collaboratifs »…), qui font l'objet de sauvegardes périodiques ;
- immédiatement déclarer la perte ou le vol de matériel informatique auprès de sa hiérarchie et du service informatique responsable du matériel.

3.6. Préservation de l'intégrité des systèmes

L'utilisateur a l'interdiction de modifier le comportement et les paramètres des matériels et logiciels qui sont mis à sa disposition, notamment au sein du ministère où la connexion d'un équipement non fourni par l'administration n'est pas autorisée.

Le ministère filtre les messages transitant par son système de messagerie et peut bloquer ou rejeter un message sur différents critères comme l'émetteur, la machine émettrice, la non-conformité du message aux normes de messagerie, l'impossibilité de vérifier l'innocuité du message et la présence de virus.

Chaque poste de travail est équipé d'un antivirus.

3.7. Respect du droit de la propriété intellectuelle

3.7.1 Protection des logiciels

Le code de la propriété intellectuelle protège en tant qu'« œuvres de l'esprit » les créations de forme originales, parmi lesquelles figurent les logiciels. L'utilisateur s'engage à respecter les licences d'utilisation de tout logiciel mis à sa disposition. À ce titre, il a l'interdiction d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues au II. de l'article L. 122-6-1 du code de la propriété intellectuelle.

3.7.2 Protection des œuvres autres que les logiciels

Le code de la propriété intellectuelle protège également les autres œuvres que sont notamment les textes, les images, les vidéos, ou les musiques[3].
L'exploitation d'œuvres protégées, par reproduction ou communication au public, est soumise à l'autorisation du titulaire du droit d'auteur, sauf mention explicite contraire ou lorsqu'une exception trouve à s'appliquer[4]. Ce principe est constant, que la mention de la protection soit explicite (notamment par l'apposition d'une mention telle que « Toute reproduction ou représentation totale ou partielle sans autorisation est interdite », « Copyright » ou « © ») ou non.

3.7.3 Protection des bases de données

Indépendamment des œuvres qu'elles peuvent contenir, les bases de données bénéficient d'un régime juridique qui leur est propre. Le code de la propriété intellectuelle prévoit notamment que l'extraction de la totalité ou d'une partie substantielle du contenu d'une base de données, ainsi que sa réutilisation par mise à disposition du public, sont soumises à l'autorisation de son producteur[5]. De même qu'en matière de droit d'auteur, l'accomplissement de tels actes sans autorisation est sanctionné.

3.8. Droit à la déconnexion

Le droit à la déconnexion a été introduit par la loi n° 2016-1088 du 8 août 2016 au 7° de l'article L. 2242-8 du code du travail, lequel prévoit que la négociation annuelle sur l'égalité professionnelle entre les femmes et les hommes et la qualité de vie au travail porte notamment sur « les modalités du plein exercice par le salarié de son droit à la déconnexion et la mise en place par l'entreprise de dispositifs de régulation de l'utilisation des outils numériques, en vue d'assurer le respect des temps de repos et de congé ainsi que de la vie professionnelle et familiale. À défaut d'accord, l'employeur élabore une charte, après avis du comité d'entreprise ou, à défaut, des délégués du personnel. Cette charte définit ces modalités de l'exercice du droit à la

3 - Article L. 112-2
4 - Articles L. 122-1 à L. 122-5
5 - Article L. 342-1

déconnexion et prévoit en outre la mise en œuvre, à destination des salariés et du personnel d'encadrement et de direction, d'actions de formation et de sensibilisation à un usage raisonnable des outils numériques. »

Ce droit à la déconnexion est applicable aux employeurs de droit privé ainsi qu'à leurs salariés, aux établissements publics à caractère industriel et commercial et aux établissements publics à caractère administratifs lorsqu'ils emploient du personnel dans les conditions du droit privé (article L. 2211-1 du code du travail).

Au sein du ministère de la Culture, les agent.e.s publics doivent pouvoir bénéficier de conditions de travail leur garantissant une qualité de vie satisfaisante dans le cadre de l'utilisation des équipements informatiques et des moyens de communication électronique fournis par le ministère. Le ministère de la Culture travaillera sur les conditions d'exercice de cette garantie pour ses personnels dans le courant de l'année 2017.

À cet effet, la Charte sur les usages de la messagerie a été diffusée en janvier 2014 par le ministère à l'ensemble des agent.e.s et est disponible sur l'intranet Sémaphore. Cette Charte préconise des conseils et recommandations permettant de préserver la qualité des conditions de travail des agent.e.s.

4. RÈGLES D'UTILISATION DE LA MESSAGERIE ET PUBLICATION SUR DES SITES INTERNET, INTRANET, MÉDIAS SOCIAUX

L'utilisation des outils informatiques est notamment encadrée par les droits et obligations des agents publics issus du statut de la fonction publique. Ainsi tout agent.e du ministère, titulaire ou non, est tenu au secret professionnel. Il doit faire preuve de mesure et de discrétion lorsqu'il ou elle s'exprime par l'intermédiaire des outils de communication. Les stagiaires, les apprenti.e.s, les prestataires et autres intervenant.e.s externes au ministère ont la même obligation de discrétion, comme précisé dans les contrats et conventions qui les lient avec celui-ci. Ils ou elles sont – ainsi que les salarié.e.s de droit privé – également soumis à une obligation de loyauté et de secret professionnel[6]

6 - Article L. 1222-1 du code du travail

De plus, l'utilisateur doit s'abstenir de publier des messages contraires à l'ordre public, diffamatoires, racistes, xénophobes, portant atteinte à la décence ou constituant une diffusion de fausses informations. Il doit prendre toutes dispositions pour consulter, reproduire ou transmettre de manière licite les données ou œuvres protégées par des droits d'auteur, sous quelque forme que ce soit (cf. 3.7).
L'utilisateur doit éviter tout usage de nature à perturber l'activité normale des services. L'utilisateur peut se référer au guide des réseaux sociaux diffusé par le ministère à l'ensemble des personnels et disponible sur l'intranet Sémaphore. Il doit aussi se conformer à la charte d'utilisation des courriels du ministère également disponible sur l'intranet Sémaphore[7].

4.1. Messagerie

4.1.1 Usage

La messagerie est destinée principalement à un usage professionnel. Toutefois, la confidentialité des messages personnels est respectée sous réserve du droit de l'administrateur du SI de filtrer les messages et les fichiers, et de prendre les mesures nécessaires si cela est justifié par des besoins de sécurité. Il est conseillé à l'utilisateur de créer un répertoire « personnel » ou « privé » dans sa messagerie afin d'y regrouper ses messages non professionnels.
Le nombre de destinataires d'un message est limité et la diffusion large de messages non professionnels interdite. Afin de garantir le bon fonctionnement de la messagerie, l'utilisateur peut dans ce cas faire appel à différents services :

- utilisation de listes de diffusion, si cette fonctionnalité est proposée par le service informatique local, à des fins professionnelles dès lors qu'un message s'adresse à un nombre important de destinataires (cf. 4.1.3) ;
- demande adressée aux services de communication interne ou externe, dès lors qu'une information de nature à intéresser les utilisateurs du ministère ou le public est à diffuser largement. Les services concernés décident alors du mode de diffusion approprié en concertation avec le demandeur.

4.1.2 Gestion d'une boîte aux lettres fonctionnelle

Une boîte aux lettres fonctionnelle est une boîte aux lettres générique, correspondant à un besoin temporaire, à une fonction, un service, une unité ou à une ressource du ministère. Les messages envoyés à cette adresse sont accessibles par une ou plusieurs personnes.
L'utilisation partagée d'une boîte aux lettres fonctionnelle par plusieurs utilisateurs est la bonne pratique à observer pour assurer la continuité de service. La méthode de travail doit dans ce cas être adaptée pour savoir qui consulte en priorité et comment notamment tous les utilisateurs sont informés qu'une réponse a été envoyée.

7 - Sémaphore > Vie pratique > Mes dossiers au quotidien > Gérer ma messagerie

4.1.3 Diffusion des messages via des listes de diffusion

L'envoi des messages est limité aux destinataires réellement intéressés ou concernés. Au-delà du nombre maximum d'adresses de destination possible d'un message indiqué dans les mesures techniques spécifiques, des listes de diffusion constituées pour un groupe de personnes partageant un même objectif professionnel peuvent être utilisées par un membre de ce groupe et doivent être privilégiées[8]. Les non-membres doivent passer par l'intermédiaire des gestionnaires de ces listes.

La création de ces listes est soumise à un accord hiérarchique. Chaque liste est sous la responsabilité de la personne qui en a demandée la création (dite propriétaire). Elle peut être gérée par un ou plusieurs utilisateurs. Elle peut être modérée : le(s) utilisateur(s) modérateur(s) est (sont) alors chargé(s) de valider les messages avant diffusion. L'usage de ces listes est, selon les cas, libre ou réservé aux membres de la liste.

Ces listes offrent aux utilisateurs de la messagerie la possibilité de s'abonner et de se désabonner à l'exception des listes générales, à caractère structurel ou géographique. Toute personne déclarée dans l'annuaire ministériel, accessible depuis Sémaphore, y est en effet abonnée d'office et ne peut s'en désabonner.

L'usage des listes générales de diffusion est réservé à l'administration. Seuls les utilisateurs habilités par leur hiérarchie peuvent utiliser ces listes en raison de l'urgence ou d'absence de publication adaptée sur un portail intranet ou plus généralement sur un site web.

4.1.4 Pièces jointes et format d'échange des documents bureautiques

L'adjonction en pièce jointe d'un fichier exécutable1 (dont l'extension peut notamment être .com, .bat, .lnk, .dll, .exe, .vbs, .js) est interdite. Il est également déconseillé d'ouvrir les pièces jointes dont le format est inconnu ou dont l'extension est multiple (exemple : .truc.jpg.vbs).

Pour l'envoi et la réception, les documents bureautiques de type traitement de texte, tableur ou présentation, destinés à être modifiés doivent par principe être établis au format OpenDocument (.ods, .odt et .odp). Les documents n'ayant pas vocation à être modifiés, quel que soit le destinataire, doivent être convertis et transmis au format .pdf.

Par exception, les documents bureautiques destinés à être modifiés par plusieurs utilisateurs dont l'un ne dispose que de la seule suite bureautique Microsoft Office doivent être établis au format par défaut de Microsoft Office (.docx, .xlsx et .pptx). Conformément aux règles interministérielles en vigueur, notamment l'arrêté du 20 avril 2016 portant approbation du

8 - Sous réserve que cette fonctionnalité soit proposée par le service informatique.
9 - Exécutable : fichier informatique contenant un programme et identifié par le système d'exploitation en tant que tel.
10 - JORF n°0095 du 22 avril 2016.

référentiel général d'interopérabilité2, les anciens formats propriétaires de Microsoft, .doc, .xls et .ppt, ne doivent plus, par principe, être utilisés. En vue de l'archivage potentiel du document, une copie du document final devra alors être établi au format OpenDocument (.ods, .odt et .odp), ce formant garantissant dans le temps son accès.
Si l'ensemble des destinataires disposent des suites bureautiques LibreOffice et Microsoft Office, le format retenu par l'initiateur du document ne doit pas être modifié, tant que le document est en construction, pour éviter les problèmes de conversion des outils actuels.

4.1.5 Taille des messages

Lorsque la taille d'un message (en-tête, corps et pièces jointes) est supérieure à la limite autorisée (voir annexe 2 pour le domaine culture.gouv.fr), celui-ci n'est pas émis. L'émetteur est informé du rejet du message. La transmission des documents doit dans ce cas s'opérer via le service de transfert de fichiers Zephyrin[11] (transfert ponctuel) ou un espace collaboratif mis à disposition par l'administration.

4.1.6 Intégrité des messages

Il est interdit de retransmettre un message après l'avoir modifié, lui ou une de ses pièces jointes, sans mentionner explicitement qu'il y a eu des modifications.

4.2. Responsabilité

En matière commerciale comme en matière administrative, le principe est celui de la liberté de la preuve qui peut être apportée par tous moyens. Un message électronique identifié par une adresse en @culture.gouv.fr ou l'adresse d'un établissement sous tutelle du ministère peut donc constituer une preuve susceptible d'engager la responsabilité de l'administration et de son auteur.

4.3. Publication sur des sites internet, intranet, médias sociaux

Tout utilisateur doit, sur les médias sociaux auxquels il a accès au sein du ministère ou en dehors :

- doit se conformer à ses obligations professionnelles lorsqu'il contribue à des forums ou des médias sociaux publics ou lorsqu'il relaie des contenus publiés sur les sites ou comptes officiels du ministère ;
- faire preuve de courtoisie à l'égard de ses interlocuteurs sur les réseaux sociaux et les forums de discussion.

De plus, seules les personnes officiellement désignées par leur hiérarchie possèdent l'autorisation de s'exprimer au nom du ministère sur les sites internet, le portail intranet et les comptes officiels ouverts en tant que moyens de communication sur les médias sociaux[12].
Les utilisateurs pourront utilement se reporter au guide des réseaux sociaux publié par le ministère.

5. SÉCURITÉ

5.1. Mot de passe et accès au poste de travail

L'utilisateur doit veiller à la confidentialité de ses mots de passe. Il ne doit pas stocker de mots de passe en clair sur son poste. Il doit choisir des mots de passe non évidents et les renouveler avec une fréquence raisonnable.
L'utilisateur ne doit pas quitter son poste de travail en laissant accessible une session en cours et doit toujours se déconnecter ou utiliser un écran de veille protégé par mot de passe.

5.2. Messagerie

Certains courriels malveillants peuvent véhiculer des liens ou pièces jointes piégés. Les utilisateurs ne doivent pas ouvrir des messages électroniques de provenance inconnue, d'apparence inhabituelle ou frauduleuse.

6. MISE EN ŒUVRE, COMMUNICATION AUX UTILISATEURS ET SUIVI DE LA CHARTE

La présente charte a fait l'objet d'une concertation avec les organisations syndicales représentatives. Elle a été soumise pour avis au comité d'hygiène, de sécurité et des conditions de travail ministériel du 2 mars 2017 et au comité technique ministériel du 18 avril 2017. Elle rentre en application le lendemain de sa publication au Bulletin Officiel du ministère de la Culture et est accessible sur le portail intranet du ministère. Elle est communiquée à l'ensemble des utilisateurs et leur est opposable. En fonction des évolutions techniques, législatives ou réglementaires, elle pourra être révisée.

11 - ou un service équivalent.
12 - Les médias sociaux comprennent, de façon non exhaustive, les services Facebook, Twitter, Dailymotion, les blogs, les forums de discussions, les réseaux sociaux professionnels et les plate-formes de partage d'image ou de vidéos.

ANNEXE 1 : PRINCIPAUX TEXTES APPLICABLES

- Code des postes et des communications électroniques, notamment ses articles L.34-1 et R.10-13 (protection de la vie privée des utilisateurs de réseaux et services de communications électroniques)
- Code civil, art. 9 (respect dû à la vie privée)
- Code pénal, notamment art. 226-13 à 226-14 (atteinte 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), 432-9 (atteinte au secret des correspondances par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public)
- Code de la propriété intellectuelle, notamment l'article L.122-6-1, alinéa II (copie de sauvegarde)
- Code du travail, notamment l'article L1222-1
- Loi du 29 juillet 1881 sur la liberté de la presse
- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés
- Loi n° 83-634 du 13 juillet 1983 modifiée portant droits et obligations des fonctionnaires, notamment art. 6 (liberté d'opinion), 8 (droit syndical), 26 et 27 (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'État
- Loi n° 2004-575 du 21 juin 2004 modifiée relative à la confiance dans l'économie numérique, notamment son article 6 (identification des personnes utilisant un moyen de communication électronique mis à leur disposition)
- Loi n°2016-483 du 20 avril 2016 relative à la déontologie et aux droits et obligations des fonctionnaires
- Décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

ANNEXE 2 : MESURES TECHNIQUES SPÉCIFIQUES

S'APPLIQUANT AUX UTILISATEURS DONT LES ADRESSES DE MESSAGERIE PROFESSIONNELLES RELÈVENT DU DOMAINE « CULTURE.GOUV.FR »

La charte d'utilisation des courriels du ministère est disponible sur l'intranet Sémaphore (Vie pratique > Mes dossiers au quotidien > Gérer ma messagerie) et est annexée à la présente charte.
Les recommandations en matière de sécurité du système d'information sont publiées sur l'intranet Sémaphore (Vie pratique > Mon informatique > Conseils et sécurité).

1. Messagerie

- nombre maximal d'adresses de destination d'un message (hors liste de diffusion) : 100 ;
- taille maximale des messages (en-tête, corps et pièces jointes) : 8 Mo ;
- les listes de diffusion, listes Sympa créées au sein du ministère, sont consultables sur https://sympa.culture.fr/sympa. Au-delà de 30 destinataires, ce mode de diffusion doit être privilégié ;
- le service de transfert de fichiers : http://zephyrin.culture.fr/ en interne ou http://zephyrin.ext.culture.fr en externe, ou encore ou https://zephyrin2.culture.fr/ tant en interne qu'en externe permet aux utilisateurs de déposer et recevoir des fichiers volumineux pour être envoyés par messagerie électronique.

2. Réseaux

- L'accès à certains services internet (messagerie instantanée ou IRC[1]) est interdit.
- Le réseau du ministère étant connecté au réseau interministériel de l'État (RIE), toute compromission du réseau du ministère peut faciliter l'attaque de réseaux sensibles. Seul le haut fonctionnaire de défense et de sécurité peut, s'il le juge utile, prendre l'attache du secrétaire général de la défense nationale pour demander des dérogations éventuelles aux règles liées à la connexion au RIE.

1 - L'IRC (Internet Relay Chat, ou, en français, discussion relayée par internet) est un protocole de communication textuelle sur internet. Il sert à la communication instantanée principalement sous la forme de discussions en groupe par l'intermédiaire de canaux de discussion, mais peut aussi être utilisé pour de la communication de un à un. Il peut par ailleurs être utilisé pour faire du transfert de fichier.

- Les matériels fournis aux utilisateurs sont conçus et paramétrés pour être utilisés au sein du ministère, en particulier le poste de travail standard qui ne peut être connecté qu'au réseau du ministère de manière filaire. L'utilisateur ne doit en aucun cas utiliser un autre type de connexion.
Pour les matériels sécurisés ayant vocation à être utilisés en dehors du ministère, les conditions d'utilisation sont soumises à des règles spécifiques devant être respectées par l'utilisateur. Seuls, ces matériels sont en effet paramétrés soit pour se connecter au réseau du ministère, soit aux réseaux externes, soit les deux. Tous les types de connexion sont concernés : ADSL, câble réseau, Wi-Fi ou tout autre moyen. Tout autre besoin doit faire l'objet d'une demande de dérogation écrite.
- Les catégories de sites autorisés ou interdits sur les postes de travail de l'administration centrale sont consultables sur http://pandore.culture.fr/terms.php.

3. Règles de sécurité

3.1. Mot de passe

Il est demandé de :
- choisir un mot de passe non évident[2] ; de 10 caractères au minimum, composé d'au moins une majuscule, un chiffre et un caractère spécial (* ! ou # par exemple) ;
- renouveler ses mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles. Le nouveau mot de passe doit être différent des derniers utilisés ;
- ne jamais communiquer son identifiant/mot de passe, que ce soit par téléphone ou via tout autre moyen ;
- ne pas stocker ses mots de passe dans un fichier ou dans son navigateur internet, ni dans son courriel (ex : Thunderbird) ou sur un papier facilement accessible ;
- ne pas réutiliser un mot de passe professionnel dans la sphère privée.

3.2. Messagerie

- ne pas répondre aux messages en masse ou en chaîne des messageries ;
- ne jamais cliquer sur un lien contenu dans un message lorsqu'on a un doute sur son origine ;
- supprimer tout message douteux, même dans la corbeille.

2 - Cf. les recommandations de l'ANSSI sur la sécurité des mots de passe

3.3. Sécurité des équipements mis à disposition

- Ne jamais quitter son poste de travail en laissant accessible une session en cours et toujours se déconnecter ou utiliser un écran de veille protégé par mot de passe. Une mise en veille protégée par mot de passe au bout de 10 minutes d'inactivité est recommandée ;
- ne pas désactiver les mises à jour automatiques (système anti-virus et logiciels) ;
- ne pas faire de sauvegarde sur des serveurs externes au ministère ;
- veiller à protéger contre le vol les équipements mis à disposition ;
- en cas de vol d'un équipement informatique, l'utilisateur doit immédiatement le déclarer auprès de sa hiérarchie et du service responsable du matériel. La personne compétente pour représenter le ministère, accompagnée de l'utilisateur, se rendra ensuite au commissariat afin de déposer plainte pour vol. Une copie du dépôt de plainte sera adressée au service informatique ;
- en cas de perte, l'utilisateur doit signer une déclaration sur l'honneur. Sous couvert de sa hiérarchie, cette déclaration sera adressée au service informatique ;
- en cas d'incident :
    1. noter les éventuels messages d'erreur, les manipulations effectuées et les symptômes constatés ;
    2. informer sans délai le support SI de proximité habituel afin que celui-ci prenne les mesures ad-hoc pour résoudre l'incident. Une saisine tardive rend par ailleurs difficile l'obtention des informations techniques susceptibles d'aider à la résolution ;

Rédaction : Secrétariat général - Graphisme et réalisation : DICOM Mission de la communication interne

ministère de la Culture
secrétariat général

juillet 2020