Conforme à l'original produit,
Début du texte, page suivante.

DIRECTION DES AFFAIRES JURIDIQUES : *sous-direction du droit public et du droit privé ; bureau de l'organisation, de la modernisation et de l'aménagement des structures.*

DÉCISION N° 1216/DEF/SGA portant mise en application de la charte de l'utilisation des ressources humaines.

Du 3 octobre 2007

NOR D E F D 0 7 5 2 4 0 9 S

Références :

1) Loi n° 78-17 du 6 janvier 1978 (BOC, 1979, p. 4161. ; BOEM 111.1.2.2, 160.6.1, 722.3.1) modifiée.
2) Décret n° 99-164 du 8 mars 1999 (JO du 9, p. 3514 ; BOC, p. 1940. ; BOEM 110.4.2.1, 640.2.1, 660.3.1) modifié.
3) Décret n° 2006-497 du 2 mai 2006 (n.i. BO ; JO n° 103 du 3 mai 2006, texte n° 9 ; JO/135/2006. ; BOEM 160.1).
4) Instruction n° 4418/DEF/SEC/DIR/SIC du 25 septembre 2000 (BOC, p. 4343. ; BOEM 160.3).

Pièce(s) Jointe(s) :

Une charte.
Quatre annexes.

Classement dans l'édition méthodique : BOEM 160.8.

Référence de publication : BOC N°33 du 21 décembre 2007, texte 2.

Art. 1er. Au sein des services mentionnés à l'article 2, la charte de l'utilisateur des ressources informatiques ci-jointe est mise en application à compter du 1er novembre 2007.

Art. 2. Les directions, services et organismes placés sous l'autorité du secrétaire général pour l'administration en tant qu'autorité en tant qu'autorité qualifiée, au sens de l'instruction du 25 septembre 2000 susvisée, sont chargés, chacun en ce qui le concerne, de l'application de le présente décision, qui sera publiée au bulletin officiel des armées.

Pour le ministre de la défense et par délégation :

Le secrétaire général pour l'administration,

Christian PIOTRE.

CHARTE DE L'UTILISATEUR DES RESSOURCES INFORMATIQUES

1. OBJET ET CHAMP D'APPLICATION.

Les ressources informatiques, électroniques ou numériques, les intranets (Intradef et Intraced) du ministère de la défense ainsi qu'Internet constituent des outils de travail. L'Intradef est dédié au traitement des informations sensibles non classifiées de défense [Rec901]. L'Intraced est réservé au traitement des informations classifiées de défense [IGI900].

Ces deux systèmes offrent des services de type messagerie, annuaire, documentation ainsi que l'accès aux applications métier.

La présente charte a pour objet d'énoncer les règles d'usage et de sécurité que doit respecter tout utilisateur de ressources informatiques au sein des entités relevant de l'autorité qualifiée secrétariat général pour l'administration (SGA). La liste des organismes concernés figure en annexe.

La charte est communiquée à tout utilisateur. Il y est fait référence dans le règlement intérieur des entités qui en disposent et, en tant que de besoin, dans les marchés ou contrats.

Le non-respect de la charte engage la responsabilité personnelle de l'utilisateur dès lors qu'il est prouvé que les fautes lui sont imputables et l'exposent éventuellement, de manière appropriée et proportionnée au manquement commis, à des sanctions disciplinaires ou pénales.

La présente charte s'applique aux organisations syndicales pour le périmètre relevant du SGA, sous réserve des dispositions de la charte ministérielle sur l'utilisation des technologies de l'information et de la communication par les organisations syndicales et des nécessités liées à l'exercice de la liberté syndicale.

2. DÉFINITIONS.

S'appliquent aux fins de la présente charte les définitions suivantes :

a) **autorité qualifiée :** désigne une autorité responsable de la sécurité des systèmes d'information dans les administrations centrales et les services déconcentrés de l'État, dans les établissements publics placés sous l'autorité d'un ministre ainsi que les organismes et établissements placés sous sa tutelle [IGI1300] ;

b) **entités relevant de l'autorité qualifiée SGA :** désigne les directions, services et organismes placés sous l'autorité du secrétaire général pour l'administration en tant qu'autorité qualifiée instituée par l'article 4.2.1 de l'[IM 4418] ;

c) **politique de sécurité des systèmes d'information** (**PSSI) :** désigne l'ensemble formalisé des éléments stratégiques, des directives, procédures, chartes, codes de conduite, règles organisationnelles et techniques ayant pour objectif la protection du(des) système(s) d'information (SI) d'un organisme ;

d) **système d'information :** le système d'information organise et structure l'information nécessaire à la décision, à la gestion et à la production d'un organisme en prenant en compte ses règles de gestion ; il intègre les fonctions de génération, de mémorisation, de communication, de diffusion et de transformation de l'information; il comprend également les moyens matériels et humains nécessaires au recueil et à l'utilisation de l'information ;

e) **ressources informatiques** ou **ressources :** désigne globalement dans un souci de simplification, les informations (documents ou messages électroniques, fichiers), les systèmes d'information, les systèmes informatiques, électroniques ou numériques des entités relevant de l'autorité qualifiée SGA et par extension les systèmes accessibles directement ou non, ainsi que les matériels mis à disposition par le SGA.

3. ACTEURS CONCERNÉS.

3.1. **L'utilisateur.**

Est dénommé utilisateur, tout personnel, quel que soit son statut (fonctionnaire, militaire, agent sur contrat, stagiaire, personnel d'un prestataire, ouvrier d'État, etc.) - qui compte tenu de son habilitation ou de son besoin d'en connaître, dispose d'une autorisation d'accès aux ressources informatiques.

On distingue en outre, un type d'utilisateur particulier résultant de l'usage spécifique des ressources par les organisations syndicales dans le cadre de la charte ministérielle sur l'utilisation des technologies de l'information et de la communication par les organisations syndicales.

L'utilisateur veille au respect de la législation et de la réglementation en vigueur ainsi qu'aux dispositions énoncées par la présente charte. Il est responsable de l'usage et de la sécurité :

- des autorisations d'accès et des droits qui lui sont attribués sur les ressources informatiques ;

- des équipements qui lui ont été affectés ;

- des documents, messages électroniques, fichiers ou supports d'information qu'il peut produire et diffuser grâce aux moyens mis à sa disposition.

3.2. **L'administrateur de système.**

Chaque système (matériel, logiciel, application, ...) ou réseau est géré par au moins un utilisateur privilégié dénommé « administrateur de système » ou « administrateur ». Soumis aux droits et devoirs de tout utilisateur, l'administrateur fait l'objet d'une procédure d'habilitation au niveau requis par la sensibilité du système géré.

L'administrateur est responsable du fonctionnement (qualité de service) et de la sécurité du système dont il a la charge. Pour cela, il dispose des droits et privilèges nécessaires et suffisants pour assurer l'administration et la sécurité du système sous son contrôle.

[Pour en savoir plus] : ANNEXE I. DROITS ET DEVOIRS DE L'ADMINISTRATEUR DE SYSTÈME.

4. PRINCIPES GÉNÉRAUX.

4.1. **Obligations des utilisateurs.**

L'ensemble du personnel du ministère de la défense est soumis à une obligation générale et permanente de discrétion professionnelle, voire de confidentialité. Les utilisateurs ne doivent pas divulguer les informations qu'ils sont 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.

4.2. **Autorisation d'accès aux ressources.**

L'utilisateur doit exécuter les tâches qui lui sont confiées exclusivement avec les moyens techniques mis à sa disposition par l'autorité qualifiée SGA.

Nota : L'usage, notamment la connexion aux réseaux et systèmes du ministère de la défense, d'un équipement « personnel » (ordinateur portable, assistant numérique personnel, etc.) même pour réaliser des tâches relevant de l'activité professionnelle est interdit(1).

L'accès aux ressources informatiques nécessite une autorisation accordée par l'autorité hiérarchique de l'utilisateur ; la mise en place est effectuée par l'administrateur du système concerné, conformément à la politique de sécurité applicable. Toute autorisation d'accès est personnelle, incessible et peut être retirée à tout moment.

Ne sont accordés à l'utilisateur que les droits nécessaires à l'exercice d'une mission précise, compte tenu de son habilitation et de son besoin d'en connaître. L'autorisation d'accès se traduit par l'attribution de dispositifs(2) permettant de gérer et de contrôler l'identité numérique(3) de l'utilisateur ainsi que les accès concédés aux ressources.

4.3. **Communication de la charte à l'utilisateur.**

À l'occasion de la mise en œuvre de l'autorisation d'accès aux ressources l'administrateur remet à l'utilisateur la charte au format papier ou l'invite à consulter la version numérique de la charte sur l'Intradef.

4.4. **Usage des ressources.**

Les ressources sont mises à disposition d'un utilisateur à titre professionnel c'est-à-dire pour réaliser les tâches qui sont confiées dans le cadre de ses attributions. Les règles d'usage et de sécurité ne peuvent être modifiées pour satisfaire le besoin particulier d'un utilisateur. Les règles spécifiques applicables à certains systèmes sont détaillées dans les documents *ad-hoc*.

L'usage des ressources pour toute activité privée, humanitaire, associative, politique est interdit, à défaut d'autorisation accordée par l'autorité compétente. L'usage des ressources par les organisations syndicales est défini par la charte ministérielle sur l'utilisation des technologies de l'information et de la communication par les organisations syndicales.

L'usage de moyens professionnels extérieurs au ministère de la défense est soumis à des règles particulières de sécurité.

Un usage à des fins personnelles des ressources est toléré, dans des limites raisonnables, sous réserve de ne pas affecter le trafic normal des communications professionnelles ni la productivité des agents et d'être compatible avec les règles de sécurité définies par l'autorité qualifiée SGA (énoncées *supra*) ou celles requises par les plans de sécurité gouvernementaux (ex : Vigipirate).

Aucune information classifiée de défense ne doit être élaborée, traitée, stockée ou transmise sur l'Intradef ou Internet. Le traitement d'informations classifiées de défense doit s'effectuer sur des systèmes et réseaux spécifiques (ex : Intraced).

4.5. **Droit de propriété sur les ressources.**

Tout équipement mis à la disposition d'un agent (utilisateur) dans le cadre de la relation de travail est la propriété de l'État et ne peut comporter que subsidiairement des informations relevant de la vie privée de l'agent.

Toute information (document, message électronique, fichier) élaborée, traitée, stockée, acheminée par les systèmes d'information ou ressources relevant de l'autorité qualifiée SGA, y compris les copies de sauvegarde, revêtent *a priori* un caractère professionnel et sont la propriété du ministère de la défense, sauf en cas d'indication manifeste du caractère personnel des informations, documents, messages précités.

4.6. **Protection de la vie privée de l'agent sur le lieu de travail.**

Pour respecter l'intimité de la vie privée et les libertés individuelles de tout agent sur son lieu de travail, les informations personnelles(1) d'un agent (utilisateur), doivent être rassemblées par celui-ci dans un dossier numérique spécial nommé « dossier privé». En outre, les messages électroniques sont protégés par les dispositions applicables au secret des correspondances émises par la voie des télécommunications.

Sauf risque ou événement particulier, l'autorité hiérarchique, les personnels en charge de l'administration ou de la sécurité des ressources informatiques ne peuvent ouvrir les fichiers ou messages identifiés par un agent comme personnels (privés) qu'en présence de ce dernier ou celui-ci dûment appelé et averti de la nécessité de l'ouverture ou de la destruction du fichier.

[Pour en savoir plus] : Point 6.1. Dossier privé.

4.7. **Surveillance des accès aux ressources et de leur utilisation.**

Tout utilisateur a droit au respect de l'intimité de sa vie privée et de ses données à caractère personnel (privé). Il doit cependant être conscient que pour des nécessités d'administration de la sécurité et de gestion des ressources, l'utilisation des systèmes, mais aussi les échanges via les réseaux peuvent être analysés et contrôlés dans le respect des exigences légales et réglementaires.

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

4.8. **Obligation de rendre compte de tout incident.**

Tout incident réel ou supposé affectant le fonctionnement ou la sécurité d'une ressource (information, application, serveur, système, réseau) doit être rapporté immédiatement à l'administrateur du système.

4.9. **Responsabilités du maître d'une information.**

Toute information (document, message électronique, fichier) créée ou utilisée au sein des entités relevant de l'autorité qualifiée SGA a un maître ou un responsable identifié. Il s'agit par défaut de son auteur.

Si une information paraît disposer de plusieurs maîtres ou responsables potentiels, il appartient à l'autorité hiérarchique *ad hoc* de désigner comme responsable de cette information celui qui est responsable de son intégrité. Le maître ou le responsable d'une information est chargé :

- de l'attribution d'un niveau de sensibilité (non protégé, sensible non classifié de défense, classifié de défense) approprié à la nature de cette information ;

- de la définition des droits d'accès et d'usage (privilèges) associés à l'information (qui peut y avoir accès et quels en sont les usages autorisés : lecture, modification, suppression, diffusion, etc.) ;

- de la définition des exigences de protection de l'information appropriées au niveau de sensibilité de l'information. En outre, si des règles spécifiques de marquage s'appliquent selon le niveau de sensibilité de l'information, le maître veille à leur respect.

5. CODE DE BONNE CONDUITE.

Une ressource informatique, un outil de communication ne doit pas être utilisé pour envoyer, stocker, publier, diffuser tout contenu :

- à caractère violent ou susceptible de porter atteinte au respect et à la dignité de la personne humaine, à l'égalité entre les hommes et les femmes, à la protection des enfants et des adolescents, notamment par la fabrication, le transport et la diffusion de messages à caractère violent ou pornographique ou de nature à porter atteinte à la dignité humaine ;

- qui encourage à la commission de crimes et délits ;

- qui incite à la consommation de substances interdites ;

- qui provoque ou puisse provoquer la discrimination, la haine, la violence en raison des origines, de l'ethnie ou de la nation ;

- qui s'apparente à une chaîne de messages, à de la publicité non sollicitée ou à un canular ;

- qui soit constitutif de harcèlement sexuel ou moral, diffamatoire, injurieux, obscène, menaçant pour la vie privée d'autrui ou de nature à heurter la sensibilité de certaines personnes ;

- qui induise en erreur d'autres utilisateurs en usurpant le nom, l'adresse mél ou la dénomination sociale d'autres personnes ;

- qui porte atteinte aux droits des tiers comme, sans que cette liste soit limitative, à tout secret de fabrication, secret professionnel, information confidentielle, marque, brevet et d'une manière générale tout droit de propriété industrielle ou intellectuelle ou tout droit portant sur une information ou un contenu protégé ;

- comprenant, sans que cette liste soit limitative, des virus informatiques ou tout autre code ou programme, conçus pour interrompre, détruire ou limiter la fonctionnalité de tout logiciel, système informatique ou moyen de télécommunication ;

- comportant des opinions personnelles susceptibles de porter préjudice aux entités relevant de l'autorité qualifiée SGA ou au ministère de la défense.

Les règles de sécurité qui s'imposent à tout utilisateur sont :

1) Ne pas utiliser d'équipement personnel pour exercer son activité professionnelle ;
2) Ne pas modifier la configuration d'un équipement ou de son poste de travail ;
3) Choisir des mots de passe sûrs, ne pas les divulguer et les changer régulièrement ;
4) Respecter les droits accordés et protéger son poste de travail et ses données ;
5) Respecter la confidentialité des données et des communications ;
6) Verrouiller ou arrêter son poste de travail lorsqu'il est inutilisé ;
7) Éteindre son poste de travail le soir avant de quitter son bureau ;
8) Ne pas tenter de manipulations hasardeuses ou tester les mesures de sécurité ;
9) Être vigilant et rendre compte de toute anomalie ou incident.

L'utilisateur d'un poste de travail portable (PC, assistant numérique, etc.) ne doit pas :

- emmener un équipement contenant des informations sensibles et a fortiori classifiées de défense dans un environnement non sécurisé ;

- laisser son matériel accessible après les heures de travail ;

- laisser son poste de travail portable allumé sans surveillance (ex : dans une chambre d'hôtel, une voiture, un lieu ou un moyen de transport, etc.) ;

- travailler sur des informations sensibles ou classifiées de défense dans des lieux ou dans les transports publics.

[Pour en savoir plus] : ANNEXE II. RÈGLES DE SÉCURITÉ.

6. RÈGLES D'USAGE.

6.1. **Dossier privé.**

Chaque utilisateur peut disposer sur son poste de travail d'un espace de stockage personnel limité à 10 Go, désigné obligatoirement « dossier privé nom patronymique_prénom », pour conserver des informations personnelles (documents, messages, fichiers) et protéger l'intimité de sa vie privée.

L'utilisateur est responsable de l'usage et du contenu de son « dossier privé ». Les règles d'usage et de sécurité du SGA sont applicables à tout « dossier privé ».

Chaque équipement relevant de l'autorité qualifiée SGA est doté des dispositifs appropriés pour assurer la sécurité des informations ; tout dossier privé bénéficie de ces mesures de protection (ex : antivirus). En revanche, aucun « dossier privé » n'est inclus dans les plans de sauvegarde des informations. Lorsqu'un utilisateur quitte ses fonctions il doit supprimer son(ses) dossier(s) privé(s). À défaut, cette opération est réalisée par l'administrateur du système.

L'importation ou l'exportation par l'utilisateur de données personnelles vers un « dossier privé » via un équipement nomade personnel (PC portable, assistant numérique personnel), un support amovible personnel (CD/DVD, clé USB, disque dur externe, etc.), un réseau (Intradef, Internet, etc.) si elle ne peut être interdite pour respecter de l'intimité de la vie privée de tout agent sur son lieu de travail, s'effectue sous sa responsabilité.

En cas, d'atteinte à la sécurité des ressources informatiques, l'utilisateur s'expose à des sanctions disciplinaires ou pénales en fonction du manquement ou de l'infraction constatée.

6.2. **Postes nomades et supports amovibles.**

Tout poste nomade (ordinateur portable, assistant numérique personnel, etc.), support amovible (CD/DVD, clés USB, etc.) mis à disposition d'un utilisateur par l'autorité qualifiée SGA est placé sous la responsabilité du détenteur et doit être utilisé conformément aux règles de sécurité liées à la sensibilité(5) des informations qu'il traite.

Les dispositifs nomades ou amovibles doivent être utilisés dans un environnement de confiance sauf nécessité (mission en France ou à l'étranger), c'est-à-dire ni dans un lieu public ni dans les transports en commun. De plus, ces dispositifs ne doivent pas être laissés sans surveillance dans un environnement non sécurisé (dans un véhicule en stationnement par exemple).

6.3. **Internet.**

Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle et une utilité au regard des fonctions exercées ou des missions à mener.

La navigation sur Internet pour un motif personnel n'est qu'une tolérance qui exige, en outre, que le contenu des sites consultés ne soit pas contraire à la loi, ni ne mette en cause la sécurité, la déontologie ou la réputation du ministère de la défense.

L'accès à certains sites Web peut être bloqué à tout moment et sans avertissement préalable pour des raisons de sécurité ou au motif d'un contenu jugé offensant ou inapproprié.

L'impression d'anonymat des navigations est trompeur puisque, même si l'utilisateur ne donne pas son identité, des données relatives au trafic (traces) peuvent être collectées par les divers équipements techniques utilisés par le ministère ainsi que par des tiers extérieurs. Tout accès à un site Internet par un utilisateur relevant de l'autorité qualifiée SGA est identifié par ce site comme une connexion en provenance du ministère de la défense. Les postes Internet en libre service sont particulièrement concernés par ces usurpations d'identité.

De plus, la consultation de sites Web sur Internet expose l'internaute à divers risques : divulgation d'informations confidentielles, vol de données ou de mots de passe, infection virale, etc. Pour diminuer ces risques, la configuration par défaut des navigateurs (ex : Internet Explorer, Firefox, etc.) est modifiée par l'administrateur de système afin d'inhiber diverses fonctions potentiellement dangereuses des sites Web.

6.4. **Messagerie électronique.**

Les procédures applicables au courrier classique (papier) sont transposables au courrier électronique sous réserve des adaptations nécessaires. Le courrier électronique est régi par des règles de rédaction, circulation, signature, protection, conservation, destruction comme le courrier papier. L'atteinte au secret des

correspondances est une infraction pénale (art. 226-15 al.1, art. 226-15 al.2 et art. 432-9 al.1 du code pénal).

La courtoisie constitue une règle de base dans tous les échanges électroniques. L'utilisateur ne doit jamais écrire un message électronique qu'il s'interdirait d'exprimer oralement ou par un autre moyen (courrier, télécopie, etc.), car un message électronique peut être stocké, réutilisé, exploité à des fins auxquelles l'utilisateur n'aurait pas pensé en le rédigeant ; il peut constituer une preuve ou un commencement de preuve par écrit.

Par défaut, les messages échangés via la messagerie électronique ne sont ni signés ni chiffrés par des dispositifs appropriés. La confidentialité et l'intégrité des messages ne sont donc pas assurées. Envoyer un mél non chiffré équivaut à envoyer une carte postale. En outre, la boîte aux lettres du destinataire peut être renvoyée vers une autre boîte aux lettres. Par ailleurs, un message envoyé sur Internet peut être lu à l'insu de l'expéditeur et du destinataire.

Enfin, il convient de rappeler que, même après la destruction du message, celui-ci peut rester longtemps sur des supports de sauvegarde ou d'autres serveurs.

[Pour en savoir plus] : ANNEXE III. RÈGLES D'USAGE DE LA MESSAGERIE.

6.5. **Forums de discussion.**

Les forums de discussions répondent aux mêmes règles de bon usage que la messagerie électronique. En outre, le sens de la responsabilité de chacun conduit à ne pas se permettre de participer anonymement à ces discussions électroniques.

6.6. **Moyens de chiffrement.**

Seuls les moyens de chiffrement fournis ou autorisés par le ministère sont utilisables.

7. TRAITEMENTS DE CONTRÔLE.

7.1. **Contrôle de la sécurité et de la qualité de service des ressources.**

L'accès et l'utilisation des ressources informatiques relevant de l'autorité qualifiée (AQ) SGA donnent lieu à la collecte de données techniques (une journalisation des événements) conformément aux mesures de sécurité requises par les plans gouvernementaux Vigipirate et Piranet destinés à protéger les systèmes d'information de l'État. Ces données techniques sont désignées sous le vocable de « données des communications électroniques » ou de « traces ».

Les traces permettent de détecter les incidents, de contrôler l'efficacité des règles de sécurité et de surveiller la qualité de service(6) des systèmes. En cas de dysfonctionnement d'un système, d'utilisation non conforme à la présente charte ou d'incident de sécurité, il est possible de reconstituer l'enchaînement des événements, d'imputer les actions effectuées à leurs auteurs et de décider des mesures nécessaires et appropriées.

Concrètement :

1) Toute demande d'accès aux systèmes et réseaux nécessite un contrôle de l'identité numérique (identification et authentification de l'utilisateur), puis une vérification des droits dont il dispose, avant d'autoriser éventuellement un accès.
2) Les équipements sollicités (réseau, serveur, ...) lors d'une transaction enregistrent leur fonctionnement et les opérations réalisées par les utilisateurs (collecte de traces).
3)Les traces sont conservées pendant une durée maximale d'un an avant d'être détruites.
4) Les traces peuvent être utilisées aux fins de recherche, de constatation et de poursuite d'infractions pénales par l'autorité judiciaire.

Ces mesures visent à garantir l'intégrité et la confidentialité des ressources relevant de l'autorité qualifiée SGA et à assurer la protection des utilisateurs aussi bien que celle de l'État.

7.2. **Contrôle de la sécurité du contenu des communications électroniques.**

En complément des moyens de lutte contre les virus ou autres codes malveillants, conformément à la politique de sécurité des systèmes d'information définie par l'autorité qualifiée SGA, des dispositifs chargés de l'examen, de l'analyse, du filtrage des messages électroniques et de celui des pages Web consultées sont mis en oeuvre.

Ce contrôle est réalisé en aveugle par des logiciels appropriés pour ne pas porter atteinte à la vie privée et au secret des correspondances. Il a pour objet d'analyser et éventuellement rejeter les pièces jointes aux messages, les documents ou fichiers téléchargés qui contiendraient un type de contenu non autorisé ou seraient trop volumineux. En résumé, les règles de filtrage instituées peuvent être employées pour éviter :

- toute divulgation d'informations confidentielles vers des destinataires non autorisés ;

- toute atteinte aux droits de la propriété intellectuelle ;

- toute perte de productivité due à une utilisation inappropriée de la messagerie ou de l'Internet ;

- la propagation du courrier électronique non sollicité (lutte contre le spam) ;

- la dégradation des performances en raison d'un trafic improductif sans lien avec le service ;

- la diffusion de contenus choquants ou délictueux.

7.3. **Contrôle des équipements.**

Les données techniques relatives aux ressources relevant de l'autorité qualifiée SGA sont recensées automatiquement par un système approprié. Cet outil permet de :

- tenir à jour un état du parc installé (cartographie des systèmes) ;

- gérer la configuration matérielle et logicielle de chaque équipement ;

- détecter les logiciels qui doivent faire l'objet d'une mise à jour de sécurité ;

- détecter les logiciels non autorisés ou malveillants ;

- télédistribuer les logiciels ou les mises à jour de ces logiciels.

En aucun cas cet outil ne permet un accès au contenu des fichiers.

8. RÉFÉRENCES.

[IGI1300] Instruction générale interministérielle n° 1300/SGDN/SSD/DR du 25 août 2003 (n.i BO)sur la protection des informations concernant la défense nationale et la sûreté de l'état (annexe de l'arrêté du 25 août 2003 relatif à la protection du secret de la défense nationale).

[IGI900] Instruction générale interministérielle n° 900/SGDN/SSD/DR du 20 juillet 1993 (n.i BO) sur la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées.

[Rec901] Recommandation n° 901/DISSI/SCSSI du 2 mars 1994 (n.i BO) pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense.

[IM4418] Instruction ministérielle n° 4418 DEF/SEC.DIR.SIC du 25 septembre 2000 relative à la mise en œuvre de la

sécurité des systèmes d'information au sein du ministère de la défense.

[Lettre 1691] Lettre n° 1691 DEF/SGA du 20 décembre 2005 (n.i BO) relative à l'organisation de la sécurité des systèmes d'information au sein des services relevant de l'autorité qualifiée SGA.

---

(1) La connexion d'équipements ou de supports personnels avec un système d'information du ministère de la défense présente des risques pour la sécurité des systèmes d'information. L'autoriser suppose de pouvoir garantir que la connexion n'affaiblirait pas cet ensemble. Or, il s'avère impossible, techniquement et juridiquement, pour le ministère, de contrôler les répercussions de cette connexion pour ses systèmes d'information, en préservant, quoiqu'il advienne, l'espace personnel réservé sur ce(s) support(s).

(2) Identifiants, mots de passe, cartes à puce, clés USB (Universal Serial Bus), certificats électroniques, etc.

(3) L'identité numérique de l'utilisateur est déterminée par les attributs suivants : nom, prénom, etc.

(4) Documents, messages, fichiers à caractère personnel.

(5) Non-protégé, sensible non classifié de défense (ex: confidentiel personnel, confidentiel industrie) ou classifié de défense (ex : confidentiel défense).

(6) La qualité de service est liée notamment au niveau de disponibilité, d'intégrité et de confidentialité du système.

ANNEXE I.

DROITS ET DEVOIRS DE L'ADMINISTRATEUR DE SYSTÈME.

L'administrateur est responsable du fonctionnement (qualité de service) et de la sécurité du système (serveur, poste de travail, équipement, application, réseau) dont il a la charge. Il dispose à cet effet des droits et privilèges nécessaires et suffisants pour assurer l'administration et la sécurité du système sous son contrôle, conformément à la politique de sécurité définie par l'officier de sécurité des systèmes d'information (OSSI) ou le responsable de la sécurité des systèmes d'information (RSSI) dont le système relève.

L'administrateur s'engage à prendre en temps opportun toutes les mesures possibles, appropriées, nécessaires et suffisantes pour maintenir la qualité de service et la sécurité du système. Il appartient à l'administrateur :

- d'appliquer les avis et recommandations diffusés par le CALID(7) ou le CERTA(8) ;

- d'appliquer après validation interne ou par le CALID les correctifs de sécurité et de mettre à jour les logiciels pour corriger les vulnérabilités du système ;

- de modifier le système dans le sens d'une meilleure qualité de service et d'une meilleure sécurité tout en respectant la politique de sécurité applicable. Ces modifications doivent s'opérer dans l'intérêt des utilisateurs. Exemples :

  - modifier la priorité ou stopper une tâche utilisateur (avec ou sans préavis) si celle-ci entraîne une utilisation excessive de ressources d'un serveur ou d'un réseau ;

  - déconnecter un utilisateur en cas de comportement dangereux ;

- de procéder, en concertation avec l'officier de sécurité des systèmes d'information du SGA ou les services appropriés du ministère de la défense ou ceux de l'État, aux investigations nécessaires au diagnostic de tout incident.

Les responsabilités d'administrateur doivent être exercées dans le souci constant de l'intérêt du service, de la sécurité du système et de l'intérêt de l'usager. Aussi, l'administrateur a le devoir :

- de préserver la confidentialité des informations des utilisateurs qu'il est amené à connaître dans l'exercice de sa fonction en limitant l'accès à ces informations au strict nécessaire ; sauf risque ou événement particulier, l'administrateur ne peut ouvrir les fichiers ou messages identifiés par un agent comme personnels qu'en présence de ce dernier ou celui-ci dûment appelé ;

- d'informer les utilisateurs des interruptions de service du système susceptibles d'occasionner une gêne ou une dégradation des performances ; l'information communiquée doit être pertinente, à jour et appropriée ;

- de minimiser ces interruptions et de choisir, si possible, les dates et les heures les moins gênantes pour les utilisateurs.

---

(7) Centre d'Analyse en Lutte Informatique Défensive.

(8) CERTA : Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques.

ANNEXE II.
RÈGLES DE SÉCURITÉ.

1. NE PAS UTILISER D'ÉQUIPEMENT PERSONNEL POUR EXERCER SON ACTIVITÉ PROFESSIONNELLE.

Vous devez pour réaliser les tâches qui vous sont confiées dans le cadre de votre activité professionnelle utiliser uniquement les moyens techniques mis à votre disposition par le ministère de la défense.

L'usage, notamment la connexion aux réseaux et systèmes du ministère de la défense, d'un équipement « personnel » (ordinateur portable, assistant numérique personnel, etc.) pour réaliser des tâches relevant de l'activité professionnelle est interdit.

2. NE PAS MODIFIER LA CONFIGURATION D'UN ÉQUIPEMENT OU DE SON POSTE DE TRAVAIL.

Vous ne devez pas modifier la configuration d'un équipement informatique ou télécoms, ni connecter ou déconnecter des équipements d'un réseau (quels qu'ils soient) sans l'intervention de spécialistes habilités.

Il est strictement interdit de modifier le paramétrage des matériels, des logiciels mis en place ou mis à votre disposition, voire d'ajouter, de supprimer des matériels ou des logiciels du poste de travail.

Vous devez respecter le code de la propriété intellectuelle et commerciale. Il est interdit de copier des logiciels sauf s'ils sont libres de droit, d'installer ou d'utiliser des copies illicites de logiciels. La responsabilité de l'utilisateur est engagée même s'il n'est pas l'auteur de la copie illicite.

3. CHOISIR DES MOTS DE PASSE SÛRS, NE PAS LES DIVULGUER ET LES CHANGER RÉGULIÈREMENT.

L'utilisateur est responsable de la gestion de ses mots de passe. Il doit toujours mettre un mot de passe quand le système le lui propose. En matière de mot de passe, les règles à observer sont les suivantes :

1) Tout mot de passe doit être associé à un identifiant unique (chaque administrateur doit utiliser un identifiant qui lui est propre) ;
2) Un même mot de passe ne doit pas être associé à plusieurs systèmes ;
3)Tout mot de passe est créé, puis géré sous la responsabilité de l'utilisateur ; lorsqu'un mot de passe est attribué par le service informatique, l'utilisateur doit immédiatement le remplacer
4) Tout mot de passe doit être composé d'au moins huit caractères alphanumériques (minuscules, majuscules, chiffres mais pas de caractères accentués) dont au minimum deux caractères spéciaux (- * =] ...), de sorte que le mot de passe résultant n'existe dans aucun dictionnaire disponible sur Internet ;
5) Un mot de passe ne doit pas être conservé dans un endroit prévisible (à proximité d'un poste de travail, d'un serveur ou dans un fichier facilement identifiable) et non protégé ;
6) Un mot de passe ne doit jamais être enregistré dans un script de connexion automatique même si cette option est proposée à l'utilisateur par le système ;
7) Un mot de passe ne doit pas être divulgué ou partagé, ni être réutilisé ;
8) Un mot de passe doit être changé :
- en principe, au moins une fois tous les 60 jours ;
- à chaque fois qu'un utilisateur n'est plus habilité à accéder au poste de travail, à une ressource ou un fichier quelconque (il est préférable de supprimer le couple « identifiant - mot de passe ») ;
- dès qu'une divulgation à un tiers est pressentie.
9) Doit être chiffré lorsqu'il est conservé sur un support de stockage ou transite sur un réseau et être si possible à usage unique ;
10) Après au maximum cinq essais infructueux de mots de passe, l'identifiant utilisé est invalidé par le système et une alarme remontée à l'administrateur du système.

4. RESPECTER LES DROITS ACCORDÉS ET PROTÉGER SON POSTE DE TRAVAIL ET SES DONNÉES.

Vous devez :

- respecter les droits ou privilèges qui vous sont accordés ; ne tentez pas d'en acquérir d'autres ou d'usurper ceux d'un autre utilisateur ;

- protéger vos moyens d'identification et d'authentification (identifiants, mots de passe, cartes à puce, clés USB, certificats électroniques, clés de chiffrement, etc.) ;

- protéger les équipements qui vous sont attribués (ordinateur portable, assistant numérique personnel, téléphone mobile, ...), les supports d'information et les informations (documents, messages, fichiers) que vous utilisez à l'aide des moyens mis à votre disposition ;

- informer dans les meilleurs délais l'autorité compétente en cas de vol de matériels ou de documents, en cas de compromission d'équipements ou d'informations ;

- lors des opérations d'entretien ou de maintenance sur votre lieu de travail, veillez à ce que les données sensibles ne soient pas accessibles sans surveillance aux intervenants.

5. RESPECTER LA CONFIDENTIALITÉ DES DONNÉES ET DES COMMUNICATIONS.

Vous devez respecter la législation relative :

- à la protection des données à caractère personnel et à l'intimité de la vie privée ;

- au secret des correspondances émises par la voie des télécommunications.

Vous ne devez pas tenter d'accéder, de lire, de modifier, de copier, d'intercepter, de détruire les données, les messages ou les fichiers d'un autre utilisateur, quelles que soient leurs protections, sans autorisation explicite de l'utilisateur.

6. VERROUILLER OU ARRÊTER SON POSTE DE TRAVAIL LORSQU'IL EST INUTILISÉ.

Vous ne devez jamais quitter votre poste de travail sans verrouiller ou arrêter votre poste de travail. De même, il convient de ne jamais laisser un document affiché sur l'écran ou en présence d'un personnel non habilité ou n'ayant pas à en connaître

7. ÉTEINDRE SON POSTE DE TRAVAIL LE SOIR AVANT DE QUITTER SON BUREAU.

Sauf consigne particulière du service informatique, vous ne devez jamais quitter votre bureau le soir sans avoir éteint votre poste de travail.

8. NE PAS TENTER DE MANIPULATIONS HASARDEUSES OU TESTER LES MESURES DE SÉCURITÉ.

Vous devez vous abstenir de toute manipulation susceptible de perturber le fonctionnement des moyens informatiques, télécoms ou réseaux du ministère de la défense ou de ceux qu'il est possible d'atteindre à partir de ces systèmes.

N'exploitez pas d'éventuelles anomalies de fonctionnement, mais signalez-les (au même titre que les tentatives d'atteinte à la sécurité) à l'administrateur du système concerné.

Notez que la simple accession à un système informatique sans autorisation constitue un délit, même s'il n'en est résulté aucune altération des données ou fonctionnement dudit système. Si de telles altérations sont

constatées les sanctions prévues sont aggravées (art. 323-1 du code pénal). La tentative d'accès est punie des mêmes peines (art.323-7 du code pénal).

9. ÊTRE VIGILANT ET RENDRE COMPTE DE TOUTE ANOMALIE OU INCIDENT.

Vous devez être vigilant et rendre compte à l'administrateur du système de toute anomalie ou incident susceptible de porter atteinte à la sécurité des ressources informatiques des entités relevant de l'autorité qualifiée SGA ; à défaut contactez l'officier de sécurité des systèmes d'information (OSSI) ou le responsable de la sécurité des systèmes d'information (RSSI) de votre organisme.

ANNEXE III.

LA MESSAGERIE ÉLECTRONIQUE.

Les procédures applicables au courrier classique (papier) sont transposables au courrier électronique sous réserve des adaptations nécessaires. Le courrier électronique est régi par des règles de rédaction, circulation, signature, protection, conservation, destruction comme le courrier papier.

1. QUELLE MESSAGERIE UTILISER ?

La transmission des informations, par le biais de la messagerie électronique, s'effectue conformément aux exigences résultant de leur niveau de protection.

L'Internet et l'Intradef doivent être réservés à l'échange d'informations non-protégées ou sensibles non classifiées de défense. Ces dernières doivent être en tant que de besoin protégées par des dispositifs fournis ou autorisés par le ministère de la défense. Les réseaux précités ne sauraient permettre de véhiculer des informations classifiées de défense, fonction réservée à l'Intraced.

L'Intradef est connecté à l'intranet interministériel SETI+(9), qui est lui-même raccordé à Internet. Ainsi l'utilisateur peut émettre et recevoir depuis l'Intradef des messages en provenance d'Internet.

Conformément au principe d'un usage professionnel des ressources, l'utilisation de la messagerie électronique sur Internet et l'Intradef pour échanger des messages à caractère personnel n'est qu'une tolérance.

On distingue sur Intradef deux types d'adresse mél :

- l'adresse mél fonctionnelle : c'est l'adresse mél officielle attribuée à un organisme, une autorité ou une fonction pour échanger du courrier officiel
(ex : msiag@defense.gouv.fr ou msiag@sga.defense.gouv.fr) ;

- l'adresse mél professionnelle : c'est l'adresse mél individuelle attribuée à titre professionnel à tout agent (utilisateur) pour échanger du courrier professionnel
(ex : prenom.nom@defense.gouv.fr ou prenom.nom@sga.defense.gouv.fr).

2. QUE PEUT-ON ENVOYER PAR LA MESSAGERIE ?

2.1. **Des messages « non protégés ».**

Un message est « non protégé » lorsqu'il contient exclusivement des informations, documents, fichiers à caractère professionnel sans marque de sensibilité explicite. Ce type de message peut être échangé à partir de l'adresse mél professionnelle d'un agent ou d'une adresse mél fonctionnelle sur tout type de réseau (Internet, Intradef).

2.2. **Des messages « sensibles ».**

Un message est « sensible » lorsqu'il contient des informations, documents, fichiers relevant de l'article 4 de la recommandation 901 [Rec901](10). Dès que les moyens appropriés sont mis en place, l'échange par Internet de messages sensibles (ex : confidentiel personnel, confidentiel industrie) implique un chiffrement (au moyen de dispositifs autorisés ou fournis par le ministère de la défense) du message et des pièces jointes.

2.3. **Des messages classifiés de défense.**

Toute communication d'informations classifiées de défense (secret défense, confidentiel défense) via la messagerie électronique doit s'opérer via des systèmes et réseaux dédiés à la communication d'informations classifiées de défense (ex : Intraced).

3. MÉLS FONCTIONNELS, PROFESSIONNELS, PERSONNELS, QUELLES CONSÉQUENCES ?

Les règles sont les suivantes :

1) Les messages échangés à l'aide des adresses mél fonctionnelles relèvent du courrier officiel et sont la propriété du ministère de la défense ;
2) Les messages échangés à l'aide de l'adresse mél professionnelle relèvent du courrier professionnel. Ils sont la propriété du ministère de la défense et non celle de l'agent, sauf en cas d'indication manifeste du caractère personnel du message, selon les dispositions énoncées à l'alinéa suivant ;
3) L'usage du mot-clé « Personnel » ou « Privé » dans l'objet d'un message (cela doit être le premier mot du champ « Objet ») échangé à l'aide d'une adresse mél professionnelle a pour effet de transformer un mél professionnel en une correspondance privée (mél personnel) ;
4) Les messages échangés à l'aide d'adresses mél personnelles ou privées relèvent par nature de la correspondance privée (mél personnel) ;
5) Les messages à caractère personnel doivent être rangés dans le « dossier privé » (cf. Protection de la vie privée de l'agent sur le lieu de travail) ;

Le classement d'un mél dans une catégorie ou une autre a les conséquences suivantes :

- Méls fonctionnels. Les messages échangés à l'aide des adresses mél fonctionnelles (courrier officiel), sont la propriété du ministère de la défense. Des mesures sont prises pour en assurer la protection et la conservation (cf. infra). Au départ du détenteur, la transmission au successeur (organisme, autorité, fonction) des messages indispensables à la continuité du service est assurée par le service informatique ;

- Méls professionnels. Ces méls (sauf s'ils relèvent de la correspondance privée) sont la propriété du ministère de la défense. Des mesures sont prises pour en assurer la protection et la conservation au départ de l'agent (cf. infra). Au préalable, un agent peut effacer des messages professionnels, échangés à partir de son adresse mél professionnelle, s'il estime que ces messages n'engagent pas l'administration ou que leur conservation n'apparaît pas indispensable à la continuité du service ou est susceptible de porter préjudice. Ensuite, avec l'autorisation explicite de l'agent les méls professionnels sont communiqués à son successeur par le service informatique ;

- Méls personnels. Dans le cas d'une correspondance privée(11), les parties prenantes sont maîtres de cette correspondance. Elles peuvent en disposer à leur convenance (ex : les supprimer, les conserver).

Les boîtes aux lettres sont supprimées par l'administrateur de la messagerie lorsqu'elles sont devenues sans objet ou sur la demande de l'utilisateur lui-même.

4. SAUVEGARDE DES MESSAGES ÉLECTRONIQUES.

Pour garantir la qualité du service du système de messagerie, les messages échangés à partir de boîtes aux lettres professionnelles ou fonctionnelles sont sauvegardés sur des supports appropriés par le service informatique concerné. La durée de conservation des messages est fixée par l'acte réglementaire portant décision de création du traitement d'informations nominatives que constitue le système de messagerie électronique. Au-delà de cette durée, l'archivage des messages est préparé selon les mesures énoncées au paragraphe suivant.

5. QUELLE EST LA VALEUR JURIDIQUE D'UN MÉL ?

En matière administrative comme en matière commerciale, le principe est celui de la liberté de la preuve qui peut être apportée par tous moyens. Un message électronique peut donc constituer un élément de preuve susceptible d'engager la responsabilité de son auteur ou de l'administration.

Dans le domaine où la preuve est dite « légale » et repose sur la règle de l'écrit, l'article 1316-4 du code civil(12) permet au juge d'admettre un écrit électronique à titre de preuve. Toutefois, pour être recevable, le justiciable qui apporte une preuve par mél doit obligatoirement prouver, d'une part, l'identité de la personne

dont il émane, et, d'autre part, qu'il a été établi et conservé dans des conditions qui en garantissent l'intégrité.

---

(9) SETI+ : tous les ministères, la Présidence de la République, le Conseil d'État, la Cour des Comptes, le Sénat et l'Assemblée Nationale sont reliés entre eux par le réseau privé de communication SETI+ (SErvice de Transport Inter-administration), dans le cadre du programme AdER (Administration en Réseau) lancé le 19 janvier 1999 lors du Comité Interministériel pour la Société de l'Information.

(10) Les informations sensibles sont des informations pour lesquelles le non respect de la confidentialité, la disponibilité ou l'intégrité mettrait en cause la responsabilité du propriétaire ou du dépositaire, ou causerait un préjudice à eux-mêmes ou à des tiers. À titre d'exemple on peut citer : les informations dont la consultation ou la communication porteraient atteinte au secret des délibérations du Gouvernement, au secret de la vie privée, aux dossiers personnels et médicaux, à la sécurité publique, au déroulement des procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, les informations relatives aux contrats et marchés publics dématérialisés, etc.

(11) Message échangé à l'aide d'une adresse mél personnelle ou d'une adresse mél professionnelle et à condition que le mot-clé « personnel » ou « privé » soit le premier mot de l'objet du message.

(12) http://www.legifrance.gouv.fr/WAspad/UnArticleDeCode?code=CCIVILL0.rcv&art=1316-4

ANNEXE IV.

ORGANISMES RELEVANT DU SECRÉTARIAT GÉNÉRAL POUR L'ADMINISTRATION AU SENS DE L'INSTRUCTION N° 4418/DEF/CAB/SEC/DIR/SIC DU 25 SEPTEMBRE 2000.

1. ORGANISMES PLACÉS DIRECTEMENT SOUS L'AUTORITÉ DU SECRÉTARIAT GÉNÉRAL POUR L'ADMINISTRATION.

Sous-direction du pilotage des programmes SGA (SDDP)
Direction des affaires financières (DAF)
Direction des ressources humaines du ministère de la défense (DRH-MD))
Direction des affaires juridiques (DAJ)
Direction de la mémoire, du patrimoine et des archives (DMPA)
Direction des statuts, des pensions et de la réinsertion sociale (DSPRS)
Direction du service national (DSN)
Service des moyens généraux (SMG)
Service d'infrastructure de la défense (SID)
Service historique de la défense (SHD)
Délégation aux restructurations (DAR)
Mission d'aide au pilotage (MAP)
Mission système d'information d'administration et de gestion (MSIAG)
Centre de formation au management du ministère de la défense (CFMD)
Centre d'études d'histoire de la défense (CEHD)
Centre d'études en sciences sociales de la défense (C2SD)
Commission consultative médicale des anciens combattants et victimes de guerre
Inspecteurs civils

2. AUTRES ORGANISMES RELEVANT DE L'AUTORITÉ QUALIFIÉE SECRÉTARIAT GÉNÉRAL POUR L'ADMINISTRATION.

Cabinet du ministre de la défense
Cabinet du secrétaire d'État aux anciens combattants
Sous-direction des bureaux du cabinet (SDBC)
Bureau des officiers généraux (BOG)
Contrôle budgétaire et comptable ministériel (CBCM)
Mission PME - PMI
Direction générale des systèmes d'information et de communication (DGSIC)
Contrôle général des armées (CGA)
Délégation aux affaires stratégiques (DAS)
Délégation à l'information et à la communication de la défense (DICOD)
Inspections générales des armées :

- Terre

- Marine

- Armement

Aumôneries :

- Aumônerie catholique

- Aumônerie israélite

- Aumônerie protestante

Trésorerie aux armées
Cercle Saint-Dominique
Commission armées jeunesse
Commission d'orientation et d'intégration des militaires
Comité médical
Commission des recours militaires
Conseil économique de la défense
Conseil supérieur de la fonction militaire
Conseil supérieur de la réserve militaire