BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°2 du 9 janvier 2009

PARTIE PERMANENTE
Administration Centrale

Texte n°1

INSTRUCTION N° 2003/DEF/DGSIC
portant code de bon usage des systèmes d'information et de communication du ministère de la défense.

Du *20 novembre 2008*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

INSTRUCTION N° 2003/DEF/DGSIC portant code de bon usage des systèmes d'information et de communication du ministère de la défense.

Du 20 novembre 2008

NOR D E F M 0 8 5 2 8 4 5 J

Références :

Ordonnance n° 2005-1516 du 8 décembre 2005 (JO n° 286 du 9 décembre 2005, texte n° 9 ; BOC, p. 8645. ; BOEM 120-0.3.1).
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).

Pièce(s) Jointe(s) :

Une annexe.

Classement dans l'édition méthodique : BOEM 160.11.

Référence de publication : BOC N°2 du 9 janvier 2009, texte 1.

Introduction.

Les systèmes d'information et de communication (SIC) mis à disposition par le ministère de la défense (dont l'internet) constituent des outils destinés à faciliter, à simplifier, le travail et les relations professionnelles dans le cadre des activités du ministère. Leur utilisation est soumise à des règles communes et d'autres plus spécifiques, dans l'optique d'une conciliation entre les droits et les devoirs de l'utilisateur * d'une part et, l'exigence d'un niveau de sécurité à atteindre, selon le système d'information concerné, d'autre part.

Le présent texte a pour finalités de rappeler aux utilisateurs :

- l'usage attendu par le ministère de ses systèmes d'information : conformité avec la législation, la réglementation interne et les règles élémentaires de courtoisie et de respect d'autrui ;

- les dispositions spécifiques liées à l'usage de certains médias et les attributions particulières des acteurs de la sécurité des systèmes d'information ;

- les moyens de contrôle mis en œuvre.

Le ministère de la défense met en place des dispositifs qui peuvent permettre directement ou indirectement de déceler les éventuelles violations aux présentes dispositions. Ces moyens sont rappelés dans ce code au titre de l'obligation d'information légale des moyens de surveillance mis en œuvre, mais également parce qu'il est important qu'une confiance mutuelle soit instaurée entre l'utilisateur et le ministère de la défense.

Le sentiment d'extrême facilité que procurent à leurs utilisateurs les nouvelles technologies ne doit pas occulter les responsabilités de chacun, qu'il s'agisse des devoirs communs à tous les citoyens, comme le respect de la dignité humaine et des règles de courtoisie ou d'obligations plus spécifiques, comme celles liées à l'usage d'un réseau ou plus généralement d'une ressource informatique au sein du ministère de la défense. Le bon fonctionnement des réseaux numériques dépend du soin que mettra chacun à observer l'ensemble de ces principes.

En expliquant dans ce texte l'utilisation qu'il attend, le ministère de la défense souhaite que le personnel concoure à la fois à la sécurité et au bon fonctionnement des systèmes d'information qu'il met à sa disposition, mais aussi au respect des dispositions législatives et réglementaires et de l'image du ministère. Les utilisateurs sont tenus de respecter l'ensemble des dispositions énoncées par le présent code. En cas de manquement aux obligations qu'il contient, les contrevenants s'exposent à des sanctions disciplinaires. Ils peuvent également s'exposer à des sanctions pénales et civiles.

Objet et champ d'application.

Le présent code constitue un code de bon usage pour l'ensemble des utilisateurs des systèmes d'information et de communication du ministère. Il ne préjuge pas des dispositions particulières devant s'appliquer aux acteurs ayant un rôle particulier dans la mise en œuvre et le soutien des systèmes d'information (administrateurs*, chargés d'audit...). Par ailleurs, l'utilisation de ressources informatiques par les organisations syndicales fait l'objet d'une charte particulière.

Tout utilisateur de ressources informatiques mises à disposition par le ministère de la défense doit prendre connaissance du présent code et le respecter, y compris en opérations extérieures et à l'étranger (1). Cette connaissance ne dispense pas de la lecture et du respect des autres textes législatifs et réglementaires, notamment ceux relatifs à la protection des informations classifiées* de défense.

Le code a été soumis aux instances paritaires du ministère de la défense.

Les termes marqués dans le texte d'un astérisque sont définis dans le glossaire situé en annexe.

Un encadré rappelle pour la majorité des domaines, le principe ou la règle principale à retenir. Les règles d'usage et de sécurité ne peuvent être modifiées pour satisfaire le besoin d'un utilisateur.

TITRE PREMIER.
DISPOSITIONS COMMUNES À L'ENSEMBLE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION DU MINISTÈRE.

1. RESPECT D'AUTRUI.

Respect de la personne et de l'institution de la défense.

Quelle qu'en soit la nature, les informations* diffusées sur les réseaux, dans les dialogues en ligne, dans les boîtes aux lettres ou les forums, ou publiées sur les sites ou les bloc-notes électroniques ne doivent nuire ni à la dignité d'autrui, ni à l'institution de la défense. L'utilisateur se conforme à la législation applicable en matière de respect des personnes.

1.1. **Législation applicable en matière de respect des personnes.**

Il s'agit de :

- ne pas porter atteinte à l'image d'une personne, à sa vie privée, à sa personnalité, à ses convictions ou à sa sensibilité, par des messages, textes ou images provocants (discriminatoires, pornographiques, ...), malveillants, menaçants (insultes, injures...), ou illégaux (pédophiles, diffamatoires...) ;

- respecter les droits des personnes sur leur image ;

- ne pas se servir des systèmes d'information et de communication du ministère pour effectuer un traitement de données à caractère personnel (collecte de telles données, constitution de fichiers, conservation, exploitation, ...) non préalablement déclaré par le ministère à la commission nationale informatique et libertés (CNIL) ;

- ne pas porter atteinte à l'image du ministère ;

- ne pas utiliser de logiciels à caractère agressif (outils de cassage de mots de passe, sondes...) sans autorisation explicite du fonctionnaire de sécurité des systèmes d'information*.

1.2. **Législation applicable en matière de respect de la propriété intellectuelle.**

L'utilisation des ressources informatiques et informationnelles du ministère doit se faire dans le respect des droits de propriété des auteurs.

Il est interdit de reproduire (à quelque titre que ce soit) ou de communiquer, intégralement ou partiellement, sauf exception légale, une œuvre de l'esprit* au public*.

Cette interdiction peut être levée par l'autorisation formelle de l'auteur ou faire l'objet d'une dérogation légale.

Les notions d'auteur et d'œuvre intéressent aussi bien les individus et les productions appartenant au ministère de la défense que ceux et celles d'origine extérieure.

2. RESPECT DES RÈGLES DE SÉCURITÉ.

L'accessibilité à de multiples bases de données et d'informations nécessite l'instauration de règles visant à en assurer la gestion et la sécurité. Mais aucun dispositif n'est pleinement efficace si tous les acteurs ne se sentent pas concernés : la sécurité est l'affaire de chacun.

L'utilisateur :

- mettra en œuvre tous les moyens à sa disposition et dont il a connaissance pour que ses actions ne puissent nuire au bon fonctionnement des systèmes informatiques et des réseaux, de quelque façon que ce soit ;

- ne cherchera pas à modifier ni remanier la configuration des systèmes d'information ;

- se conformera aux éventuels règlements spécifiques [politique de sécurité des systèmes d'information (SI), procédures d'exploitation de sécurité...] complémentaires aux dispositions du présent code.

Il est interdit de modifier ou de tenter de modifier son environnement de travail sans autorisation (ajout et suppression de programmes, de supports externes ou de périphériques ...).

2.1. **Vérifications sommaires.**

L'utilisateur vérifie :

- au préalable que son environnement de travail correspond bien au niveau de sécurité attendu pour les informations qu'il va traiter ;

- la décontamination de tout fichier importé avant de l'ouvrir, selon les procédures en vigueur, accessibles auprès du responsable local de la sécurité des systèmes d'information.

2.2. **Utilisation de moyens personnels.**

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 (2). L'autoriser suppose de pouvoir garantir que la connexion n'affaiblirait pas cet ensemble. Or, il s'avère compliqué voire impossible, techniquement et juridiquement, pour le ministère, de contrôler les répercussions de cette connexion pour ses systèmes d'information, en particulier en préservant, quoiqu'il advienne, l'espace personnel réservé sur ce(s)

support(s). C'est pourquoi, le ministère de la défense n'autorise pas l'usage d'équipements ou supports personnels.

Il est interdit de connecter les équipements et les supports personnels avec tout système d'information du ministère de la défense.

2.3. **Supports professionnels extérieurs au ministère de la défense.**

L'intégration (3) et l'interconnexion (4) de moyens professionnels extérieurs avec un système d'information du ministère de la défense constituent une menace potentielle pour l'ensemble du système.

C'est pourquoi, le régime relatif à l'utilisation de moyens personnels vaut pour les équipements professionnels n'appartenant pas au ministère de la défense. Cependant, si pour des raisons de service une telle opération avec un système d'information du ministère s'avérait incontournable, les moyens professionnels extérieurs (5) sont, préalablement à l'intégration ou l'interconnexion, puis a posteriori, soumis au respect de procédures de contrôle*.

L'utilisation de moyens professionnels extérieurs au ministère de la défense est en principe interdite. Dans le cadre d'une exception, elle est soumise au respect de procédures de contrôle.

2.4. **Autorisation d'accès.**

Pouvant être subordonnés à la détention d'une habilitation*, des droits d'accès et privilèges* sont accordés sur les systèmes d'information, selon la fonction occupée et le besoin d'en connaître de la personne. Ils définissent un profil (6) qui peut être retiré à la cessation de la fonction ou à tout moment si le comportement de l'intéressé ne permet plus de lui accorder toute confiance.

Les droits d'accès et privilèges* sont personnels et incessibles. L'utilisateur respecte les mesures de sécurité(7) suivantes :

- verrouillage de l'accès logique ou arrêt de son poste de travail lorsqu'il s'absente (8) ;

- choix de mots de passe sûrs [en utilisant différents types de caractères (9)], qu'il change régulièrement selon les préconisations en vigueur dans son organisme ;

- conservation en lieu sûr des moyens permettant son identification ou son authentification (carte à puce) et non divulgation des éléments secrets (mots de passe, clé privée...) y concourant.

Les droits d'accès et privilèges sont personnels et incessibles.

2.5. **Principe de confidentialité et de discrétion.**

L'ensemble du personnel du ministère de la défense est soumis à une obligation générale et permanente de discrétion professionnelle. Ce devoir de discrétion s'exerce également à l'égard des informations et documents électroniques disponibles sur les réseaux internes.

Afin de préserver la discrétion et la confidentialité des informations, l'utilisateur doit :

- s'assurer, au besoin auprès de sa hiérarchie en cas de doute, du niveau de protection à affecter aux documents avant de les traiter et de les diffuser ;

- veiller à ce que des tiers non habilités ou non autorisés ne puissent avoir accès à des informations sensibles ou classifiées, notamment celles affichées sur les écrans des portables et des postes fixes ;

- stocker les fichiers contenant des informations classifiées aux emplacements autorisés, spécifiés par la politique de sécurité (10) ;

- ne pas utiliser, sans son accord, les moyens informatiques et les accès réseaux d'un autre utilisateur.

L'utilisateur respecte les règles de protection de l'information et des systèmes qui les supportent, en fonction de leur niveau de sensibilité.

2.6. **Prévention contre les contenus malveillants*.**

Il est mis à la disposition de chaque utilisateur des moyens de protection et de contrôle technique, adaptés aux différents environnements de travail contribuant à la sécurité informatique. Dans ce contexte, l'utilisateur doit :

- contrôler, avant utilisation, tout support, document informatique (fichier ou pièce jointe) importé, selon les moyens et procédures de sécurité en vigueur ;

- éjecter tout support amovible de son lecteur avant d'éteindre son ordinateur pour limiter les risques d'activation de contenu malveillant au prochain démarrage.

L'utilisateur respecte les mesures de lutte contre les contenus malveillants.

2.7. **Réaction/Incidents.**

En cas d'incidents réels ou supposés, menaçant directement ou indirectement le fonctionnement des systèmes d'information ou la sécurité d'une ressource, l'utilisateur :

- se conforme aux fiches réflexes et prescriptions (11) qui, selon les circonstances, peuvent prévoir le débranchement manuel de l'ordinateur ou sa déconnexion (sans l'éteindre ni le redémarrer) ;

- alerte immédiatement de l'incident son correspondant de sécurité des systèmes d'information.

L'utilisateur doit rendre compte de tout incident et prendre les mesures conservatoires prescrites à son niveau.

3. RESPECT DES RÈGLES D'UTILISATION.

3.1. **Finalité professionnelle.**

Les systèmes d'information du ministère de la défense ont une vocation professionnelle.

L'utilisation à des fins personnelles de systèmes d'information non classifiés de défense est tolérée sous réserve qu'elle reste exceptionnelle et sans impact sur le bon fonctionnement général du système ou sur la bonne marche du service.

L'utilisation à des fins personnelles de systèmes d'information classifiés de défense est interdite.

Afin de concrétiser le droit au respect de sa vie privée, l'utilisateur mentionne clairement le caractère privé de la correspondance et de ses fichiers personnels en les consignant notamment dans un dossier nommé « personnel » (12). À défaut, ils seront présumés professionnels.

En utilisant les ressources informatiques du ministère de la défense, l'utilisateur a pleinement conscience que même si, en principe, personne ne doit accéder à son espace personnel clairement indiqué :

- du personnel soumis à une obligation de non-divulgation tels les administrateurs, auditeurs, contrôleurs et inspecteurs de la sécurité des systèmes d'information (SSI) ;

- des agents automatiques tels les anti-virus ;

peuvent y être autorisés dans le cadre de leurs missions ou en cas d'anomalie ou d'incident réel ou supposé menaçant la sécurité ou le bon fonctionnement des dites ressources.

Avant restitution à l'administration de supports informatiques, l'utilisateur efface toutes les données à caractère personnel qu'il aurait pu y enregistrer.

3.2. **Règles d'utilisation de la messagerie.**

L'utilisateur peut bénéficier d'une messagerie interne ou Internet professionnelle (boîtes aux lettres, services...) mise à sa disposition par le ministère. Son utilisation obéit à différentes règles :

*3.2.1. **Application des règles relatives au courrier papier.***

À la différence des échanges de messages informels, la diffusion de courriers professionnels officiels, par le biais de la messagerie électronique, est, sauf dérogation écrite du commandement, soumise aux règles formelles de validation similaires à celles adoptées pour le support papier.

*3.2.2. **Respect du principe de discrétion.***

Il convient de ne pas rechercher ou ouvrir un message dont on n'est manifestement pas destinataire pour action ou en copie, sauf si ce dernier a donné explicitement mandat ou procuration pour le faire, afin de prévenir son absence ou un empêchement. Par ailleurs, il est nécessaire de vérifier, avant l'envoi d'un message, qu'aucune erreur ne s'est glissée dans la sélection des destinataires.

*3.2.3. **Échanges et diffusion de courriers professionnels.***

La transmission des informations, par le biais de la messagerie électronique, s'effectue conformément aux exigences résultant de leur niveau de sensibilité. L'Internet et les intranets* défense sensibles (comme l'Intradef*) ne sauraient permettre de véhiculer des informations classifiées de défense, fonction réservée aux intranets classifiés de défense (tels l'Intraced).

L'origine et l'authenticité* d'un message électronique ne sont pas systématiquement garanties. C'est pourquoi, l'utilisateur peut être fondé à en vérifier l'origine réelle et l'authenticité, selon la gravité, la portée et l'origine du message par des moyens parallèles (en téléphonant, par exemple, à l'expéditeur).

Qu'il réponde ou pas à des conditions de forme (présence de la Marianne, numérotation, ...), le courrier transitant par les systèmes d'information du ministère peut être officiel, c'est-à-dire émaner de l'autorité compétente.

Il convient d'informer la hiérarchie et lui retransmettre les messages ou copies de messages, reçus en fonction de la nature et de l'importance des contenus échangés (le respect des règles habituelles de compte-rendu au supérieur s'applique également aux intranets pour le personnel du ministère).

*3.2.4. **Pertinence du choix des destinataires pour éviter la saturation du réseau et des serveurs.***

Pour éviter la saturation du réseau et des serveurs, et pour ne pas obliger les destinataires à lire des messages qui ne présenteraient pas d'intérêt pour eux, l'utilisateur d'une messagerie interne doit :

- limiter l'envoi de chaque message aux destinataires réellement concernés. L'ouverture des réseaux du ministère vers l'interministériel et l'Internet nécessite une vigilance particulière ;

- s'abstenir de solliciter l'envoi de messages par un grand nombre d'intranautes à une même boîte aux lettres ;

- ne pas abuser de certaines fonctionnalités de la messagerie telles que « transférer à » ou « répondre à tous ».

3.2.5. ***Vigilance selon le média utilisé pour atteindre les destinataires en s'assurant du niveau autorisé pour les informations transmises.***

La diffusion à tous est réservée à l'autorité et, dans le cadre de leurs attributions, à l'administrateur du réseau et aux acteurs mandatés dans le cadre de leurs fonctions.

Un message envoyé sur un réseau échappe au contrôle de son expéditeur : il peut être redistribué à d'autres destinataires, que ceux initialement visés.

3.2.6. ***Forme des messages et contenu*.***

L'utilisateur facilite la gestion des informations par ses destinataires en choisissant un titre clair et explicite comme objet du message qu'il désire envoyer. Par exemple, il peut débuter l'objet, qui apparaît dans l'outil de messagerie, par un terme significatif tel que « Comité de direction : ordre du jour de la réunion de ../../.. ».

La lecture du message par le destinataire doit être rendue aisée. Ainsi, il convient de s'assurer que le corps du message ne dépasse pas une page dactylographiée, et qu'il indique l'objet des pièces jointes lorsqu'il en contient.

Il est conseillé d'aborder un seul sujet par message et de relire les messages avant envoi. Il importe de vérifier qu'il ne manque aucune pièce jointe, et que les fichiers émis sont de la dernière version, dans le cas où les documents auraient fait l'objet de plusieurs versions. Le marquage « Urgent » n'est à utiliser qu'en cas de réelle nécessité.

Les messages électroniques (pièces jointes comprises) sont envoyés selon des critères qualitatifs (innocuité du contenu, sa pertinence) et quantitatif (volume réduit au minimum). Des tailles de message peuvent être fixées selon les types de messagerie : si un message excède la taille prescrite, il peut ne pas atteindre son destinataire.

3.2.7. ***Conservation et protection des courriels.***

Selon le type de messagerie et la politique de conservation des données, l'utilisateur est informé de règles de conservation et de protection des courriels en vigueur dans son organisme (il s'agit de la taille maximum de la boîte aux lettres et de la durée technique de conservation avant effacement). À intervalles réguliers, les boîtes aux lettres peuvent faire l'objet de restrictions d'usage ou être vidées automatiquement de leur contenu après l'avertissement préalable des utilisateurs.

Vider régulièrement sa boîte aux lettres, en sauvegardant sur un autre support les anciens messages qui doivent être conservés.

3.2.8. ***Certificat électronique.***

L'identité de l'expéditeur affichée dans de simples courriers électroniques n'est pas une preuve de l'identité réelle de l'expéditeur. De même, l'intégrité et l'authenticité* du message ne sont pas, a priori, garanties. C'est pourquoi un système de certificat électronique est mis progressivement en place au sein du ministère de la défense.

L'usurpation d'identité constitue un délit. Les utilisateurs doivent signaler toute usurpation d'identité qu'ils constatent et ne pas générer eux-mêmes des faux en écriture sous peine de poursuites.

3.2.9. ***Moyens de chiffrement*.***

Seuls les moyens de chiffrement fournis ou autorisés d'emploi par le ministère sont utilisables. Ils font l'objet de prescriptions en terme d'emploi et de conservation (ACSSI*).

L'utilisation de moyens de chiffrement est réglementée selon le niveau de protection à accorder aux informations.

3.3. **Propriété et conservation des documents électroniques.**

L'utilisateur est responsable de ses documents électroniques (fichiers et correspondances). Il veille à leur conservation et les classe, aux endroits définis par l'administrateur, selon les autorisations et règles de sécurité prescrites, selon leur catégorie d'appartenance (personnel ou professionnel).

3.3.1. ***Propriété des documents électroniques.***

Les documents électroniques, à moins qu'ils ne relèvent de la correspondance privée ou du dossier « personnel », appartiennent au ministère de la défense.

Ces documents électroniques professionnels sont à conserver méthodiquement et soigneusement (archivage et transmission au successeur).

L'utilisateur obéit à des règles particulières lorsqu'il entend modifier un document électronique dont il n'est pas l'auteur ou qui a fait l'objet de diffusion officielle.

Il existe alors deux cas de figure :

- soit le document de référence est protégé et accessible en lecture seule, auquel cas le destinataire pourra faire, s'il le veut, des propositions de modifications ;

- soit l'utilisateur peut apporter des modifications sur le document lui-même, à condition de les rendre identifiables comme telles (par exemple au moyen du « mode correction » ou « suivi des modifications » des traitements de texte).

3.3.2. ***Preuve*.***

L'écrit électronique peut constituer une preuve admissible devant une juridiction.

L'écrit électronique (courriel, fichier etc.) pouvant constituer une preuve, l'utilisateur doit prendre toute mesure pour conserver les documents électroniques dans de bonnes conditions, selon les règles d'emploi prescrites.

3.3.3. ***Organisation de l'exploitation et de l'archivage des documents électroniques.***

Les documents électroniques sont susceptibles d'engager ou de décharger l'administration. Par ailleurs, la conservation de certains fichiers est indispensable à la continuité du service.

Afin de faciliter l'exploitation et préparer l'archivage des documents électroniques, il est indispensable de classer lisiblement et fonctionnellement les dossiers électroniques.

TITRE II.

DISPOSITIONS PROPRES À CERTAINS MÉDIAS ET À CERTAINS ACTEURS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.

1. À CERTAINS MÉDIAS.

1.1. **À l'Internet.**

1.1.1. ***Rappels élémentaires.***

L'internet est un média spécifique utilisé par le ministère de la défense mais dont la sécurité ne dépend pas de lui et sur lequel un niveau minimum de sécurité ne peut être garanti. C'est pourquoi, le ministère de la défense attire l'attention de tous les utilisateurs quant à son emploi.

- fausse impression d'anonymat sur l'Internet. Contrairement à l'impression couramment ressentie par les internautes, la navigation sur l'Internet n'est pas anonyme. Ainsi avec notamment l'adresse IP, Internet Protocol, attribuée à chaque connexion ou à un ordinateur particulier, il est possible de remonter jusqu'à l'utilisateur et en l'occurrence jusqu'au ministère de la défense ;

- différents risques : infection virale, vol de données ou mots de passe etc. ;

- fiabilité des informations présentées sur l'Internet.

De plus, tout système d'information relié à l'Internet est susceptible d'être l'objet d'attaques (virus, cheval de Troie, vols de données, de mots de passe ...) basées souvent sur la naïveté et le manque de vigilance des internautes. Le ministère de la défense n'échappe pas à ce phénomène.

1.1.2. ***Règles applicables à la navigation.***

L'emploi d'Internet peut être :

- soit consacré à l'activité professionnelle du personnel du ministère de la défense. Il doit être utilisé au regard des fonctions ou des missions à mener confiées à l'utilisateur ;

- soit utilisé ponctuellement, dans le respect de la priorité de l'activité précédente, à des fins personnelles. Cette utilisation ne doit pas nuire au service ni gêner le travail des collaborateurs en cas de partage des postes Internet.

Sont consultés des sites dont le contenu ne contrevient pas à la loi et sans conséquence pour la sécurité ou la réputation du ministère. L'accès à certains sites web peut être bloqué pour répondre à des impératifs de sécurité ou au motif d'un contenu jugé offensant ou inapproprié.

1.1.3. ***Forum de discussion, dialogue en ligne (chat), bloc-notes électronique (blog), réseaux sociaux.***

La participation d'un utilisateur à des forums de discussion, dialogue en ligne, bloc-notes électronique, réseaux sociaux s'effectue dans les conditions définies pour la navigation sur l'Internet.

Elle obéit aux règles citées supra dont notamment, celles concernant le devoir de réserve, la protection des informations et la discrétion professionnelle. L'agent du ministère sera vigilant quant aux propos qu'il y tient.

1.2. **Aux systèmes d'information et de communication traitant d'informations classifiées.**

En raison des intérêts opérationnels en jeu, de la sensibilité de l'information et des risques potentiels encourus, des politiques de sécurité spécifiques à chaque système classifié définissent les règles complémentaires à respecter par les utilisateurs.

1.3. **Aux supports amovibles*.**

Les supports amovibles sont utilisés conformément à la politique de sécurité des systèmes d'information et aux règles relatives à la protection des informations. Notamment, ils sont soumis aux règles relatives à la protection des informations qu'ils contiennent.

Les supports amovibles du ministère de la défense sont toujours placés sous la responsabilité et la surveillance du détenteur du support.

Les supports amovibles traitant d'informations classifiées de défense sont conservés conformément à la réglementation.

La perte d'un support contenant ou ayant contenu des informations classifiées doit faire l'objet d'un compte-rendu aux autorités hiérarchiques. Plus généralement, toute compromission (13) supposée d'information classifiée doit être portée à la connaissance de la direction de la protection et de la sécurité de la défense qui estime s'il y a risque de compromission.

2. À CERTAINS ACTEURS DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION.

Les auditeurs, contrôleurs, inspecteurs SSI, administrateurs, gestionnaires de réseaux participent activement à la SSI. À cette fin, ils disposent des droits et des moyens nécessaires et suffisants à l'exercice de leur mission avec, en corollaire, des devoirs.

C'est pourquoi, il apparaît utile d'expliquer brièvement à l'utilisateur leurs rôles et de préciser les dispositions générales auxquelles ils sont tenus. Les auditeurs, contrôleurs, inspecteurs SSI, les gestionnaires de réseaux et les administrateurs sont soumis aux dispositions spécifiques les concernant.

2.1. **Application des politiques de sécurité des systèmes d'information.**

Échelons techniques de la sécurité sur les systèmes d'information et de communication du ministère de la défense, ces acteurs suivent les politiques et appliquent les plans d'action pour la sécurité des systèmes d'information déterminés aux échelons supérieurs.

Leur intervention s'inscrit dans l'intérêt du service, de l'usager et de la sécurité du système.

Dans cet esprit, il leur incombe de :

- veiller à ce que tout utilisateur d'un système d'information possède les droits d'accès correspondant à son profil et à son habilitation ;

- minimiser les interruptions de service tant dans la durée, dans le moment choisi que dans leur étendue et en informer, si possible, au préalable les utilisateurs ;

- déconnecter un utilisateur en cas de comportement dangereux et d'en aviser sa hiérarchie.

2.2. **Obligation de secret professionnel et limite.**

Administrateurs et gestionnaires de réseaux n'accèdent pas en principe aux dossiers et messages privés des utilisateurs. Néanmoins, ils peuvent en prendre connaissance, en cas d'anomalie, de risque détecté, réel ou supposé, pour remplir leur mission de préservation de la sécurité des systèmes d'information.

Certaines informations sont couvertes par le secret des correspondances ou relèvent de la vie privée. Dès lors, les administrateurs, les gestionnaires de réseaux, les auditeurs SSI sont soumis à l'obligation de non-divulgation s'exerçant à l'égard même des supérieurs hiérarchiques, excepté si le bon fonctionnement des systèmes ou l'intérêt de l'institution sont mis en cause et sauf dispositions législatives particulières pouvant les contraindre à dévoiler des informations.

TITRE III.

MOYENS DE CONTRÔLE DU RESPECT DES RÈGLES ÉDICTÉES PAR LE CODE.

Pour prévenir et détecter les actions potentiellement dommageables pour la défense et ses systèmes d'information, le ministère de la défense adopte des mesures et des moyens techniques qui respectent les droits fondamentaux des utilisateurs. Les dispositions contenues dans le présent paragraphe visent, conformément à la loi, à informer le personnel du ministère de la défense des moyens mis en œuvre.

1. MISE EN ŒUVRE DE MESURES DESTINÉES À PRÉVENIR LA VIOLATION DES RÈGLES ÉDICTÉES PAR LE PRÉSENT CODE.

1.1. **Outil informatique.**

Le choix d'un équipement s'opère selon ses caractéristiques techniques et les besoins de l'administration notamment ceux spécifiés en matière de sécurité. Pour leur protection et parce que la sécurité couvre l'ensemble du système, les supports informatiques extérieurs font l'objet d'un contrôle de sécurité préalablement à leur utilisation.

1.2. **Système d'identification et d'authentification.**

Un paramétrage est mis en place par les administrateurs selon le profil du poste de travail et de l'utilisateur. Il prend en compte le niveau de confidentialité du système, l'habilitation de l'utilisateur et son besoin d'en connaître. L'accès à un système d'information classifié de défense ou sensible respecte le strict besoin d'en connaître de la personne.

L'utilisateur s'identifie et, le cas échéant, s'authentifie, ce qui permet au ministère de la défense de lui imputer ses actions.

1.3. **Inspections, contrôles et audits.**

Sont prévus et définis par voie d'instruction des inspections, des contrôles et des audits, effectués régulièrement afin de vérifier ou apprécier le niveau de sécurité des systèmes d'information.

Ils peuvent intervenir à différents échelons et font systématiquement l'objet d'une remontée de l'information au fonctionnaire de sécurité des systèmes d'information.

1.4. **Banque de connaissances.**

Il existe une base ministérielle d'incidents. Elle est essentiellement alimentée par les utilisateurs qui avisent leur responsable local de sécurité des systèmes d'information des incidents rencontrés. Ces responsables locaux remontent et traitent l'information avec les centres d'expertises du ministère.

1.5. **Filtrage du contenu des communications électroniques.**

Afin de lutter contre les contenus malveillants ou interdits, le ministère de la défense actionne des dispositifs chargés de l'examen, de l'analyse, du filtrage des communications électroniques (messages électroniques et pages Internet consultées).

Ces dispositifs automatiques, configurés spécialement pour ne pas violer la vie privée et le secret des correspondances, peuvent bloquer les éléments non conformes à la politique de filtrage (pièces jointes aux messages, téléchargement de fichiers trop volumineux, protocoles ou contenus non autorisés...). Ils contribuent :

- au fonctionnement efficace des systèmes d'information et de communication du ministère de la défense (évitent notamment l'encombrement et la saturation du réseau par un trafic improductif ou des courriels non sollicités) ;

- à la protection des systèmes d'information et de communication en détectant et contrant certaines attaques ;

- à la protection du patrimoine informationnel et du secret de la défense nationale.

Ces dispositifs se situent à différents niveaux : sur les postes de travail, sur les passerelles et sur les réseaux du ministère de la défense. Ils sont conformes à la politique de sécurité des systèmes d'information.

Attention, les dispositifs de protection et de surveillance n'excluent pas une grande vigilance de la part de chaque utilisateur.

2. MISE EN ŒUVRE DE MESURES DESTINÉES À EFFECTUER UNE SURVEILLANCE A POSTERIORI.

2.1. **Conservation des données techniques, « logs ».**

Toute application informatique peut enregistrer les évènements associés au traitement d'un fichier, en y incluant la date et l'heure, laissant plus généralement des traces*.

Les traces d'accès aux données et aux ressources informatiques sont consignées via des mécanismes ou journaux du système pour permettre de détecter, d'imputer et de réagir a posteriori à toute utilisation non conforme (accidentelle ou intentionnelle) de l'un des composants du système. Ces traces techniques ou fonctionnelles peuvent être utilisées à des fins judiciaires ou pour résoudre des dysfonctionnements.

Tout enregistrement de données à caractère personnel, c'est-à-dire d'informations concernant des personnes identifiées ou identifiables, respecte la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés en faisant l'objet d'une déclaration auprès de la commission nationale informatique et libertés (CNIL).

Les données techniques sont conservées dans des conditions garantissant leur intégrité et leur confidentialité. Les fichiers de données techniques sont analysés régulièrement.

2.2. **Intervention judiciaire.**

Procureur de la République, juge d'instruction et officier de police judiciaire peuvent, sur réquisitions à l'autorité militaire, entrer dans un établissement militaire afin de constater des infractions ou rechercher des personnes ou des objets relatifs à celles-ci. Sauf nécessité, les réquisitions précisent la nature et les motifs des investigations jugées nécessaires. L'autorité militaire est tenue de s'y soumettre et se fait représenter. Le représentant est tenu au respect du secret de l'enquête et de l'instruction.

Les autorités judiciaires peuvent utiliser les traces informatiques conservées par le ministère de la défense.

2.3. **Pouvoir d'investigation de la commission nationale informatique et libertés.**

La commission nationale informatique et libertés dispose de pouvoirs d'investigation sous l'autorité et le contrôle du juge. Dans ce cadre, elle peut procéder à des vérifications ou obtenir des copies de tous documents ou supports d'information. Elle charge alors un ou plusieurs de ses membres ou agents, après en avoir informé le Procureur de la République, de se rendre entre 6H00 et 21H00 sur les lieux d'un traitement de données à caractère personnel, à l'exception des fichiers de souveraineté*. Si le responsable des lieux s'oppose à cette visite, le président du tribunal de grande instance devra alors l'autoriser, aux termes d'une ordonnance motivée.

Pour le ministre de la défense et par délégation :

L'ingénieur général des télécommunications,
directeur général des systèmes d'information et de communication,

Henri SERRES.

---

(1) Dans le respect des accords internationaux de sécurité.

(2) Tels que la contamination potentielle du système d'information, le risque d'affaiblissement du niveau de sécurité de l'ensemble, le risque de fuites de données etc.

(3) Données sur support amovible.

(4) Équipements.

(5) Prise de diagnostic, maintenance, intégration de données...

(6) Par exemple : "utilisateur" ou "administrateur".

(7) Accès au site, au bâtiment, à la pièce/bureau, au meuble renforcé ou coffre.

(8) À l'exception des postes devant être maintenus en activité en permanence, pour lesquels des procédures externes garantissant l'imputabilité des responsabilités sont instaurées.

(9) Mélanger lettres majuscules et minuscules, chiffres et, si possible, des caractères spéciaux, le mot de passe ne devant exister dans aucun dictionnaire.

(10) Selon des droits d'accès, des règles de filtrage et de stockage sûres.

(11) Issues en général des procédures d'exploitation de sécurité établies par le responsable SSI.

(12) Pris selon l'acception d'informations propres et privées liées à l'individu, la dénomination "personnel" du dossier pourra être complétée du nom de famille de l'agent.

(13) Une information classifiée est compromise lorsqu'une personne non habilitée ou n'ayant pas besoin d'en connaître est susceptible d'en avoir pris connaissance.

ANNEXE.

GLOSSAIRE.

ACSSI* : (article contrôlé de la sécurité des systèmes d'information).

Tout document, logiciel ou matériel qui, par son intégrité ou sa confidentialité, contribue à la sécurité d'un système d'information.

Administrateur*.

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 (secret professionnel), 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.

Authenticité*.

Conformité des qualités et du contenu du document, de l'auteur auquel on l'attribue et de sa prétendue ancienneté (horodatage) à la vérité.

Contenus malveillants*.

Selon leurs effets (atteinte à l'intégrité, à la disponibilité ou à la confidentialité), leur cible technique (fonctions de protection, système d'exploitation, client de messagerie, navigateur...) ou encore leurs propriétés (capacité de reproduction, de masquage, d'autoprotection, de déplacement autonome, d'auto extraction ou de diffusion massive ...), ils sont connus sous les noms génériques de virus, de chevaux de Troie, de bombes logiques, etc....

Fichier de souveraineté*.

Il s'agit des fichiers intéressant la sûreté de l'État, la défense nationale, la sécurité publique ou la répression pénale, ainsi que les fichiers utilisant le numéro d'inscription au répertoire national d'identification des personnes physiques ou portant sur la quasi-totalité de la population tels certains fichiers tenus par la direction générale de la sécurité extérieure (DGSE), la direction de la protection et de la sécurité de la défense (DPSD) ou encore la direction générale de la gendarmerie nationale (DGGN).

Fonctionnaire de sécurité des systèmes d'information*.

Les attributions du fonctionnaire de sécurité des systèmes d'information sont fixées par instruction ministérielle.

Forme des messages et contenu*.

Pour de plus amples informations sur le contenu et la forme de la correspondance électronique, l'utilisateur peut se référer à la Netiquette ou RFC 1855, un ensemble de règles de savoir-vivre sur l'Internet.

Habilitation*.

L'appréciation du « besoin d'en connaître » est fondée sur le principe selon lequel une personne ne peut avoir connaissance d'informations classifiées que dans la mesure où l'exercice de sa fonction ou l'accomplissement de sa mission l'exige. La procédure d'habilitation est déclenchée par l'employeur de la personne concernée. C'est à cette autorité que revient la responsabilité de déterminer en conformité avec le catalogue des emplois, le besoin, le type et le niveau de contrôle à effectuer, compte tenu notamment des informations classifiées dont la personne doit avoir connaissance.

Intradef*.

Réseau intranet du ministère de la défense traitant d'informations sensibles non classifiées de défense.

Intranet*.

Le ministère de la défense déploie des réseaux informatiques internes utilisant les technologies de communication d'Internet. Ces réseaux sont appelés intranets de manière générique.

Information*.

Renseignement ou élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement.

Information classifiée*.

L'information est classifiée lorsqu'elle intéresse la défense nationale et parce que sa divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Moyens de chiffrement*.

Dénommés parfois « moyens de cryptologie », les moyens de chiffrement sont des matériels ou des logiciels qui transforment, à l'aide de conventions secrètes, des informations ou des signaux clairs en informations ou signaux inintelligibles pour des tiers ou qui réalisent l'opération inverse. La fourniture, l'utilisation et l'exportation de ces moyens ou prestation de chiffrement sont réglementées.

Public* (accédant aux œuvres de l'esprit).

Ensemble indéterminé de personnes ayant accès à l'œuvre, sans qu'il soit nécessaire que ces personnes soient réunies ou prennent connaissance de l'œuvre en même temps.

Preuve*.

Il existe deux systèmes de preuve : celui de la liberté de la preuve (faits juridiques, droit administratif, droit commercial et droit pénal) et celui de la preuve dite « légale » (droit civil).

Les conséquences avec les nouvelles technologies sont :

- pour le système de la liberté de la preuve : sont admis tous les moyens de preuve, y compris le simple courriel. Les magistrats apprécient librement cette preuve ;

- pour le système de la preuve dite « légale » où la preuve repose sur la règle de l'écrit : l'écrit électronique est admis à titre de preuve [article 1316-4 du code civil (n.i. BO)] sous certaines conditions. Doivent être prouvés l'identité de la personne dont il émane, l'établissement et la conservation de la preuve numérique dans des conditions qui en garantissent l'intégrité.

Privilèges*.

Le terme de « privilège » fait référence, dans le présent code, aux droits plus étendus dont bénéficient les administrateurs.

Procédure de contrôle*.

Il s'agit pour l'utilisateur de confier l'objet du contrôle à l'officier de sécurité des systèmes d'information dont il dépend. Ce dernier s'assure de la stricte conformité de l'équipement candidat (innocuité du contenu, passage préalable par un sas, « dump » du disque dur...) par tout procédé ou procédure garantissant le respect des objectifs de sécurité (intégrité, disponibilité, confidentialité) du système d'information atteint, en présence du responsable de l'équipement.

Œuvre de l'esprit* (destinée au public).

Constituent des œuvres de l'esprit au sens du code de la propriété intellectuelle, les logiciels, bases de données et autres créations tels que cartes, articles de presse, photographies, pages Internet, films, etc.

Support amovible*.

Support informatique qui peut être enlevé ou remis à volonté. À la différence du support extractible, l'insertion d'un support amovible ne nécessite aucune intervention particulière sur le poste de travail. En effet, ce dernier possède une interface naturelle (physique et logique) pour accueillir les supports amovibles. Dans cette catégorie on peut citer la disquette, le CD-Rom et la clé USB.

Support informatique*.

Disque dur, disquette, CD-Rom, clé USB ou toute mémoire recevant, conservant et restituant l'information numérique.

Système d'information*.

Ensemble des moyens humains et matériels ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.

Traces*.

Elles désignent les données :

- relatives au trafic ou « données de connexion » *(Network based logs)* désignent toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, avec indication notamment des informations suivantes : origine, destination, itinéraire, heure, date, taille et durée de la communication ou type du service (réseau) sous-jacent ;

- de localisation, données traitées dans un réseau de communications électroniques (réseau de télécommunications), en plus de celles traitées en tant que données relatives au trafic au cours ou en vue d'une communication, indiquant la position géographique de l'équipement terminal d'un utilisateur d'un système informatique ;

- relatives aux systèmes informatiques enregistrées, stockées et conservées dans des fichiers, des bases de données, des mémoires, ...

Les traces sont aussi appelées données techniques ou fichiers log.

Utilisateur*.

Est dénommé utilisateur, tout personnel (permanent ou temporaire) ou toute personne (personnel d'une entreprise partenaire du ministère de la défense, fonctionnaire relevant d'un autre ministère...) qui, compte tenu de son habilitation ou de son besoin d'en connaître, dispose d'une autorisation d'accès (permanente ou temporaire) à un système d'information du ministère de la défense.

L'utilisateur veille à respecter la législation et réglementation en vigueur ainsi que les dispositions du présent code de bon usage. Il est responsable de l'usage et de la sécurité :

- des autorisations d'accès et des droits qui lui sont attribués, en permanence ou de façon temporaire ;

- des équipements qui lui ont été affectés ;

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

Les officiers et agents de police judiciaire, les inspecteurs de recherches du ministère, les administrateurs, les gestionnaires de réseaux et les auditeurs SSI sont soumis au présent code, lorsqu'ils utilisent les systèmes d'information mis à leur disposition par le ministère hors de toute mission particulière.