DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION :

INSTRUCTION N° 2004/DEF/DGSIC relative à la fonction d'administrateur de systèmes d'information et de communication au sein du ministère de la défense.

Du 14 décembre 2009

NOR D E F E 0 9 5 3 2 5 8 J

Précédent modificatif :

Autre du 07 août 2012 de classement.

Pièce(s) jointe(s) :

Une annexe.

Classement dans l'édition méthodique :

BOEM 160.1.1.

Référence de publication :
BOC N°2 du 15 janvier 2010, texte 1.

---

1. OBJET ET CHAMP D'APPLICATION.

Relevant hiérarchiquement de la voie commandement et fonctionnellement de différentes voies techniques, les administrateurs de systèmes d'information et de communication du ministère de la défense disposent - pour les besoins de leur mission - de droits particuliers leur donnant potentiellement accès à l'ensemble des informations traitées par les utilisateurs du système sans pour autant posséder le droit d'outrepasser le principe du « besoin d'en connaître ».

Ce principe s'applique tout particulièrement aux traitements :

- des informations relevant du secret de la défense nationale, ou classifiées de défense OTAN, Europe, coalition, etc... ;
- des informations sensibles pourvues de mentions de manipulation ou nécessitant un traitement discret (confidentiel médical, confidentiel personnel...) ;
- des données à caractère personnel (1) ;
- des fichiers ou courriers électroniques revêtant un caractère privé.

De la même façon, certains administrateurs ont en charge le paramétrage et l'exploitation des dispositifs de surveillance des réseaux et des systèmes mis en place par le ministère dans un but de protection, ce qui leur donne une visibilité sur les activités des utilisateurs de ces

systèmes.

Enfin, ils sont souvent les premiers témoins de situations ou d'incidents pouvant déboucher sur des poursuites disciplinaires ou judiciaires, comme le recel et la consultation de contenus prohibés ou l'intrusion dans un système d'information.

La présente instruction présente le cadre légal et réglementaire dans lequel doivent s'inscrire les actions d'administration des systèmes d'information mis en œuvre par le ministère de la défense, y compris en opérations extérieures et à l'étranger (dans le respect des accords internationaux).

Elle vient en prolongement du code de bon usage des systèmes d'information et de communication du ministère de la défense [IM_CODEUSAGE] et concerne directement les administrateurs de systèmes d'information ainsi que le personnel en charge du soutien des ressources informatiques du ministère, mais aussi le commandement et toute la chaîne hiérarchique impliqués dans la mise à disposition et le bon fonctionnement de ces ressources.

Il est recommandé que les directions et services incluent tout ou partie des principes exposés dans la présente instruction dans les cahiers des charges des marchés publics incluant des prestations d'administration de systèmes d'information pour le compte du ministère de la défense.

Un encadré rappelle pour la majorité des domaines, le principe ou la règle principale à retenir.

Dans le corps du texte, les mentions entre crochets [EXEMPLE] renvoient vers la liste des textes de référence située en fin de document.

Ce document a vocation à être mis à jour régulièrement. La direction générale des systèmes d'information et de communication (DGSIC) a, sous l'autorité du ministre de la défense, la responsabilité de la mise à jour de cette instruction ministérielle.

À ce titre, les remarques formulées par les différents utilisateurs devront être adressées à la DGSIC, sous couvert de leur hiérarchie.

2. LES ADMINISTRATEURS.

2.1. **Rôle et organisation du ministère.**

L'administrateur est la personne chargée de gérer tout ou partie d'un système d'information et de communication en assurant sa mise en œuvre, sa disponibilité, son optimisation et son maintien en condition opérationnelle par des interventions techniques préventives et correctives. Il peut être amené, le cas échéant, à communiquer auprès des utilisateurs.

L'administrateur tient en outre à jour la documentation technique et les configurations de tous les composants du système d'information.

Selon la partie du système d'information gérée, il peut s'agir (liste non exhaustive) :

- d'un administrateur de services communs ou dédiés ;
- d'un administrateur de bases de données ou de progiciel de gestion intégré ;
- d'un administrateur système ;
- d'un administrateur de site Web (Intranet, Internet…) ;
- d'un administrateur réseaux (LAN, MAN, WAN…) ;
- d'un administrateur de système de communication (PABX, IPBX…) ;
- d'un administrateur de sécurité.

Conformément aux dispositions ministérielles relatives à la sécurité des systèmes d'information et à la lutte informatique défensive [IM_LID], trois « voies » interagissent avec la fonction de l'administrateur :

- la voie commandement (ou voie opérationnelle) ;
- la voie fonctionnelle SSI ;
- la voie technique SSI.

Tout administrateur relève hiérarchiquement de sa voie commandement.

Pour autant, pour conduire ses actions quotidiennes, l'administrateur exécute les consignes issues des autres voies subordonnées à la voie commandement :

- la voie fonctionnelle SSI pour ce qui concerne l'application des mesures de sécurité préventives ou curatives, le maintien en condition de sécurité, et la remontée d'informations dans le cadre de la lutte informatique défensive ;
- les différentes voies techniques, dont la voie technique SSI pour ce qui concerne les demandes d'expertise et d'assistance en matière de SSI.

Outre les voies techniques et fonctionnelles, les administrateurs sont également impliqués lors des inspections, contrôles et audits. Dans ce cadre, les administrateurs communiquent aux intervenants les informations nécessaires au bon déroulement des volets techniques de ces activités. Sous couvert de leur hiérarchie, ils se tiennent à disposition de l'autorité qui réalise l'inspection, le contrôle ou l'audit. Ils répondent aux questions relatives à leur domaine de compétence et ils donnent toute facilité pour le déroulement de ces activités.

2.2. **Attendus de la fonction.**

2.2.1. ***Compétence.***

Outre les formations techniques adaptées aux ressources matérielles et logicielles gérées,

chaque administrateur doit posséder et entretenir [2] régulièrement ses connaissances et son information dans les domaines suivants :

- la réglementation du ministère en matière de SSI ;
- la politique de sécurité du (des) système(s) servi(s) (dont PSSI et PES) ;
- les instructions techniques liées aux systèmes administrés ;
- le niveau d'alerte SSI et l'actualité de la menace.

Les administrateurs doivent également suivre les évolutions des lois et règlements (sécurité, CNIL, ...), et plus généralement le domaine juridique des nouvelles technologies.

2.2.2. ***Principe de maîtrise des droits.***

Les droits particuliers attachés aux comptes de connexion de type « administrateur » ou « root » sont justifiés par le besoin inhérent à certaines actions d'administration des systèmes, et non attachés à l'administrateur en tant que personne. Ainsi, il est INTERDIT à l'administrateur de faire usage de ces droits à d'autres fins que celles de sa mission.

Le compte « administrateur » ou « root » n'est attribué qu'au responsable de l'équipe d'administration qui ne l'utilise qu'en dernier recours. Dans le cadre de leurs fonctions, tous les administrateurs utilisent un compte individuel [3] pourvu des privilèges d'administration [4].

Lorsque l'utilisation de droits particuliers n'est pas nécessaire, les administrateurs s'identifient sur le système d'information avec un profil « utilisateur ».

Dans tous les cas (utilisation d'un profil « administrateur » ou d'un profil « utilisateur »), les administrateurs respectent l'instruction ministérielle portant code de bon usage des SIC du MINDEF [IM_CODEUSAGE].

2.2.3. ***Principe de moindre gêne.***

Les opérations d'administration doivent être conduites de manière à maintenir au maximum la continuité du service rendu aux utilisateurs.

Lorsque l'intervention de l'administrateur (planifiée ou pas) peut avoir une influence sur le service rendu par le système, il doit intégrer au maximum les contraintes opérationnelles [5] en recueillant l'autorisation de sa hiérarchie et en avertissant les utilisateurs avec un préavis et une information suffisants (conséquences, date et heure de début et de fin prévue de l'intervention).

Dans tous les cas, l'administrateur qui doit interrompre tout ou partie du service rendu aux utilisateurs limite la gêne occasionnée en réduisant autant que possible la durée et la fréquence de ces interruptions et en choisissant des plages horaires adaptées.

2.2.4. ***Principes de confidentialité.***

Bien que la fonction d'administrateur ne soit pas soumise à l'obligation de « secret professionnel » s'imposant à certaines professions [(6)] détentrices de secrets délibérément confiés par des tiers, l'administrateur est soumis à un devoir de discrétion propre à sa fonction et au milieu dans lequel il exerce.

Néanmoins, il ne peut pas se prévaloir d'obligation de secret dans des domaines autres que ceux prévus par la loi :

2.2.4.1. *Le secret de la défense nationale.*

Bien que les administrateurs ne soient pas en général destinataires à titre personnel d'informations revêtant un caractère de secret de la défense nationale, ils ont par fonction un accès potentiel à l'ensemble des informations de ce type traitées par le système d'information.

Aussi, dans le cas où ce dernier manipule des données classifiées de défense, l'administrateur ne doit ni consulter, ni divulguer, ni imprimer, ni reproduire, ni détruire illégitimement l'information [CP Art. 413-10]. La copie électronique est autorisée uniquement dans le cadre d'un plan de sauvegarde officiel.

Afin de tenir compte de leurs droits particuliers et de l'effet cumulatif des informations accessibles, les administrateurs doivent être habilités au niveau immédiatement supérieur (limité à SD dans un cadre national ou COSMIC TOP SECRET dans un cadre OTAN) au niveau de classification du système administré [I_133 - PER.R 4].

Ainsi :

- seul un administrateur disposant d'une habilitation correspondant au niveau secret défense peut administrer un système traitant d'informations classifiées confidentiel défense ou secret défense ;
- seul un administrateur disposant d'une habilitation correspondant au niveau confidentiel défense peut administrer un système traitant d'informations non classifiées de défense.

En outre, selon les fonctions occupées (administrateur de sécurité notamment), une décision d'accès SSI (admission ou agrément) peut être nécessaire [D_911].

2.2.4.2. *La discrétion professionnelle.*

Cette notion désigne l'obligation instituée, dans l'intérêt du service, pour protéger les informations de l'administration dont la divulgation pourrait nuire au bon fonctionnement de ses tâches. Le non respect de cette obligation, hormis dans les cas expressément prévus par la loi ou sous couvert de l'autorité dont dépend l'agent, l'expose à des sanctions disciplinaires

([CODE_D Art. L. 4121-2] et [STAT_F Art. 26]).

2.3. **Relation avec les utilisateurs.**

Les règles et procédures d'administration des systèmes d'information et de sécurité servent en priorité à la mise en œuvre, au maintien, voire à l'amélioration de la qualité des prestations délivrées à l'utilisateur.

L'administrateur s'assure de la qualité du service rendu aux utilisateurs et contribue à leur soutien en liaison avec les autres intervenants, notamment par le transfert d'un minimum d'informations permettant aux utilisateurs d'utiliser le système en condition normale (processus de connexion, liste des outils et des ressources mis à leur disposition, modalités générales d'utilisation...) et de faire appel, le cas échéant, à une assistance (support d'assistance téléphonique).

2.4. **Responsabilités.**

Dans la majorité des cas, les fautes commises par les administrateurs en qualité d'agents de l'État - civils ou militaires - sont des fautes de service, c'est à dire imputables à l'exercice de la fonction et engageant donc la responsabilité de la personne publique et non la responsabilité personnelle de l'agent.

Cependant, l'administrateur peut engager sa responsabilité propre en cas de faute personnelle, c'est à dire :

- de faute dépourvue de tout lien avec le service ;
- exemple : utilisation de l'expérience acquise dans les fonctions pour se livrer à des actes de piratage informatique dans la vie privée....
- de faute commise en dehors de l'exercice des fonctions mais non dépourvue de tout lien avec elles ;
- exemple : utilisation d'outils d'administration ou autres moyens à des fins personnelles...
- de faute commise dans l'exercice des fonctions mais revêtant une particulière gravité ou jugée inexcusable ;
- exemple : agissements motivés par des préoccupation d'ordre privé (volonté de nuire, détournement d'argent....), comportements manifestement excessifs (excès de boisson....), négligences graves (compromission d'un document classifié de défense...)....

En outre, les administrateurs peuvent également être pénalement condamnés pour des faits non intentionnels commis dans l'exercice de leurs fonctions s'il est établi qu'ils n'ont pas accompli les diligences normales compte tenu de leurs compétences, du pouvoir et des moyens dont ils disposaient ainsi que des difficultés propres aux missions que la loi leur confie et qu'ils ont contribué à créer une situation qui a permis la réalisation d'un dommage ou qu'ils n'ont pas

pris les mesures permettant de l'éviter ([CP-Art. 121-3], [CODE_D Art. L. 4123-11] et [STAT_F-Art. 11 bis A]).

Dans tous les cas, les fautes personnelles commises par les administrateurs peuvent les exposer à des sanctions disciplinaires ([CODE_D Art. L. 4137-1], [STAT_F-Art. 29]).

Toutefois, conformément à [CODE_D Art. L. 4122-1] et [STAT_F Art. 28], tout agent public a le devoir de refuser d'obéir à un ordre manifestement illégal et de nature à compromettre gravement un intérêt public (conditions cumulatives) sans qu'aucune sanction disciplinaire ne puisse être retenue contre lui.

2.5. **Conduite à tenir.**

Au regard de ces responsabilités, les administrateurs doivent respecter strictement les principes de base suivants :

- l'administrateur doit toujours agir dans le seul intérêt du maintien en condition opérationnelle - et en particulier du niveau de sécurité - du système géré et dans le strict respect de la confidentialité (cf. 2.2.4) des informations qu'il est amené à connaître, de la réglementation et des droits qui lui sont alloués ;
- l'administrateur doit appliquer les politiques d'exploitation de sécurité (PES) attachées aux systèmes d'information et de communication dont il a la charge de la mise en œuvre et rendre compte de toute difficulté d'application. À défaut de PES, il applique, sous couvert de l'autorité d'emploi responsable du système d'information, voire de l'autorité qualifiée concernée, les règles générales de sécurité correspondant à l'environnement d'exploitation prescrit (intranet sensible, classifié, Internet...) ;
- les principales actions d'administration doivent être consignées soit de manière automatique, soit de manière manuelle, afin que le cours des évènements puisse être au besoin fidèlement retracé ;
- tout incident [7] constaté ou supposé [8] sur le système d'information, tout manquement aux règles de [IM_CODEUSAGE] ainsi que tout risque potentiel doit faire rapidement l'objet d'un compte rendu à la voie commandement d'une part et à la voie fonctionnelle SSI d'autre part ;
- en cas de découverte de crimes ou de délits, ceux-ci doivent être rapportés sans délais - soit directement sans omettre un compte-rendu hiérarchique à l'issue, soit par l'intermédiaire de la voie hiérarchique - à la gendarmerie ou aux services de police [CPP Art. 40].

Nota : si l'administrateur venait à prendre illégalement connaissance de faits infractionnels, il serait lui-même répréhensible d'une infraction pénale pour violation du secret de la vie privée ou des correspondances (voir point 3.3.).

En cas de requête officielle, l'administrateur a l'obligation de remettre à l'autorité judiciaire (procureur de la république ou officier de police judiciaire) ou à l'autorité militaire destinataire de la requête toute information non classifiée susceptible d'intéresser une enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives [CPP-Art. 60-1 et 60-2].

Dans le cas de supports couverts par le secret de la défense nationale, l'autorité judiciaire peut saisir les supports et les mettre sous scellés aux fins de remise ou de transmission au président de la commission consultative du secret de la défense nationale qui doit en assurer la garde. Il revient alors à l'autorité judiciaire de demander la déclassification et la communication des éléments ainsi placés sous scellés [CPP-Art 56-4] et [CODE_D-Art. L. 2312-1 et suivants].

3. L'ADMINISTRATION DES SYSTÈMES D'INFORMATION.

En vertu de son pouvoir de direction et dans le cadre des lois en vigueur, le ministère de la défense dispose d'un pouvoir de contrôle sur les moyens informatiques mis à la disposition de ses agents et, plus généralement, sur leur activité. Ce pouvoir s'accompagne néanmoins de principes à respecter strictement :

3.1. **Principes applicables aux outils de surveillance des réseaux supports et systèmes.**

L'instruction ministérielle [IM_CODEUSAGE] informe les utilisateurs de la possible mise en place d'outils de surveillance des réseaux et des systèmes au sein du ministère.

Dans le cas où ces outils de surveillance recueillent des données à caractère personnel, leur traitement est strictement soumis aux principes suivants issus de [L_INFLIB] :

- déclaration préalable à la CNIL ;
- principe de finalité et de non détournement des traitements : les données ne sont recueillies et traitées que pour un usage déterminé et légitime ;
- principe de proportionnalité : la surveillance effectuée et les dispositifs mis en place sont proportionnés au but recherché ;
- principe de durée limitée de conservation des données ;
- principe de sécurité et de confidentialité des données ;
- principe du respect des droits des personnes : informations des personnes, droit d'accès, de rectification et d'opposition le cas échéant.

3.2. **Principes applicables aux outils de prise de contrôle à distance.**

L'administration des systèmes d'information peut nécessiter ou être facilitée par la mise en

œuvre d'outils de prise de contrôle à distance.

L'usage de ces outils à de strictes fins de maintenance informatique n'est pas soumise à déclaration à la CNIL.

En revanche, leur utilisation à des fins de contrôle sans déclaration à la CNIL est illicite, car ni conforme au principe de proportionnalité, ni respectueuse du principe de finalité posés par [L_INFLIB].

L'utilisation de ces outils doit être entourée de précautions afin de garantir la transparence dans leur emploi et la confidentialité des données auxquelles l'administrateur accédera par ce moyen, dans la stricte limite de ses besoins :

- les outils d'administration à distance utilisés doivent être approuvés par l'autorité qualifiée dont dépendent les administrateurs ;
- l'accès au(x) compte(s) utilisateur(s) sera limité au strict besoin des opérations de maintenance ;
- les conditions d'intervention des administrateurs doivent être portées à la connaissance des utilisateurs au titre de l'obligation de transparence à la charge du ministère ;
- l'utilisateur doit être informé de la date et heure de l'intervention à distance et doit pouvoir donner son accord par acquittement au moment de la connexion, ou à défaut, par un accord de principe via la messagerie ;
- dans les cas de force majeure [(9)] où l'intervention doit être faite en l'absence de l'utilisateur, celle-ci sera effectuée sous couvert de la voie hiérarchique ou la voie fonctionnelle SSI qui s'assurera du caractère d'urgence ainsi que du bien fondé des interventions et qui informera l'utilisateur des actions entreprises dans les meilleurs délais ;
- l'administrateur doit s'assurer de la traçabilité des opérations de maintenance ;des mesures de sécurité doivent être prises pour garantir la confidentialité des flux entre le poste de l'administrateur et des utilisateurs, ainsi que celle des informations auxquelles les administrateurs ont accès ;
- les postes de travail des administrateurs permettant une prise de contrôle à distance sur d'autres ordinateurs sont sécurisés, et notamment protégés contre le risque d'intrusion.

3.3. **Respect de la correspondance et de la vie privée.**

L'utilisation à des fins personnelles des systèmes d'information du ministère par les agents est tolérée selon les limites fixées par [IM_CODEUSAGE], et notamment sous réserve que le système ne soit pas classifié, et que cette utilisation reste exceptionnelle et sans impact sur le bon fonctionnement général du système ou sur la bonne marche du service.

Le régime juridique - et donc les règles de manipulation par l'administration - des messages ou fichiers dépendant de leur caractère professionnel ou privé, il est du ressort des utilisateurs de

faire apparaître dans l'objet ou le titre des messages ou des dossiers le terme « personnel » afin de concrétiser leur droit à la vie privée [IM_CODEUSAGE].

Sans mention explicite « personnel », tout message envoyé ou reçu depuis le poste de travail professionnel d'un utilisateur du ministère, ainsi que les fichiers déposés sur les espaces de stockage mis à sa disposition revêtent, par défaut, un caractère professionnel. Le ministère de la défense peut donc y accéder librement (10), en ou hors présence de l'agent.

Les mails identifiés comme personnels - de par leur dénomination ou leur classement (11) - sont en revanche protégés par le secret de la correspondance [L_SECCOR]. Leur ouverture et/ou leur destruction par l'administration est sanctionnée pénalement [CP Art. 432-9].

Au titre du respect de la vie privée, les dossiers identifiés comme personnels sont quant à eux protégés par le code civil [CC Art. 9].

Toutefois, dans les cas où le maintien en condition de sécurité du système d'information considéré l'exige, l'accès aux dossiers ou mails revêtant la mention « personnel » peut être opéré par les outils automatiques (antivirus notamment) ou les administrateurs eux-mêmes.

Dans ce cas, l'accès aux dossiers ou mails personnels de l'agent par l'administrateur doit se faire en présence de l'agent, sauf cas de force majeure.

En tout état cause, tous les moyens nécessaires doivent être mis en œuvre pour informer l'agent préalablement à l'intervention de l'administrateur (12). Cette intervention n'autorise en aucune manière l'administrateur à révéler à quiconque le contenu des fichiers personnels, en dehors des cas de découvertes de crimes et de délits.

Les connexions Internet établies par les agents au moyen des postes mis à leur disposition par le ministère sont présumées avoir un caractère professionnel, de sorte que l'administration peut en consulter librement l'historique aux fins d'identification.

Dans le cas du départ des agents de leur organisme d'emploi, il est recommandé que les organismes formalisent le processus de prise en compte de ces départs, et en particulier les modalités d'information (13) des utilisateurs relatives à la fermeture technique de leur(s) compte(s) informatique(s) et à la destruction des données à l'issue.

Dans tous les cas, il est du ressort de l'utilisateur « quittant » de remettre à son successeur toutes les données électroniques (fichiers, mails...) nécessaires à la continuité de la mission [IM_CODEUSAGE] et de supprimer ses données à caractère personnel de tous les espaces de stockage mis à sa disposition.

3.4. **Téléphonie, vidéo surveillance et visio-conférence.**

L'installation et l'exploitation de systèmes dédiés à la capture et/ou l'enregistrement d'images ou de conversations à des fins de surveillance, de preuve, de formation, d'évaluation ou de tout autre motif font l'objet d'un cadre juridique strict basé sur les principes issus de [L_INFLIB], notamment les principes de proportionnalité entre le dispositif envisagé et les buts poursuivis, d'information préalable des intéressés et de respect des conditions d'exploitation.

En particulier, les informations issues de ces dispositifs ne doivent être consultées que par le personnel habilité, formé et investi d'une mission de surveillance ou de contrôle, ce qui exclut normalement le personnel administrateur.

Si un administrateur venait exceptionnellement [(14)] à prendre connaissance du contenu des enregistrements pour des motifs légitimes de maintien en condition de sécurité du système, les principes exposés précédemment lui interdisent de divulguer les informations qu'il aurait été ainsi amené à connaître.

S'agissant de la surveillance courante des relevés téléphoniques, les quatre derniers chiffres de ces numéros doivent être occultés sur les relevés d'appels. Cependant, dans les cas exceptionnels (utilisation manifestement abusive par exemple), les supérieurs hiérarchiques peuvent accéder aux numéros complets.

Cas particulier : toute utilisation des informations issues de l'utilisation des services de téléphonie pour un contrôle des appels émis et reçus par les représentants syndicaux dans le cadre de leur mandat est interdite.

3.5. **Traitement des dysfonctionnements et des incidents de sécurité.**

3.5.1. ***Généralités.***

Dans le cadre de leurs fonctions, les administrateurs peuvent être alertés sur des dysfonctionnements ou des incidents de sécurité touchant le système d'information :

- les dysfonctionnements regroupent toutes les défaillances physiques ou logiques rencontrées sur le système, voire sur les servitudes indispensables à son bon fonctionnement (énergie, climatisation....). L'administrateur réagit alors selon les consignes propres au système concerné ;
- les incidents de sécurité regroupent tous les faits ou événements volontaires ou involontaires, issus d'un utilisateur légitime ou non, voire d'un système externe, et portant atteinte à la sécurité du système administré ou au respect de la loi.

Un administrateur constatant un incident de sécurité prend immédiatement les mesures permettant :

- de faire cesser l'incident actuel [15] [ainsi que ses éventuels effets ultérieurs [16]] en cohérence avec le besoin opérationnel qui reste prioritaire ;
- de recouvrer le niveau de sécurité nominal du système ;
- d'assurer la continuité de service, au besoin en mode dégradé.

Il rend compte sans délai à la voie commandement et à la voie fonctionnelle SSI (selon les règles énoncées dans le point 3.3) des faits constatés et des actions conduites.

En outre, certains incidents pouvant déboucher sur des poursuites disciplinaires ou judiciaires (intrusions ou tentatives d'intrusion, attaques de systèmes tiers par rebond sur les systèmes du ministère, recel et consultation de contenus prohibés...), l'administrateur prend les mesures adaptées (cf. point « infra ») afin de préserver les éléments de preuve de l'action malveillante.

3.5.2. ***La préservation des preuves.***

La preuve est la démonstration de la réalité d'un fait, d'un état, d'une circonstance ou d'une obligation. Elle a pour finalité soit d'apporter des éléments contradictoires aux faits reprochés, soit d'affirmer les allégations et ainsi d'aider le juge à se forger une intime conviction, ou le commandement à apprécier l'opportunité d'une éventuelle sanction ou action en justice.

L'administrateur doit agir rapidement, et si possible en présence d'un représentant de la voie fonctionnelle SSI en qualité de témoin, afin de fixer la preuve dans le temps et d'éviter sa disparition ou son altération. À ce titre, les actions suivantes sont à mener sans délais :

- déconnecter [17] le serveur, l'élément de stockage ou le poste client du réseau [18] afin d'éviter toute action d'effacement ou de modification de preuve postérieure à la découverte du délit ;
- éviter, dans la mesure du possible, d'éteindre l'équipement incriminé (cette opération pourrait avoir pour effet d'effacer les traces présentes en mémoire) ; si la machine doit cependant être éteinte, ne pas utiliser la fonction d'extinction du système mais débrancher le cordon d'alimentation ;
- verrouiller le(s) compte(s) du (des) utilisateur(s) incriminé(s), ainsi que l'accès aux comptes de messagerie (boîtes mails ou Webmails) ;
- ne pas connecter de supports amovibles (ce qui génèrerait des traces perturbatrices dans les journaux) ;
- restreindre l'accès physique à l'élément incriminé de manière à ce que personne ne modifie sa configuration avant l'intervention des services compétents ;
- noter, sur un journal de bord, l'ensemble des constatations faites et des actions effectuées de manière à assurer une traçabilité et un historique de l'incident en précisant :
- les dates et heures [heure système du poste et heure GMT « réelle » [19]] ;
- le nom des fichiers ou commandes exécutés ainsi que login et mot de passe utilisés si des

actions d'administration sont nécessaires ;

- préserver le plus grand nombre d'informations pertinentes pouvant compléter les investigations (supports de sauvegardes récentes, journaux d'évènements....).

Dans tous les cas, il y a lieu d'agir avec la plus grande discrétion et respecter le principe de présomption d'innocence. Selon le besoin, prétexter des opérations de maintenance pour justifier les opérations conduites.

Pour le ministre de la défense et par délégation :

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

Christian PÉNILLARD.

Notes

En cohérence avec le besoin opérationnel qui reste prioritaire. 17La continuité de service devra, le cas échéant, être assurée par la mise en œuvre d'un mécanisme de secours correctement configuré.18Ces heures peuvent être différentes en cas de désynchronisation de l'heure système.19