Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

BULLETIN OFFICIEL DES ARMEES

Edition Chronologique n°33 du 12 août 2010

PARTIE PERMANENTE
Administration Centrale

Texte n°2

DIRECTIVE N° 13/DEF/DGSIC
sur la sécurité des accès aux services de l'internet et la sécurité de l'hébergement des services internet du ministère.

Du *30 juin 2010*

DIRECTION GÉNÉRALE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION.

DIRECTIVE N° 13/DEF/DGSIC sur la sécurité des accès aux services de l'internet et la sécurité de l'hébergement des services internet du ministère.

Du 30 juin 2010

NOR D E F E 1 0 5 1 3 3 4 X

Pièce(s) Jointe(s) :

Trois annexes.

Classement dans l'édition méthodique : BOEM 160.1

Référence de publication : BOC N°33 du 12 août 2010, texte 2.

SOMMAIRE

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. Généralités.

1.2. Les usages.

1.3. Les risques.

1.4. Présentation de la directive.

1.5. Niveaux de préconisation.

1.6. Modalités d'application.

1.7. Gestion des dérogations.

2. CADRE DOCUMENTAIRE.

2.1. Documents applicables.

2.2. Normes et standards applicables.

3. DOMAINE COUVERT ET EMPLOI.

3.1. Services attendus.

3.1.1. Protéger le patrimoine applicatif et informationnel du ministère de la défense contre les menaces issues de l'internet.

3.1.2. Réduire la complexité des accès internet.

3.1.3. Différencier les accès aux services de l'internet.

3.1.4. Assurer une certaine discrétion des échanges vis-à-vis de l'extérieur.

3.1.5. Appliquer le principe de défense en profondeur.

3.1.6. Renforcer la culture de sécurité des utilisateurs.

3.1.7. Appliquer un contrôle des activités liées à l'internet.

3.1.8. Respecter les droits et libertés fondamentales des agents.

3.2. Périmètre et limites.

3.2.1. L'accès au réseau et services de l'internet.

3.2.2. Le prestataire chargé d'assurer l'hébergement des services internet.

3.2.3. Volet lutte informatique défensive.

3.2.4. Cas particuliers hors périmètre.

3.3. Interopérabilité et interfaçage.

4. LES RÈGLES.

4.1. Généralités et articulation.

4.2. Rappel.

4.3. Règles communes.

4.4. Règles relatives aux accès de première catégorie.

4.5. Règles relatives aux accès de seconde et de troisième catégorie.

4.5.1. Organisation.

4.5.2. Dispositif frontière de protection.

4.5.3. Administration.

4.5.4. Contrôle des activités.

4.6. Règles complémentaires aux accès de seconde catégorie.

4.6.1. Organisation.

4.6.2. Dispositif frontière de protection.

4.6.3. Administration.

4.6.4. Règles spécifiques aux postes privés.

4.7. Règles complémentaires aux accès de troisième catégorie.

4.7.1. Organisation.

4.7.2. Dispositif frontière de protection.

4.7.3. Administration.

4.8. Règles relatives aux accès de quatrième catégorie.

4.9. Règles relatives à l'hébergement des services internet du ministère.

4.9.1. Environnement.

4.9.2. Impératifs de sécurité.

4.9.3. Démarche de sécurité.

4.9.3.1. Règles générales.

4.9.3.2. Règles spécifiques à l'hébergement des services internet par le ministère.

4.9.3.3. Règles spécifiques à l'externalisation de l'hébergement des services internet du ministère.

5. GLOSSAIRE ET ACRONYMES.

6. RÉFÉRENCES.

ANNEXE(S)

ANNEXE I. ACCÈS AUX SERVICES DE L'INTERNET.

ANNEXE II. CLAUSES DE SÉCURITÉ COMPLÉMENTAIRES.

ANNEXE III. VISION SYNTHÉTIQUE DES RÈGLES PAR PRINCIPE.

1. PRÉSENTATION GÉNÉRALE ET GUIDE D'USAGE.

1.1. **Généralités.**

Internet est communément admis comme étant le réseau public mondial utilisant le protocole de communication internet protocol (IP). Il donne accès à des services d'échange tels que le courrier électronique et le World Wide Web.

Il se distingue par :

- une offre extensible de services en constante évolution ;
- un contrôle étatique réduit ;
- une grande facilité d'accès (coût d'accès réduit voire gratuit, nombreuses possibilités de raccordement filaires ou sans-fils...) ;
- une capillarité mondiale.

Ces trois dernières caractéristiques jouent aussi en faveur des parties adverses qui bénéficient d'un vecteur d'attaque puissant impliquant une dangerosité de ce réseau accrue par rapport à nos intranets.

Internet s'est considérablement développé pour être considéré aujourd'hui comme une infrastructure vitale de nos sociétés (1). Il constitue un nouveau monde de l'information, le « cyberespace » (2), encore en expansion et

en évolution. Cette révolution informationnelle introduit de nouveaux rapports, entre le ministère et le reste du monde, renforcés par le développement de l'économie numérique et l'arrivée du très haut débit.

1.2. **Les usages.**

Le ministère puise et met à disposition de l'information sur internet. En outre, en raison de besoins d'échanges d'informations accrus, d'accès à des téléservices ou de la dématérialisation obligatoire de certaines procédures (portail achats publics), l'utilisation des services du réseau mondial internet est devenue complémentaire de l'emploi des différents intranets déployés au sein du ministère. En particulier, son usage est de plus en plus étendu pour les activités professionnelles et à des fins personnelles, sur les théâtres d'opérations.

Le développement des usages et des technologies utilisées par internet est permanent. Internet bouscule les modes de pensée traditionnels et nécessite une adaptation perpétuelle des moyens et des processus nécessaires pour faire face aux évolutions des services proposés et des menaces induites. Ainsi, le conseil supérieur de la défense, comme indiqué dans son rapport [CSD], a recommandé la définition d'une doctrine d'emploi ambitieuse et réaliste de l'internet civil par le ministère.

1.3. **Les risques.**

En utilisant internet, le ministère prend le risque d'engager la sécurité de certaines de ses informations et de ses ressources, sa réputation et sa responsabilité.

- les informations.

Le ministère doit assurer au juste besoin, une protection des services ouverts qu'il utilise sur internet en termes de disponibilité, de confidentialité, d'intégrité et de preuve.

Certaines informations opérationnelles ou soumises à des dispositions légales ou réglementaires de protection de l'information (3) sont à protéger vis à vis d'un accès illicite depuis internet.

- les ressources.

Les ressources (4) du ministère de la défense, sans une mise en sécurité adéquate, peuvent faire l'objet d'intrusion et être détournées vers des activités malveillantes. Ces dernières peuvent cibler un service interne, nos applications ou un système extérieur au ministère (attaque par rebond).

- la réputation.

Le ministère de la défense porte l'héritage de la confiance dont il fait l'objet de la part de l'opinion française en matière de protection de son patrimoine. Il doit donc être au fait de l'état de l'art en matière de sécurité informatique et être exemplaire. Dès lors, une évaluation des risques insuffisante, permettant certaines attaques (5) pourrait nuire à son image.

- la responsabilité juridique.

Le ministère doit garantir un niveau de sécurité approprié aux données qu'il traite (6). La perte, destruction, l'altération de certaines de ces données peuvent engager la responsabilité du ministère et de ses agents (7). C'est également le cas si, par manque de mesures de sécurité adéquates, un intrus introduit des données à caractère illégal ou conduit des attaques à partir d'une ressource ou d'une application du ministère. La responsabilité peut également être mise en jeu en cas d'activité illicite des agents du ministère sur internet (téléchargement illégal, consultation de sites illicites, diffamation, injures, racisme...).

Il est dès lors nécessaire de se doter de capacités pour protéger nos systèmes et limiter au niveau nécessaire (8) les risques de voir notre responsabilité et celle de nos agents engagée.

1.4. **Présentation de la directive.**

Sans attendre la rédaction d'une doctrine d'emploi, cette directive traduit de façon concrète quelques règles de sécurité d'usage lorsque le ministère de la défense permet à son personnel de se connecter à l'internet ou d'utiliser des services de l'internet. Elle complète l'instruction ministérielle [IM8192] relative aux modalités d'accès et de raccordement à l'internet. Elle précise les principes, les buts et les objectifs ainsi que les moyens généraux pour y parvenir.

La présente directive a pour objectif de limiter les risques du ministère de la défense exposés au point 1.3. À cette fin, la directive :

- apporte aux autorités offrant un accès aux services de l'internet une information sur les exigences de sécurité et de mise en œuvre ;

- définit le socle des exigences de sécurité concernant l'hébergement des services internet du ministère (9) .

Elle s'inscrit dans les missions de la direction générale des systèmes d'information et de communication (DGSIC) aux termes du décret n° 2006-497 du 2 mai 2006 portant création de la DGSIC et fixant l'organisation des systèmes d'information et de communication du ministère de la défense.

1.5. **Niveaux de préconisation.**

Les règles définies dans ce document ont différents niveaux de préconisation et sont conformes au [RGI] et à la [RFC 2119] :

- obligatoire : ce niveau de préconisation signifie que la règle édictée indique une exigence absolue de la directive ;

- recommandé : ce niveau de préconisation signifie qu'il peut exister des raisons valables, dans des circonstances particulières, pour ignorer la règle édictée, mais les conséquences doivent être comprises et pesées soigneusement avant de choisir une voie différente ;

- déconseillé : ce niveau de préconisation signifie que la règle édictée indique une prohibition qu'il est toutefois possible, dans des circonstances particulières, de ne pas suivre, mais les conséquences doivent être intégrées et le cas soigneusement apprécié ;

- interdit : ce niveau de préconisation signifie que la règle édictée indique une prohibition absolue de la directive.

1.6. **Modalités d'application.**

Ces règles sont applicables à tout nouveau projet ou raccordement de nouveaux postes. Elles seront prises en compte par les systèmes existants au fur et à mesure de leurs évolutions dans un délai de 3 ans à compter de cette date.

Une autorité d'emploi peut inclure dans ses directives des conditions distinctes si celles-ci sont plus exigeantes que la présente directive.

Cette directive peut être précisée par des référentiels techniques et méthodologiques au sein de chaque organisme. Les directions et services transposent les exigences de la présente directive dans les cahiers des charges des marchés publics impactés par la présente directive.

1.7. **Gestion des dérogations.**

Les dérogations aux règles recommandées ou déconseillées font l'objet d'une saisine de la DGSIC par l'organisme responsable de la sécurité. Les cas structurants sont débattus en commission ministérielle spécialisée des SIC (CMSSI, CMTSIC). Il n'est pas possible de déroger aux règles obligatoires ou interdites.

2. CADRE DOCUMENTAIRE.

2.1. **Documents applicables.**

Code pénal (n.i. BO).

Code des postes et des communications électroniques (n.i. BO).

Code de la santé publique (n.i. BO).

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Ordonnance n° 2005-1516 du 8 décembre 2005 [ORD] relative aux échanges entre les usagers et les autorités administratives et entre les autorités administratives.

Décret n° 2007-207 du 19 février 2007 relatif aux attributions des hauts fonctionnaires de défense et de sécurité [DFSSI].

Référentiel général d'interopérabilité [RGI] et référentiel général de sécurité [RGS] (n.i. BO).

Arrêté du 9 novembre 2009 portant approbation du référentiel général d'interopérabilité (n.i. BO).

Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques (n.i. BO).

Directives DGSIC (n.i. BO).

Instruction 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 [IM4418].

Instruction n° 1829/DEF/CAB/CM/3 du 19 janvier 1999 relative à la charte de nommage internet du ministère de la défense [IM1829].

Instruction n° 1830/DEF/CAB/CM/3 du 19 janvier 1999 relative à la mise en œuvre de services en ligne ou de sites internet par les états-majors, directions et services du ministère de la défense [IM1830].

Instruction n° 133/DEF/SEC/DIR/SIC du 18 mars 2002 relative à la politique de sécurité des systèmes d'informations du ministère de la défense [IM133].

Instruction n° 8192/DEF/SEC.DIR.SIC du 30 juin 2003 relative aux modalités d'accès, de raccordement et d'utilisation des réseaux externes au ministère de la défense [IM8192].

Instruction n° 2003/DEF/DGSIC du 20 novembre 2008 portant code de bon usage des systèmes d'information et de communication du ministère de la défense [IMCODE USAGE].

Instruction n° 486/DEF/DGSIC du 24 juillet 2007 relative aux attributions du fonctionnaire de sécurité des systèmes d'information [IM486].

Guide n° 830/SGDN/SCSSI/SI du 11 décembre 1998 relatif à l'internet et la sécurité [G830] (n.i. BO).

2.2. **Normes et standards applicables.**

ISO/CEI 27001 : technologies de l'information – techniques de sécurité – systèmes de gestion de la sécurité de l'information – exigences.

ISO/CEI 27002 : technologies de l'information – techniques de sécurité – code de bonne pratique pour la gestion de la sécurité de l'information.

ISO/CEI 27005 : technologies de l'information – techniques de sécurité – gestion du risque en sécurité de l'information.

ISO 20000-1 : norme internationale traitant de la gestion des services informatiques. Elle s'appuie sur les recommandations ITIL.

3. DOMAINE COUVERT ET EMPLOI.

3.1. **Services attendus.**

Ce chapitre décrit les principales fonctions et principes qui doivent prévaloir pour les accès aux services de l'internet.

Un système peut être connecté au réseau internet de deux façons :

- soit directement. Le système est dit « dédié » (10). Il n'est connecté qu'au réseau internet ;

- soit depuis un intranet de la défense par l'intermédiaire de segments d'interface sécurisés. Le système est dit « mutualisé ou partagé ».

3.1.1. ***Protéger le patrimoine applicatif et informationnel du ministère de la défense contre les menaces issues de l'internet.***

La France peut faire l'objet d'agressions directes ou indirectes au travers de frappes massives ou ciblées. Le ministère de la défense n'est pas épargné par des attaques informatiques et constitue une cible de choix pour les attaquants informatiques de tout bord. Il connait une progression importante de ses besoins professionnels d'accès à des services ouverts sur l'internet qu'il tente de satisfaire au mieux en multipliant les contrats avec des partenaires extérieurs. Dès lors, le ministère se doit de réduire les vulnérabilités de ses systèmes ouverts sur l'internet et de réagir efficacement aux attaques informatiques.

Par ailleurs, le ministère doit se doter de centres d'hébergement de données durcis à la menace et en nombre réduit afin de concentrer les efforts de sécurité.

3.1.2. ***Réduire la complexité des accès internet.***

La multiplication des accès dédiés aux services de l'internet impose au ministère un effort important de sécurisation. Dans un souci d'optimisation des ressources financières, matérielles et humaines, il convient d'adapter les architectures de sécurité des accès au réseau internet au juste besoin et d'optimiser leur maintien en condition de sécurité (MCS).

Le ministère doit centraliser les accès aux services de l'internet afin de permettre la concentration des efforts de sécurité.

3.1.3. ***Différencier les accès aux services de l'internet.***

Accéder aux services de l'internet impose de disposer des éléments suivants :

- un point d'accès [11] ;

- des équipements de desserte (équipement réseau) ;

- un poste terminal.

Le point d'accès est sous maîtrise du fournisseur d'accès internet (FAI). Par contre, les équipements de desserte et les postes terminaux peuvent être mis en œuvre (au sens installés et exploités) soit par un prestataire externe au ministère soit par le ministère lui-même.

Les mesures de sécurité diffèrent selon que la desserte est mise en œuvre par un prestataire ou par le ministère.

En outre, les points d'accès aux services de l'internet sur un site de la défense sont classés en quatre catégories. Les trois premières catégories fixent un cadre d'accès aux services de l'internet au profit du personnel de la défense. D'autres cas d'emploi peuvent apparaître. Ils s'inscrivent dès lors dans la quatrième catégorie. Un tableau récapitulatif est joint en annexe I.

- première catégorie :

  - tout accès faisant l'objet d'un contrat de droit privé entre un FAI (ou prestataire privé) et un agent du ministère ;

  - tout accès faisant l'objet d'un marché conclu par la défense dont la mise en œuvre jusqu'à la desserte des postes terminaux incombe au prestataire privé.

Cette catégorie concerne toute forme d'usage privé d'internet dans une enceinte défense, en métropole, outre-mer, à l'étranger ou en OPEX faisant appel à l'utilisation :

  - de postes privés mis en œuvre par leur propriétaire pour une utilisation détachable du service, à titre privé ;

  - de postes informatiques mis en œuvre par un prestataire dans le cadre d'un marché de délivrance de services internet (exemple : bornes internet à accès gratuit ou onéreux).

L'utilisation d'un poste privé peut être élargie exceptionnellement à un usage professionnel dans le cadre de mesures d'un plan de continuité d'activité (par exemple en cas de pandémie).

- deuxième catégorie : tout accès faisant l'objet d'un marché conclu par la défense dont la mise en œuvre de la desserte jusqu'au poste client incombe au ministère.

Cette catégorie concerne toute forme d'usage professionnel d'internet dans une enceinte défense, en métropole, en outre-mer, à l'étranger ou en OPEX et d'usage privé [12] lié à l'amélioration du bien-être des personnels de la défense faisant appel à l'utilisation :

  - de postes informatiques mis en œuvre par le ministère dans le cadre de systèmes dédiés ou mutualisés ;

  - de postes privés dans le cadre de systèmes dédiés à l'internet, mais dont le propriétaire est issu du personnel de la défense.

Les postes concernés sont généralement connectés en réseau et partagent le même accès internet.

L'autorisation de connexion d'un poste privé sur un réseau à vocation internet avec un accès de deuxième catégorie est soumise à une décision de commandement.

- troisième catégorie : tout accès faisant l'objet d'un marché conclu par la défense pour toute forme d'usage professionnel d'internet en métropole, en outre-mer, à l'étranger ou en OPEX utilisant des technologies de mobilité.

L'accès s'effectue par l'emploi d'un module externe (13) ou interne (14) reliant un poste terminal appartenant au ministère à un opérateur connecté à l'internet.

- quatrième catégorie : tous les cas n'entrant pas dans les trois premières catégories.

3.1.4. ***Assurer une certaine discrétion des échanges vis-à-vis de l'extérieur.***

L'accès aux informations doit pouvoir être rendu le plus discret possible vis-à-vis de l'extérieur. De plus, dans un contexte stratégique, certaines recherches ou communications par des acteurs (15) du ministère imposent l'anonymat.

3.1.5. ***Appliquer le principe de défense en profondeur.***

La défense en profondeur peut s'établir à trois niveaux.

a) Le premier niveau de défense est assuré par les fournisseurs d'accès internet.

b) Le deuxième niveau de défense se situe aux frontières de l'internaute ou des données. Il s'applique sur :

- les dispositifs frontières de protection placés aux points d'accès ;

- les postes terminaux mobiles ou fixes.

c) Le troisième niveau de défense est assuré par une protection au niveau des centres assurant l'hébergement des services internet du ministère (messagerie, sites ou applications WEB...) ou des services de l'intranet connectés à l'internet.

En outre, elle se décline selon cinq axes complémentaires.

1. Prévenir : éviter la présence ou l'apparition de failles dans les constituants des systèmes d'information. L'exposition à des vulnérabilités logicielles identifiées par les éditeurs doit être la plus réduite possible.

Il s'agit principalement de disposer d'équipements à jour de configuration, de respecter les directives ministérielles (notamment celles relatives aux postes terminaux, prévention contre les codes malveillants...) et de sensibiliser les utilisateurs potentiels à ces menaces. Ce dernier point est consolidé au point 3.1.6.

2. Bloquer : empêcher les attaques de parvenir jusqu'aux composants sensibles et potentiellement vulnérables du système d'information. Plus généralement, réduire les chances de succès des attaques même si elles ciblent des composants vulnérables.

Il s'agit principalement de s'appuyer sur des composants de sécurité déployés en série et répartis sur les trois niveaux identifiés.

3. Renforcer : limiter les conséquences de la perte d'intégrité de l'un ou l'autre des composants des systèmes d'informations.

Il s'agit principalement d'appliquer le principe du moindre privilège et d'augmenter la résilience de l'architecture de sécurité en mettant en œuvre des mécanismes redondants, complémentaires et qui se soutiennent mutuellement.

4. Détecter : pouvoir identifier, en vue d'y réagir, les incidents ou la perte d'intégrité survenant sur le système d'information.

Cette capacité nécessite la mise en œuvre d'outils de détection d'incidents de sécurité mais surtout une exploitation des journaux adaptée aux enjeux de sécurité.

5. Réparer : disposer de moyens pour remettre en fonctionnement le système d'information suite à un incident ou à une perte d'intégrité.

Les moyens mis en œuvre devront répondre aux besoins de disponibilité attendus.

3.1.6. ***Renforcer la culture de sécurité des utilisateurs.***

Un point faible de toute architecture de sécurité est l'utilisateur. Cette vulnérabilité doit être maîtrisée le plus possible sans pour autant réduire l'ergonomie indispensable attendue par les utilisateurs d'internet. Le personnel de la défense est néanmoins confronté à des menaces plus marquées lorsqu'il navigue sur la « toile » ou échange des données. Dès lors, il convient de l'en protéger et de l'informer par toutes les mesures nécessaires.
À ce titre, l'effort sur la sensibilisation des agents aux menaces de l'internet doit rester constant et régulier.

3.1.7. ***Appliquer un contrôle des activités liées à l'internet.***

Les faits dommageables accomplis par un agent public peuvent engager tant la responsabilité de l'État que celle de l'agent. Aussi, le ministère doit pouvoir être en mesure de réunir toute preuve permettant d'identifier les usages abusifs et/ou illégaux (téléchargement illégal, consultation de sites illicites, diffamation, injures, racisme...) afin d'engager *a posteriori* la responsabilité personnelle de l'utilisateur en faute et de dégager la responsabilité de l'administration.

Pour cela, le ministère doit contrôler la cyber-activité (16) des agents du ministère afin de prévenir et détecter toute attaque d'origine interne ou externe ainsi que tout contournement des directives de sécurité (présence et fuite de données confidentielles, présences de codes malveillants...) et du code de bon usage [IMCODE USAGE] qui peuvent mettre en défaut le ministère de la défense.

3.1.8. ***Respecter les droits et libertés fondamentales des agents.***

Le personnel du ministère de la défense peut exercer son droit d'expression et d'opinion (17) tout en respectant son devoir de réserve et de discrétion professionnelle. En outre, il ne doit porter atteinte ni à la loi, ni aux intérêts de la défense, ni à la sécurité ou au bon fonctionnement des systèmes d'information du ministère.

Aussi, nonobstant le caractère professionnel des postes de seconde ou troisième catégorie, les personnels de la défense bénéficient d'un espace de vie privée résiduelle dans le cadre du périmètre qui leur aura été accordé.

Les principes du secret des correspondances (18) et du respect des espaces privatifs sur le poste seront appliqués dans la limite des conditions fixées dans l'instruction ministérielle [IMCODE USAGE].

3.2. **Périmètre et limites.**

La directive est applicable à l'ensemble des organismes du ministère sauf cas particulier défini dans le point 3.2.4.

3.2.1. ***L'accès au réseau et services de l'internet.***

La présente directive s'attachera à détailler les règles applicables pour les systèmes connectés à l'internet que ce soit en métropole, en outre-mer, à l'étranger ou en opération extérieure (dans le respect des accords internationaux).

Les règles de sécurité liées à l'utilisation d'internet en tant que simple réseau de transport entre des réseaux d'organismes ou des utilisateurs isolés ne seront pas développées.

En outre, la réflexion s'est bornée à l'emploi de réseaux utilisant le protocole de transport de données IPv4 (19). La transition des réseaux vers l'IPv6 (20) devra conduire à vérifier la pertinence des règles définies dans la présente directive.

3.2.2. ***Le prestataire chargé d'assurer l'hébergement des services internet.***

L'hébergement et l'exploitation des services de l'internet est confié à un ou plusieurs prestataires. Ils peuvent être soit des organismes de la défense, soit des entreprises privées extérieures au ministère. La directive fixe le socle commun des règles de sécurité à respecter dans le domaine de l'hébergement.

3.2.3. ***Volet lutte informatique défensive.***

Le volet lutte informatique défensive (LID) ne sera que très légèrement abordé dans la mesure où il est pris en compte au travers de l'organisation permanente veille, alerte et réponse (OPVAR) du ministère.

3.2.4. ***Cas particuliers hors périmètre.***

Dans le cadre de leurs missions particulières, les services spécialisés (par exemple ceux du renseignement ou des services de lutte informatique), pourront déroger partiellement aux règles de cette directive sous la responsabilité de leur autorité qualifiée. Le FSSI (21), au titre du décret [DFSSI], sera informé de ces dérogations.

3.3. **Interopérabilité et interfaçage.**

La directive s'inscrit complètement dans une logique d'interopérabilité ministérielle voire interministérielle.

Certaines règles décrites dans ce document peuvent préciser ou compléter celles d'autres directives ministérielles dont notamment celles traitant de la prévention contre les codes malicieux et du poste terminal. Ceci est justifié car les règles de la directive ont pour objectif de couvrir le contexte de dangerosité accrue de l'internet. En cas de redondance, les règles les plus contraignantes s'appliquent.

4. LES RÈGLES.

4.1. **Généralités et articulation.**

La directive est déclinée sous deux angles : règles organisationnelles (RO) et règles techniques (RT). Les règles sont numérotées de manière séquentielle suivant l'articulation suivante.

<table>
<tr><td rowspan="4">Accès.</td><td>Cat 1.</td><td rowspan="4">Règles communes
point 4.3.</td><td colspan="2">Règles relatives aux accès de première catégorie
point 4.4.</td></tr>
<tr><td>Cat 2.</td><td rowspan="2">Règles relatives aux accès de seconde et de troisième catégorie
point 4.5.</td><td>Règles complémentaires aux accès de deuxième catégorie
point 4.6.</td></tr>
<tr><td>Cat 3.</td><td>Règles complémentaires aux accès de troisième catégorie
point 4.7.</td></tr>
<tr><td></td><td></td></tr>
</table>

	Cat 4.		Règles relatives aux accès de quatrième catégorie point 4.8.
Hébergement des services.			Règles relatives à l'hébergement des services ministériels de l'internet point 4.9.

Un tableau récapitulatif des règles répondant aux principes est présenté en annexe III.

4.2. **Rappel.**

Afin d'éviter toute interprétation abusive des règles rédigées dans ce document, il est utile de rappeler les conditions d'emploi des informations soumises au secret de la défense nationale sur le réseau internet. Ces deux règles déclinent de l'instruction ministérielle [IM8192] et leur non respect fait l'objet d'articles du code pénal.

RO 1 Il est interdit de traiter ou de stocker des informations soumises au secret de la défense nationale (22) sur des réseaux ou postes standards connectés à l'Internet.

RO 2 Il est interdit de traiter ou de stocker des informations sensibles (23) sur les réseaux ou postes standards dédiés à l'internet.

Commentaire : dans le cas de postes mettant en œuvre une architecture agréée multi-niveau permettant un cloisonnement de confiance entre une instance dédiée à l'internet et une instance d'un niveau de sécurité supérieur, la règle s'applique uniquement à l'environnement connecté à l'internet.

4.3. **Règles communes.**

La présente directive sera déclinée en un document précisant les mesures techniques et non techniques élaborées à partir d'une analyse de risque et sur la base de la politique de sécurité du ministère [IM133]. L'opérateur défense est chargé d'instruire le dossier en collaboration avec les organismes hors de son périmètre.

RO 3 Il est obligatoire de faire valider le document compilant ces mesures et ses évolutions par la DGSIC.

RO 4 Il est obligatoire que l'opérateur défense mène une gestion continue des risques formalisée.

RO 5 Il est obligatoire de sensibiliser les utilisateurs potentiels du ministère à l'utilisation des services de l'Internet au minimum une fois par an.

Cette sensibilisation portera sur :

- le code de bon usage des systèmes d'information et de communication du ministère de la défense [IMCODE USAGE] ;

- les menaces (24) liées à l'utilisation des services de l'internet ;

- les attaques les plus courantes du moment qui peuvent toucher entre autres le ministère ;

- les dispositifs de protection et de contrôle des activités liées à l'internet mis en œuvre dont notamment une présentation de leur finalité ;

- les principes du respect des droits et libertés fondamentales des personnes ;

- les réactions à tenir en cas de constatation d'un incident de sécurité.

Commentaires :

- les règles particulières liées à la coexistence sur les sites concernés de moyens classifiés de défense et non classifiés seront rappelées et systématiquement vérifiées (ex : internet Welfare WIFI à proximité des centres d'opérations de théâtre).

- l'effort de sensibilisation est constant et régulier.

RO 6 Il est obligatoire de différencier les accès aux services de l'internet suivant les catégories définies au point 3.1.3.

RT 1 Il est recommandé de mettre en application les principes de défense en profondeur rappelés au point 3.1.5.

Commentaires :

- il conviendra de les appliquer au maximum. Contrairement à la gestion des dérogations décrite au point 1.7., le choix de déroger à certains principes non obligatoires est laissé à l'appréciation de l'autorité qualifiée à partir des éléments de l'analyse de risque.

- le principe du moindre privilège se traduit, entre autres, par :

  - interdire les droits « administrateur » à l'utilisateur ;

  - interdire les ports réseaux non utilisés ;

  - supprimer sur les postes, serveurs et éléments actifs tous les programmes et processus non indispensables.

4.4. **Règles relatives aux accès de première catégorie.**

Les démarches d'abonnement sont à la charge exclusive du client (agent ou personne morale du ministère de la défense).

Les démarches de mise en œuvre de postes pour des accès de première catégorie ne sont pas du ressort du ministère de la défense. La personne morale ou l'agent ayant passé à titre privé ce contrat doit respecter l'environnement dans lequel il se situe.

RO 7 Il est obligatoire que toute demande d'accès de catégorie 1 fasse l'objet d'une déclaration préalable à l'OSSI de site afin d'instruire les contraintes de sécurité locales, notamment SPC dans le cadre de la mise en œuvre de bornes WIFI ou de liaisons *via* la technologie courant porteur en ligne (CPL).

Une base de défense ou autre (site) peut néanmoins être amenée à agir en tant qu'intermédiaire entre le fournisseur d'accès et les postes terminaux.

4.5. **Règles relatives aux accès de seconde et de troisième catégorie.**

4.5.1. ***Organisation.***

RO 8 Il est obligatoire de doter les acteurs du ministère, ayant à utiliser l'internet de manière discrète dans le cadre de leur mission, des dispositifs techniques adaptés.

Commentaire : la liste des organismes ou services concernés par cette règle est fixée par l'état-major des armées (EMA).

4.5.2. ***Dispositif frontière de protection.***

RT 2 Il est recommandé de disposer d'un dispositif frontière de protection pour chaque accès internet de seconde et de troisième catégorie. Ce dispositif devra permettre *a minima* :

- de tracer les connexions ;

- de filtrer et tracer les flux jusqu'au niveau 5 de la couche OSI ;

- d'analyser en innocuité virale les flux entrants et sortants suivant l'état de l'art de la technologie ;

- de contrôler l'accès des utilisateurs.

Commentaires :

- le dispositif frontière de protection à mettre en œuvre respectera les impératifs fixés par l'évaluation des risques ;

- il peut être réparti sur différents endroits (FAI, segment d'interface, poste terminal, centre d'hébergement de services internet : messagerie, etc) ;

- la conception de ce dispositif de sécurité incombe à l'opérateur défense. Dans le cadre de certaines exceptions, les organismes hors périmètre DIRISI s'appuieront sur, voire complèteront, les travaux de la DIRISI ;

- le choix des outils de sécurité se portera en premier lieu sur des outils de confiance, notamment ceux ayant reçu une certification CSPN (25) ou qualifiés élémentaire, voire standard (au sens ANSSI). Cependant, lorsque le recours à un produit qualifié n'est pas possible pour prendre en charge des fonctions de sécurité, les outils largement déployés ou éprouvés par la communauté ou par les forces pourront être sélectionnés. L'accent sera également porté sur l'efficience des analyses des journaux. L'opérateur fera procéder dès lors à une analyse (26) de l'état de sécurité des produits.

RT 3 Il est recommandé de détecter voire de limiter les intrusions.

Commentaire : contrairement à la gestion des dérogations décrite au point 1.7., le choix de déroger à cette règle est laissé à l'appréciation de l'autorité qualifiée à partir des éléments de l'analyse de risque.

RT 4 Il est recommandé de filtrer les flux WEB au niveau 7 de la couche OSI,

Commentaire : la mise en œuvre d'un outil de filtrage d'URL peut être assurée en central.

4.5.3. ***Administration.***

L'ergonomie des configurations des postes terminaux dédiés à l'internet du ministère reste une exigence forte de la part des utilisateurs du ministère. Aussi, il conviendra de pouvoir réaliser l'installation de logiciels répondant aux besoins des utilisateurs sans pénaliser la sécurité globale. Les logiciels installés devront avoir systématiquement fait l'objet d'une validation sous les axes gouvernance, emploi, SSI et intégration afin de limiter les récupérations hasardeuses de logiciels sur des sites internet n'offrant aucune garantie de sécurité en termes de présence de codes malveillants.

Les règles inhérentes à ce principe sont décrites dans la directive poste terminal. En outre,

RT 5 Il est obligatoire de mettre à jour les briques logicielles du poste terminal et de tous les outils de sécurité déployés.

Commentaire : les mises à jour sont effectuées directement et automatiquement par les logiciels eux-mêmes sur des sites ayant été identifiés de confiance par l'administration. En particulier et à défaut de sites de confiance maîtrisés, pour les systèmes dédiés à l'internet, les mises à jour s'effectueront depuis les sites

officiels des éditeurs des briques logicielles. Cette mesure tend à fournir une capacité de maintien en condition de sécurité des systèmes dédiés à l'internet.

RT 6 Il est obligatoire d'activer la journalisation des événements de sécurité au niveau des postes terminaux.

Commentaire : la journalisation est activée pour permettre l'analyse interne liée à un dysfonctionnement ou à un incident de sécurité puis, le cas échéant, pour dégager la responsabilité de l'État, les journaux constituent des éléments de preuve dans le cadre d'une enquête judiciaire ou d'une procédure disciplinaire. L'opérateur défense et les organismes hors de son périmètre définiront les éléments de journalisation nécessaires à une analyse post-incident.

*4.5.4. **Contrôle des activités.***

Les contrôles seront réalisés conformément aux dispositifs législatifs et réglementaires en vigueur et respectueux des principes développés par la CNIL dans le cadre de la cybersurveillance [GCNIL] dont notamment les principes de proportionnalité (27) et du respect des droits des personnes (28).

RO 9 Il est recommandé de mettre en place un contrôle des activités liées à l'utilisation des services de l'internet.

RT 7 Il est recommandé de mettre en place un dispositif de contrôle individuel des utilisateurs destiné à produire un relevé des connexions ou des sites visités, poste par poste.

L'analyse des journaux doit pouvoir préciser la nature des sites visités (catégorie, URL du site), la date et heure de chaque connexion, le temps passé et le nombre de connexions.

Commentaires :

- il s'agit de mettre en place un dispositif de filtrage automatique amont des URL pour se prémunir de tout accès à des sites interdits (sites réprimés par la loi) et contraires aux bons usages (ex : catégorie des sites pornographiques, catégorie des sites de jeux en ligne, etc) ;

- compte-tenu de l'absence de correspondants informatiques et libertés au sein du ministère, le traitement de données à caractère personnel mis en œuvre doit être déclaré à la CNIL ;

- la définition des profils et des catégories incombe à l'opérateur défense en liaison avec les organismes hors de son périmètre. À titre d'exemple, trois profils peuvent être envisagés :

  - profil 0 : aucune restriction ;

  - profil 1 : restriction aux sites réprimés par la loi, aux sites dans la catégorie pornographique, jeux, autres. Les autres catégories sont à définir par l'opérateur ;

  - profil 2 : accès uniquement à des catégories de sites autorisées ;

- ce dispositif doit être centralisé et adapté à un fonctionnement en mode multi-sites.

RO 10 Il est recommandé de mettre en place et d'exploiter des statistiques sur l'utilisation d'internet au niveau de chaque entité.

Commentaire : contrairement à la gestion des dérogations décrite au point 1.7., le choix de déroger à cette règle est laissé à l'appréciation de l'autorité d'emploi.

RT 8 Il est recommandé d'adresser mensuellement à l'utilisateur la synthèse de ses connexions.

Commentaire : cette règle contribue à renforcer la sensibilisation des utilisateurs vis-à-vis de leurs habitudes de navigation. De même, elle assure une capacité de contrôle, à titre individuel, de la non usurpation de leurs accès.

RT 9 Il est obligatoire de mettre en place un dispositif de contrôle individuel de la messagerie professionnelle dans le cadre d'analyse de contenu des messages électroniques entrants et sortants.

Des contrôles sémantiques automatiques de diffusion illégale d'informations classifiées seront systématiquement mis en œuvre.

Commentaire : compte-tenu de l'absence de correspondants informatiques et libertés au sein du ministère, le traitement de données à caractère personnel mis en œuvre doit être déclaré à la CNIL.

En outre, les messages professionnels n'intégrant pas une balise spécifique dans les entêtes ne seront pas autorisés à être transmis.

RT 10 Il est obligatoire que les messages transitant sur l'internet et dont l'adresse de l'émetteur identifie clairement une adresse du ministère de la défense, portent une balise explicitant que le message a été envoyé par internet.

Commentaires :

- l'action de marquer les messages est un acte volontaire confirmant que les informations transmises ne sont pas de nature « sensible » ou « protégée ».

- les passerelles de messagerie Internet du ministère bloqueront les messages ne portant pas cette balise.

- le choix des termes de cette balise incombe à l'opérateur défense en liaison avec les organismes hors de son périmètre.

4.6. **Règles complémentaires aux accès de seconde catégorie.**

4.6.1. ***Organisation.***

L'intradef est le seul réseau professionnel (29) sur lequel les postes peuvent être mutualisés pour accéder aux services de l'internet et aux services de l'intradef. L'accès aux services de l'internet s'effectuera au travers du segment d'interface sécurisé unique de l'intradef.

Dans le cadre de systèmes dédiés à l'internet :

RO 11 Il est recommandé de mutualiser les accès aux services de l'internet pour concentrer les efforts de sécurité sur le ou les points d'accès haut débit.

Commentaires :

- cette mutualisation peut s'effectuer au niveau du site (30), voire de la base de défense, voire d'une région, etc. La définition de l'architecture incombe à la DIRISI en partenariat avec les organismes hors de son périmètre ;

- le choix d'accès multiples fera l'objet d'une validation en sous-commission architecture du comité des intranets.

RO 12 Il est obligatoire**,** au minimum, de mutualiser les accès aux services de l'internet au niveau du site.

4.6.2. ***Dispositif frontière de protection.***

RT 11 Il est obligatoire de contrôler l'accès des utilisateurs en entrée et en sortie du réseau constitué.

La règle suivante traduit l'exigence de traçabilité et d'imputabilité des actions des personnels de la défense lorsqu'ils se connectent aux services de l'internet.

RT 12 Il est obligatoire d'identifier et d'authentifier nominativement les utilisateurs sur l'ensemble des flux sortants et entrants du réseau.

Commentaire : la mise en œuvre d'un pare-feu authentifiant associant les droits d'accès à un utilisateur identifié est requise au niveau de la passerelle de sécurité.

RT 13 Il est obligatoire de masquer le plan d'adressage interne vis-à-vis de l'extérieur.

Par ailleurs, un accès internet prévu pour un nombre de postes connectés inférieur ou égal à trois, sur un site isolé et ne pouvant être mutualisé avec un accès internet d'un autre site de la défense n'est pas soumis à la mise en œuvre d'une telle passerelle de sécurité. Néanmoins, les dispositifs frontières de protection seront mis en œuvre au niveau de chaque poste terminal.

Cette configuration doit rester exceptionnelle afin de ne pas augmenter les charges d'administration.

4.6.3. ***Administration.***

RO 13 Il est recommandé de prévoir des tests de non régression pour les constituants des dispositifs frontières de protection.

Commentaires :

- dans le cadre des outils de sécurité (31) nécessitant une mise à jour régulière (base de signatures par exemple), cette règle ne s'applique pas ;

- contrairement à la gestion des dérogations décrite au point 1.7., le choix de déroger à cette règle est laissé à l'appréciation de l'autorité qualifiée à partir des éléments de l'analyse de risque.

RT 14 Il est obligatoire d'activer la journalisation des événements de sécurité au niveau des constituants des dispositifs frontières de protection.

RO 14 Il est obligatoire d'exploiter les journaux de sécurité issus des constituants du dispositif frontière de protection :

- la surveillance est permanente et en temps réel pour les segments d'interface de systèmes mutualisés ;

- une fréquence quotidienne d'exploitation des journaux est recommandée pour les segments d'interfaces de systèmes dédiés.

RT 15 Il est recommandé de déporter et centraliser les journaux de sécurité.

Commentaire : contrairement à la gestion des dérogations décrite au point 1.7., le choix de déroger à cette règle est laissé à l'appréciation de l'autorité qualifiée à partir des éléments de l'analyse de risque.

RT 16 Il est obligatoire de conserver les journaux pendant un an.

4.6.4. ***Règles spécifiques aux postes privés.***

Les accès de deuxième catégorie peuvent associer aussi bien des postes privés que des postes dits professionnels appartenant au ministère de la défense. Aussi, afin de limiter les dangers d'interconnexion de

ces deux types de postes, il convient de respecter les deux règles suivantes.

RT 17 Il est obligatoire de cloisonner logiquement les réseaux dits privés (bulles réseaux permettant la connexion des postes privés) des réseaux dits professionnels (bulles réseaux permettant la connexion des postes appartenant au ministère).

Commentaire : les réseaux dits privés et professionnels pourront être raccordés à un même dispositif frontière de protection.

RO 15 Il est obligatoire que le propriétaire du poste privé s'engage sur le respect de règles de sécurité intrusives. En l'occurrence :

- le poste devra disposer d'un antivirus configuré pour se mettre à jour automatiquement sur internet ;

- le système d'exploitation, les logiciels de navigation et de messagerie seront configurés pour pouvoir se mettre à jour automatiquement sur internet ;

- le propriétaire du poste privé a lu, compris et applique l'instruction ministérielle [IMCODE USAGE].

- le propriétaire du poste privé accepte les contrôles de la configuration attendue du poste.

Commentaire : en cas de refus de ces règles ou de manquements constatés, le poste privé ne devra pas pouvoir se connecter aux services de l'internet par l'accès de catégorie 2. Le personnel devra alors s'orienter vers un accès de catégorie 1.

4.7. **Règles complémentaires aux accès de troisième catégorie.**

*4.7.1. **Organisation.***

La règle suivante contribue à apporter les réponses sur l'identité de l'utilisateur du module dans le cadre d'une enquête.

RO 16 Il est obligatoire d'attribuer, à titre comptable, le module (32) permettant l'accès mobile à l'internet à une personne physique.

RO 17 Il est déconseillé d'utiliser un terminal privé pour les accès de troisième catégorie.

Commentaire : une telle utilisation doit demeurer exceptionnelle et répondre à un besoin fonctionnel.

*4.7.2. **Dispositif frontière de protection.***

La conservation des données de connexions sera assurée par le FAI comme le prévoit la LCEN et le code des postes et des communications électroniques.

*4.7.3. **Administration.***

RT 18 Il est recommandé de conserver les journaux pendant un an.

RT 19 Il est obligatoire de conserver les journaux pendant un an sur les postes de type 2a (33).

4.8. **Règles relatives aux accès de quatrième catégorie.**

RO 18 Il est interdit de mettre en œuvre un accès internet de quatrième catégorie sans autorisation préalable de la DGSIC.

Commentaire : le CODIR des intranets instruira tout dossier de réalisation d'accès de quatrième catégorie.

4.9. **Règles relatives à l'hébergement des services internet du ministère.**

Les crises relatives aux attaques informatiques contre les sites institutionnels de certains pays ont mis en exergue la nécessité de protéger les services internet de la défense, cibles de choix pour les attaquants voulant, entre autres, discréditer l'image du ministère. Cet objectif de sécurité complété par le besoin de rationalisation des moyens humains, financiers et matériels pousse le ministère de la défense à concentrer les efforts de sécurité autour de 2 ou 3 centres d'hébergement des services internet.

Le choix du ou des prestataires incombe à l'opérateur défense (hébergement par un prestataire civil et/ou ministériel).

L'intérêt de disposer d'une plate-forme opérationnelle confrontée à de véritables menaces pour conforter une expérience LID devra être pris en considération.

4.9.1. ***Environnement.***

Dans le respect des recommandations interministérielles en termes d'ÉCO-TIC [34], le ministère doit favoriser les économies d'énergie.

RO 19 Il est recommandé de mettre en œuvre des architectures informatiques respectant les principes ÉCO-TIC

Commentaire : contrairement à la gestion des dérogations décrite au pointe 1.7., le choix de déroger à cette règle est laissé à l'appréciation de l'autorité d'emploi.

4.9.2. ***Impératifs de sécurité.***

RO 20 Il est recommandé que l'hébergement des services internet du ministère soit centralisé.

Commentaire : deux centres de production physiquement distincts assurant la disponibilité des services sont à envisager.

RO 21 Il est obligatoire que la plate-forme de production mise à disposition par les prestataires soit dédiée aux services internet du ministère (zone, serveurs, composants réseaux et sécurité, bande passante).

RO 22 Il est obligatoire de localiser les données hébergées et de pouvoir identifier rapidement celles impactées en cas d'attaque.

RO 23 Il est obligatoire que les lieux d'hébergement [35] des services internet et données du ministère soient localisés sur le territoire de l'union européenne.

Commentaires : il convient de vérifier que les obligations légales spécifiques (protection des données à caractère personnel, protection des données de santé, etc) sont respectées dans l'environnement d'hébergement, le propriétaire des données étant juridiquement responsable en cas d'infraction à la législation.

RO 24 Il est recommandé que les lieux d'hébergement des services internet et données du ministère soient localisés sur le territoire français.

RO 25 Il est recommandé que le prestataire ait mis en œuvre une démarche qui lui permettrait d'obtenir une certification ISO/CEI 20000-1 [36] et ISO/CEI 27001 [37].

Commentaire : si le prestataire est issu du ministère, une démarche d'homologation de sécurité à l'instar de celle pour un système sensible doit être menée. En parallèle, la mise en place d'un SMSI [38] sur le périmètre de l'hébergement ainsi qu'une démarche ITIL doivent être recherchées.

RT 20 Il est recommandé que le centre d'hébergement réponde aux exigences de certification TIER IV de la norme de disponibilité définie par l'Uptime Institute [39] .

Commentaire : les centre de données TIER IV disposent des redondances nécessaires [40] permettant de maintenir un fonctionnement nominal de l'activité lors d'entretien, de maintenance annuelle ou de remplacement d'un élément actif. La certification TIER IV engage le prestataire à assurer un taux de disponibilité de 99,995 p. 100 sur un an (soit une indisponibilité cumulée de moins de deux jours par an).

Le référentiel général de sécurité fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées. Ces règles concernent la confidentialité et l'intégrité des données, ainsi que la disponibilité et l'intégrité des systèmes et l'identification des utilisateurs.

Sans préjuger de la teneur de la directive certificat à paraître, certains services auront besoin de s'authentifier.

RT 21 Il est obligatoire d'utiliser des certificats électroniques de type authentification délivrés par des prestataires de service de certification électronique (PSCE) conformes à une politique de certification type authentification de niveau de sécurité au moins égal à une étoile .

RT 22 Il est obligatoire de conserver les journaux de sécurité pendant un an.

Commentaire : la durée de conservation des données de connexion à l'internet a fait l'objet d'une décision de la part de la direction des affaires juridiques [DAJ_DUREE_TRACE].

RO 26 Il est obligatoire de transmettre au centre technique LID du ministère l'inventaire des systèmes d'information hébergés et la cartographie de l'infrastructure d'hébergement.

Commentaire : la nature exacte des informations à transmettre ainsi que les modalités de transfert seront définies par le centre technique LID du ministère.

RO 27 Il est obligatoire de déclarer les sites WEB internet auprès du centre technique LID du ministère.

Commentaires :

- cette responsabilité incombe à chaque autorité d'emploi mettant en œuvre un site WEB internet ;

- la nature exacte des informations à transmettre ainsi que les modalités de transfert seront définies par le centre technique LID du ministère.

4.9.3. ***Démarche de sécurité.***

4.9.3.1. Règles générales.

L'hébergement des services internet du ministère doit être géré comme un projet. Il fera l'objet d'une évaluation des risques et d'une gestion continue des risques. Pour suivre la sécurité de ce projet :

RO 28 Il est obligatoire de désigner un responsable sécurité du système d'information (RSSI) dès l'initialisation du projet et de s'assurer de ses compétences en la matière.

RO 29 Il est obligatoire de procéder à une analyse des risques de la fonction d'hébergement.

Commentaires :

- l'analyse des risques conduit à déterminer les objectifs de sécurité permettant de rendre les risques acceptables ;

- les objectifs de sécurité, traduits dans la FEROS, permettent de définir une cible de sécurité servant de cadre au contrat établi avec le futur prestataire.

RO 30 Il est recommandé d'utiliser le référentiel de menaces génériques de la méthode EBIOS.

RO 31 Il est recommandé que l'analyse de risque ne soit pas menée par le titulaire du marché d'hébergement.

Commentaire : il convient d'éviter que le titulaire du marché d'hébergement soit à la fois juge et partie puis mène une analyse réduite à ce qu'il sait faire.

RT 23 Il est obligatoire qu'un audit de sécurité soit mené au minimum une fois par an dans le périmètre de la fonction d'hébergement.

Commentaire : l'audit de sécurité est mené par un organisme différent du prestataire.

RT 24 Il est recommandé de mener des tests d'intrusions sur la plate-forme d'hébergement afin de mesurer le niveau de résistance de l'architecture et l'efficience des administrateurs chargés de la sécurité.

Commentaire : dans le cadre d'une externalisation de l'hébergement, ces tests devront être menés en liaison avec le prestataire et contractualisés. Le processus de réalisation de ces tests d'intrusion doit être inséré dans le contrat.

4.9.3.2. Règles spécifiques à l'hébergement des services internet par le ministère.

RO 32 Il est obligatoire de mener un processus d'homologation de sécurité de l'infrastructure d'hébergement.

Commentaires :

- le dossier d'homologation comprend :

  - l'expression des objectifs de sécurité (FEROS) ;

  - le plan de sécurité présentant les mesures [41] techniques et non techniques prises pour atteindre ces objectifs ;

  - le dossier des risques résiduels ;

  - les procédures d'exploitation de sécurité ;

  - les rapports d'audit, de contrôle et d'inspection.

- la commission d'homologation se réunit une fois par an pour statuer du niveau de sécurité ;

- l'homologation est prononcée pour une durée maximale de cinq ans.

4.9.3.3. Règles spécifiques à l'externalisation de l'hébergement des services internet du ministère.

La démarche de prise en compte de la sécurité lors de l'externalisation doit amener le futur prestataire à s'engager sur les mesures techniques et organisationnelles visant à répondre aux exigences de sécurité du ministère.

RO 33 Il est obligatoire que la démarche soit conforme à celle décrite dans le guide ANSSI « externalisation des systèmes d'information » [ANSSI_CSE].

RO 34 Il est obligatoire de créer un comité de suivi chargé de coordonner les actions, prévues au contrat, au titre de la sécurité et de piloter l'évolution du volet sécurité de la prestation.

Commentaires :

- le comité de suivi :

  - est une instance décisionnaire co-présidée par l'opérateur défense et le prestataire ;

  - décide au vu des résultats de l'audit et de la vérification de bon fonctionnement de la mise en service opérationnelle de la plate-forme d'hébergement ;

  - s'assure des conditions techniques et financières des transferts des moyens matériels et logiciels de sécurité mis en place, en cas de réversibilité de l'opération ;

  - traite des questions techniques touchant à la sécurité (collaboration dans la gestion des droits et la gestion des incidents, détection des anomalies et préconisation d'améliorations, exploitation des résultats des audits de contrôle des prestations sécurité) ;

  - approuve et vérifie l'exécution des plans d'actions issus des rapports d'audit pour remédier aux vulnérabilités résiduelles constatées.

- le RSSI défense est membre de droit du comité de suivi.

L'opérateur défense spécifie les exigences de sécurité et les clauses de sécurité (42) dans le cahier des charges. Le cahier des clauses techniques particulières exigera du titulaire la fourniture du plan d'assurance sécurité (PAS) (43), du dossier de sécurité, d'un plan de secours, du plan de gestion des incidents ainsi que des compte-rendus de réunion du comité de suivi.

RO 35 Il est obligatoire que le soumissionnaire du marché d'hébergement réponde à la consultation avec un PAS préliminaire.

Commentaires :

- le PAS devra répondre aux exigences de sécurité issues des objectifs de sécurité définis dans la FEROS ;

- le PAS respectera les modalités définies dans le guide [ANSSI_CSE]. Le plan type du PAS sera défini dans le marché afin de faciliter la comparaison des offres ;

- le soumissionnaire fournira les éléments justificatifs en même temps que les mesures techniques et organisationnelles proposées ;

- le PAS préliminaire, amendé au besoin et accepté par l'opérateur défense en conformité avec ses exigences, est annexé au contrat.

5. GLOSSAIRE ET ACRONYMES.

ANSSI : agence nationale de sécurité des systèmes d'information.

AQ : autorités qualifiées.

CALID : centre d'analyse de lutte informatique défensive.

CELEX : cellule d'expertise.

CERTA : centre d'expertise gouvernementale de réponse et de traitement des attaques informatiques.

CMSSI : commission ministérielle SSI.

CMTSIC : commission ministérielle technique des systèmes d'information et de communication.

CPCO/J6/LI : centre de préparation et de conduite opérationnelle/bureau j6/lutte informatique.

CPL : courant porteur en ligne.

ÉCO-TIC : écotechniques de l'information et de la communication.

FCM : fiche de caractéristique militaire.

FEROS : fiche d'expression rationnelle des objectifs de sécurité.

FSSI : fonctionnaire de la sécurité des systèmes d'information.

IGI : instruction générale interministérielle.

LCM : lutte contre les codes malveillants.

LCEN : loi pour la confiance dans l'économie numérique.

LID : lutte informatique défensive.

MCO : maintien en conditions opérationnelles.

MCS : maintien en condition de sécurité.

OPVAR : organisation permanente veille alerte réponse.

SI : système d'information.

SMSI : système de management du système d'information.

SPC : signaux parasites compromettants.

SSI : sécurité des systèmes d'information.

STB : spécification technique de besoin.

6. RÉFÉRENCES.

[ANSSI_CSE] note n° 742/ANSSI/ACE du 29 mars 2010 (n.i. BO) relative à la prise en compte de la sécurité des systèmes d'information dans les opérations d'externalisation. Ce guide est publié sur le site de l'ANSSI (www.ssi.gouv.fr).

[DAJ_DUREE_TRACE] note n° 70578/DEF/SGA/DAJ/D2P/CCM du 5 novembre 2008 (n.i. BO) relative à la durée de conservation des données de connexion à l'internet.

[GCNIL] Guide pour les employeurs et les salariés édition 2008 (n.i. BO).

[AVIS_CSD] Avis sur internet et défense n° 08.109/CSD du 14 novembre 2008 (n.i. BO).

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

Christian PÉNILLARD.

---

(1) Livre Blanc sur la défense et la sécurité nationale.

(2) Le cyberespace peut être considéré comme le réseau interdépendant de l'ensemble des infrastructures des technologies de l'information, incluant l'internet, les réseaux de télécommunications, les systèmes informatiques ainsi que les serveurs et protocoles d'usages propres à certaines industries critiques.

(3) Données à caractère personnel, données médicales, etc.

(4) Une ressource est caractérisée par le matériel permettant l'accès au réseau internet (poste terminal, serveur, éléments actifs, etc).

(5) Par exemple : intrusion, déni de service distribué, défiguration d'un site institutionnel voire utilisation frauduleuse d'une ressource par un personnel du ministère.

(6) Par exemple l'article 34 de loi « Informatique et Liberté » dispose que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. ». Cet article s'applique aux données à caractère personnel (dont les données de santé à caractère personnel).

(7) Article L. 226-17 du code pénal : « le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34. de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».

(8) Défini par la FEROS.

(9) Tant en interne que par un prestataire extérieur au ministère de la défense.

(10) Les systèmes multi-niveaux sont inclus dans ce périmètre.

(11) Ex : Modem.

(12) L'usage privé se fait dans le cadre de l'exécution du contrat de travail (c'est à dire aux heures et lieux de travail).

(13) Exemple : clef 3G.

(14) Technologies constitutives des postes terminaux type 2b suivant la typologie retenue dans la directive DGSIC n° 8 définissant les règles à appliquer au système de postes terminaux.

(15) Notamment, les acteurs chargés de la lutte informatique et du renseignement.

(16) L'ensemble des activités d'un agent sur internet.

(17) Déclaration des droits de l'homme et du citoyen du 26 août 1789, Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (art. 8. et 10.) ; Charte des Droits fondamentaux de l'Union européenne (art. 7.).

(18) Article 432-9 C. Pénal.

(19) Internet Protocol version 4.

(20) Internet Protocol version 6.

(21) En tant que représentant du haut fonctionnaire correspondant de défense et de sécurité (HFCDS).

(22) Au sens du code pénal (article 413-9 à 413-12 du code pénal).

(23) Informations sensibles non classifiées de défense au sens de la recommandation du Premier ministre n° 901/DISSI/SCSSI du 2 mars 1994.

(24) Cause potentielle d'incident qui peut résulter en un dommage au système ou à l'organisation.

(25) Certificat de de sécurité de premier niveau.

(26) Une analyse type ASPC ou équivalente est requise.

(27) La mise en place d'un dispositif de contrôle des salariés ne doit pas conduire à apporter aux droits et libertés des personnes de restrictions qui ne seraient pas proportionnées au but recherché et justifiées par l'intérêt légitime du ministère.

(28) Outre la consultation des comités techniques paritaires du personnel, les agents ainsi que leurs interlocuteurs, doivent être informés, préalablement à la mise en place du dispositif :

- des objectifs poursuivis par l'installation de ce système ;

- des conséquences individuelles qui pourront en résulter ;

- des destinataires des enregistrements ;

- des modalités d'exercice de leur droit d'accès.

(29) Pour information, le réseau Ext du SGA est un réseau dédié internet.

(30) Lieu de stationnement de formations et d'unités sous responsabilité d'un chef de corps ou d'un administrateur.

(31) Antivirus, IPS, IDS, etc

(32) À défaut, le terminal de type 2b.

(33) Suivant la typologie retenue dans la directive n° 8 définissant les règles à appliquer au système de postes terminaux

(34) Techniques de l'information et de la communication dont la conception ou l'emploi permettent de réduire les effets négatifs des activités humaines sur l'environnement.

(35) Site principal, site de secours, sites hébergeant les sauvegardes, sites de télémaintenance s'ils peuvent accéder aux données, etc.

(36) La norme ISO/CEI 20000-1 est un référentiel relatif à la gestion des services informatiques. Elle s'appuie sur les recommandations d'ITIL (Information Technology Infrastructure Library), ensemble de bonnes pratiques en matière de gestion des services liés aux technologies de l'information.

(37) La norme ISO/CEI 27001 est un référentiel relatif aux systèmes de management de la sécurité de l'information.

(38) Système de management du système d'information.

(39) http://www.uptimeinstitute.org

(40) Le centre de données dispose, entre autres, de plusieurs circuits électriques pour l'énergie et pour la distribution de refroidissement.

(41) Aspects organisationnels, administration du système et de sa sécurité, supervision de la sécurité, protection physique, protection du personnel, protection des documents, mesures de sécurité informatique et des communications, gestion de la configuration, maintenance, sauvegardes et mesures d'urgence (reconfiguration, évacuation, destruction).

(42) Les clauses de sécurité spécifiées dans le guide [ANSSI_CSE] sont complétés par celles décrites en annexe II.

(43) Le PAS précise les dispositions contractuelles prises par ce dernier pour répondre aux exigences de sécurité.

ANNEXE I.

ACCÈS AUX SERVICES DE L'INTERNET.

	ACCÈS BACKBONE (FAI).											
LIEU.	SITES MINDEF (MÉTROPOLE, OM, OPEX, ÉTRANGER).								MOBILITÉ.			
DESSERTE.	AUTRE (a).				MINDEF (b).				MINDEF (b).			
TERMINAL.	Autre (c).		Mindef (d).		Autre (c).		Mindef (d).		Autre (c).		Mindef (d).	
USAGE.	Privé (e)	Pro (f)	Privé (e)	Pro (f)	Privé (e)	Pro (f)	Privé (e)	Pro (f)	Privé (e)	Pro (f)	Privé (e)	Pro (f)
CONTRAT PRIVÉ.	X	X (g)										
CONTRAT DÉFENSE.	X	X (h)			X	X	X (i)	X		X (j)	X (i)	X
	Cat 1				Cat 2					Cat 3		

Les autres cas d'emploi s'inscrivent dans la quatrième catégorie (Cat 4).

(a) La desserte est mise en œuvre par un agent du ministère à titre privé ou par un prestataire privé.

(b) La desserte est mise en œuvre par les agents du ministère dans un cadre professionnel.

(c) Le terminal n'appartient pas au ministère. Il peut s'agir de postes privés ou mis en œuvre par un prestataire privé.

(d) Le terminal appartient au ministère et est mis en œuvre par le ministère.

(e) L'usage est privé.

(f) L'usage est professionnel.

(g) Exemple : utilisation de poste privé dans le cadre du plan de continuité d'activité lors d'une pandémie.

(h) Exemple : externalisation de la mise en œuvre du réseau internet professionnel.

(i) Un espace de vie privée résiduel est accepté dans la limite des conditions fixées dans l'instruction ministérielle [IMCODE USAGE].

(j) L'usage d'un poste privé doit demeurer du domaine de l'exceptionnel.

ANNEXE II.

CLAUSES DE SÉCURITÉ COMPLÉMENTAIRES.

Plan d'assurance sécurité.

Cette clause précise que le prestataire s'engage à exécuter ses obligations selon un plan d'assurance sécurité (PAS), définit en accord avec l'opérateur défense. Cette clause doit annuler et remplacer la clause de sécurité générique proposée par le prestataire dans son contrat type.

Journaux d'événements et conservation des traces.

Cette clause engage le titulaire à assurer la journalisation des accès et des événements (système, Web...) sur tous les équipements informatiques de la plate-forme d'hébergement et définir conjointement avec le ministère d'une directive d'archivage des traces collectées.

Commentaires : le ministère :

- peut être amené à demander un extrait de ces traces, soit dans le cas d'un incident, soit à des fins de suivi de la (des) ressource(s). À ce titre, les informations présentes sur les journaux doivent être exploitables au regard de l'état de l'art ;

- doit pouvoir avoir accès contractuellement aux journaux d'événements en temps réel ;

- doit, de plus, être sûr que les journaux concernant ses ressources hébergées ne sont pas divulgués à d'autres organismes co-hébergés (garantie de confidentialité).

Suivi des ressources utilisées pour le ministère.

Cette clause engage le titulaire à présenter l'état d'utilisation des ressources mises à disposition du ministère et mettre en œuvre un nombre d'indicateurs définis conjointement avec le ministère.

Commentaires :

- le fait de pouvoir disposer d'indicateurs sur l'historique des ressources utilisées par le ministère est utile pour dégager les principaux événements relatifs à l'utilisation de la ressource précédant une éventuelle crise ;

- à titre d'exemple, quelques indicateurs pouvant être mis en œuvre (liste non exhaustive) :

- fréquence et suivi des mises à jour effectuées ;

- durée d'indisponibilité maximum et suivi de ces indisponibilités ;

- fréquence des sauvegardes et tests de restauration effectués ;

- indicateurs sur les ressources dont l'accès et la mise à disposition ne dégradent pas la sécurité du système d'information ;

- charge réseau pour les serveurs et pour les ressources ;

- charge processeur utilisée par les ressources et pourcentage de la charge des serveurs ;

- charge mémoire utilisée par les ressources et pourcentage de la charge des serveur.

Gestion des incidents.

La clause prévoit la mise en place d'une organisation permettant aux deux parties d'échanger des informations et de décider de toute action corrective 24 H/24 H et 7 J/7 J toute l'année dans le cadre de la gestion des incidents.

À ce titre, elle engage le titulaire :

- à identifier un contact technique (ou plusieurs) ;

- à identifier un contact décisionnel (ou plusieurs) ;

- à garantir une information immédiate (le ministère doit être tenu informé sans délais en cas d'attaque afin de déclencher le circuit de réaction adéquat) ;

- à définir des procédures de remontée d'incidents de sécurité ayant un impact sur la disponibilité, la confidentialité et l'intégrité des services internet du ministère ;

- à définir conjointement avec le ministère des procédures liées à la gestion des incidents et à la conduite des actions postérieures dans le respect des procédures ministérielles de l'OPVAR.

La clause précisera les points de contacts côté ministère.

Cette clause doit permettre également d'imposer au titulaire l'application de certaines mesures de contournement à une faille ou des mesures conservatoires face à une attaque ou un incident.

Commentaires :

- l'hébergeur doit prévoir le cas d'éventuelles attaques informatiques sur les services internet du ministère. Compte tenu de l'importance des conséquences en termes d'image, la réactivité en cas d'incident est requise ;

- le ministère peut désigner un organisme chargé d'analyser un incident. Cet organisme doit pouvoir jouir au nom du ministère d'un accès total à l'environnement de la ressource à des fins d'analyse. Par exemple :

  - prélèvement de tout élément nécessaire à l'analyse conformément aux règles de l'art pour la constitution d'éléments de preuve ;

  - analyse du système en fonctionnement.

Recette du système.

Cette clause prévoit les modalités de réception du système externalisé, notamment dans sa composante sécurité. Sous la responsabilité de l'opérateur défense, la recette du système inclut quatre vérifications.

1. Tests de validation fonctionnelle : ils ont pour objet de vérifier que le système réalise toutes les fonctionnalités qu'exige la satisfaction du besoin défini dans le contrat et le document de spécification système. Ces fonctionnalités sont vérifiées dans des conditions normales de fonctionnement. Ils permettent de vérifier les réactions du système dans des conditions parfaitement déterminées.

2. Tests de réaction technique : ils ont pour objet de vérifier la persistance ou la reprise du fonctionnement global pendant ou après des conditions de fonctionnement particulières. Les tests permettent de vérifier les capacités de reprise et de continuité d'activité du centre d'hébergement.

3. Tests de performance : ils visent à mesurer les caractéristiques quantitatives de performance définies dans le contrat dans des conditions de fonctionnement représentatives de l'utilisation réelle du système. Chaque scénario de test relatif aux performances fera l'objet d'une procédure qui précisera :

- la grandeur mesurée et les modalités de la mesure ;

- les conditions annexes de la mesure avec, en particulier toutes les conditions de charge des machines et du réseau par les autres activités.

Toutes les mesures de performances s'entendent dans un contexte de charge donné, représentatif de l'activité des utilisateurs. Les documents définissant les procédures d'acceptation système et les fiches d'essais système préciseront les outils de mesures qui seront mis en œuvre pour s'assurer du respect des exigences de performance et de capacité du système.

4. Contrôles de sécurité : les tests visent à démontrer la résistance du système aux tentatives de pénétration et de récupération d'information. Un audit de sécurité du centre d'hébergement du prestataire retenu sera mené afin de s'assurer que la plate-forme opérationnelle et l'organisation mises en place correspondent aux exigences de sécurité définies dans le marché.
La réalisation de l'audit peut être sous-traitée mais ne doit en aucun cas être menée par le prestataire. Le premier audit sera réalisé juste avant la mise en service opérationnelle de la plate-forme d'hébergement.

Commentaires :

- cette recette consiste à réaliser des opérations de vérification visant à s'assurer de la capacité de l'architecture d'hébergement à satisfaire l'ensemble des exigences définies dans le contrat (niveau de service inclus) ;

- le comité de suivi prononcera la mise en service opérationnelle de la plate-forme d'hébergement.

ANNEXE III.

VISION SYNTHÉTIQUE DES RÈGLES PAR PRINCIPE.

Règles organisationnelles.

PRINCIPES.		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
PROTÉGER LE PATRIMOINE APPLICATIF ET INFORMATIONNEL DU MINISTÈRE DE LA DÉFENSE CONTRE LES MENACES ISSUES DE L'INTERNET.	Cat 1			x	x																															
	Cat 2											x	x	x	x	x																				
	Cat 3																	x																		
	Cat 4																																			
	Hbg(44)																				x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
RÉDUIRE LA COMPLEXITÉ DES ACCÈS INTERNET.	Cat 1							x																												
	Cat 2											x																								
	Cat 3																																			
	Cat 4																																			
	Hbg																				x															
DIFFÉRENCIER LES ACCÈS AUX SERVICES DE L'INTERNET.	Cat 1						x																													
	Cat 2																																			
	Cat 3																																			
	Cat 4																		x																	
	Hbg																				x															
ASSURER UNE CERTAINE DISCRÉTION DES ÉCHANGES VIS-À-VIS DE L'EXTÉRIEUR.	Cat 1																																			
	Cat 2								x																											
	Cat 3								x																											
	Cat 4																																			
	Hbg																					x														
APPLIQUER LE PRINCIPE DE DÉFENSE EN PROFONDEUR.	Cat 1			x																																
	Cat 2											x	x	x	x	x																				
	Cat 3																																			

	Cat 4																																				
	Hbg																			x		x	x			x			x				x		x	
RENFORCER LA CULTURE DE SÉCURITÉ DES UTILISATEURS.	Cat 1			x		x																															
	Cat 2															x																					
	Cat 3																																				
	Cat 4																																				
	Hbg																																				
APPLIQUER UN CONTRÔLE DES ACTIVITÉS LIÉES À L'INTERNET.	Cat 1			x	x			x																													
	Cat 2									x	x				x	x																					
	Cat 3									x	x						x																				
	Cat 4																		x																		
	Hbg																						x				x	x									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

Règles techniques.

PRINCIPES.		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
PROTÉGER LE PATRIMOINE APPLICATIF ET INFORMATIONNEL DU MINISTÈRE DE LA DÉFENSE CONTRE LES MENACES ISSUES DE L'INTERNET.	Cat 1	x																							
	Cat 2		x	x	x	x	x								x			x							
	Cat 3		x	x	x	x	x																		
	Cat 4																								
	Hbg (45)																				x	x		x	x
RÉDUIRE LA COMPLEXITÉ DES ACCÈS INTERNET.	Cat 1																								
	Cat 2																								
	Cat 3																								
	Cat 4																								
	Hbg																								
DIFFÉRENCIER LES ACCÈS AUX SERVICES DE L'INTERNET.	Cat 1																								
	Cat 2																								
	Cat 3																								
	Cat 4																								
	Hbg																								
ASSURER UNE CERTAINE DISCRÉTION DES ÉCHANGES VIS-À-VIS DE L'EXTÉRIEUR.	Cat 1																								
	Cat 2													x											
	Cat 3																								
	Cat 4																								
	Hbg																								
APPLIQUER LE PRINCIPE DE DÉFENSE EN PROFONDEUR.	Cat 1	x																							
	Cat 2		x	x	x	x	x								x	x		x							
	Cat 3		x	x	x	x	x																		
	Cat 4																								
	Hbg																				x	x		x	x

RENFORCER LA CULTURE DE SÉCURITÉ DES UTILISATEURS.	Cat 1	x																							
	Cat 2								x		x														
	Cat 3								x		x														
	Cat 4																								
	Hbg																								
APPLIQUER UN CONTRÔLE DES ACTIVITÉS LIÉES À L'INTERNET.	Cat 1																								
	Cat 2		x		x		x	x	x	x	x	x	x		x		x								
	Cat 3		x		x		x	x	x	x	x								x	x					
	Cat 4																								
	Hbg																					x	x		x
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

(44) Hébergement.

(45) Hébergement.