PREMIER MINISTRE

Secrétariat général
de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Paris, le 12 janv. 2005
N° **920**/SGDN/DCSSI

INSTRUCTION INTERMINISTÉRIELLE

RELATIVE

AUX SYSTÈMES TRAITANT

DES INFORMATIONS

CLASSIFIÉES DE DÉFENSE

DE NIVEAU CONFIDENTIEL-DÉFENSE

Version 1.0

51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP - Tél 01.71.75.84.05 - Fax 01.71.75.84.00

MODIFICATIFS[1]

à l'instruction interministérielle N°920/SGDN/DCSSI relative aux systèmes traitant d'informations classifiées de défense de niveau Confidentiel-Défense

Numéro des modificatifs	Date du modificatif	Pages Concernées	Articles modifiés ou nouveaux

[1] Depuis la parution de l'instruction.

SOMMAIRE

INTRODUCTION

Le développement rapide des technologies de l'information a entraîné une dépendance croissante des organismes envers leur système d'information, devenu une composante vitale de l'organisation elle-même. Par ailleurs, l'utilisation croissante des systèmes d'information pour des applications variées a fait prendre conscience à la communauté des utilisateurs qu'il ne suffisait pas de mettre en œuvre les moyens de communication les plus performants, mais que ces derniers devaient être fiables et sûrs (disponibilité, intégrité dont preuve, et confidentialité).

La révision de l'instruction générale interministérielle **n°1300/SGDN/PSE/SSD** [IGI 1300] sur la protection du secret de la défense nationale, le retour d'expérience de la mise en œuvre de mesures de sécurité dans les systèmes d'information et de communication amenés à traiter des informations classifiées de défense de niveau Confidentiel-Défense, ainsi que l'établissement au niveau de l'Union Européenne comme de l'OTAN de règlements, directives et recommandations en matière de protection des informations classifiées de niveau équivalent, permettent et justifient le besoin de définir au niveau national des règles harmonisées de sécurité des systèmes d'information (SSI) pour les systèmes traitant des informations classifiées de défense de niveau Confidentiel-Défense.

Tel est l'objet de la présente instruction, qui s'inscrit dans un cadre de sécurité global[2] et complète ainsi :

- [IGI 1300], en détaillant les exigences de protection pour les systèmes de niveau Confidentiel-Défense, en particulier pour la constitution d'un local sécurisé ;
- l'instruction interministérielle **n°900/SGDN/SSD/DR** [II 900] du 20 juillet 1993 sur la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées, en déclinant ses grands principes en exigences de sécurité applicables et pratiques.

Article 1er

OBJET DE LA PRÉSENTE INSTRUCTION

La présente instruction définit[3] les exigences particulières de protection des informations classifiées de défense de niveau Confidentiel-Défense dans les systèmes d'information.

Elle prend en compte le cycle de vie des systèmes qui traitent ces informations, et sert de référence pour l'homologation de sécurité de ces systèmes.

Article 2

CHAMP D'APPLICATION

La présente instruction fixe les règles de sécurité des systèmes d'information traitant, même à titre occasionnel, d'informations classifiées de défense de niveau Confidentiel-Défense - qu'on dénomme

[2] Ceci impose donc la connaissance et l'application des textes de plus haut niveau ; cependant, à des fins didactiques et de sensibilisation à la SSI, la présente instruction reprend nombre de principes et d'exigences issus de ces textes, surtout dès lors qu'elle y apporte une précision pour les systèmes d'information de niveau Confidentiel-Défense.

[3] Conformément aux règles d'élaboration des textes juridiques français, le présent de l'indicatif vaut impératif pour les exigences exprimées.

dans la suite de l'instruction « informations Confidentiel-Défense » - , avec ou sans mention relevant du besoin d'en connaître (Spécial France, ACSSI, renseignement, nucléaire, ...).

Elle s'applique, conformément à [IGI 1300] :
- dans tous les départements ministériels ;
- dans les services déconcentrés de l'État ;
- dans les établissements publics nationaux placés sous l'autorité d'un ministre ;
- et, d'une façon générale, dans tous les organismes publics ou privés et par toutes les personnes dépositaires, soit par état ou profession, soit en raison d'une fonction ou d'une mission temporaire ou permanente, de secrets de la défense nationale.

Elle doit être référencée dans la politique de sécurité des systèmes d'information des organismes qui traitent d'informations Confidentiel-Défense. Elle peut également être particularisée au sein d'un organisme : déclinaison en une instruction ministérielle, par exemple.

Son application aux systèmes concernés doit être vérifiée dans le contexte de l'homologation de ces systèmes, puis lors des audits[4] de sécurité.

La décision de ne pas satisfaire l'ensemble des exigences exprimées ne peut intervenir que dans le cadre formel du processus d'homologation et selon les modalités décrites dans la politique de la sécurité des systèmes d'information des ministères. Ces dérogations doivent être réduites au minimum nécessaire, limitées et suivies dans le temps.

Certaines informations sensibles non classifiées de défense appartenant à des domaines particuliers (médical, industrie, judiciaire, police, …) peuvent nécessiter des mesures de niveau équivalent, qui relèvent de la politique de sécurité du ministère concerné.

Dès lors que le système traite exclusivement d'informations classifiées de niveau confidentiel de l'UE ou de l'OTAN, les règles de protection de ces organisations s'appliquent selon les protocoles en vigueur avec les États ou organisations associées, dans le cadre d'accords de sécurité ; la présente instruction n'est alors plus applicable.

Article 3

GRANDS PRINCIPES DE LA SÉCURITÉ D'UN SYSTÈME TRAITANT D'INFORMATIONS CONFIDENTIEL-DÉFENSE

Les principes généraux de sécurité des systèmes d'information sont établis par [IGI 1300] et [II 900]. Toutefois, l'évolution de la doctrine et des pratiques de la SSI conduit à compléter ces principes, notamment par celui de la défense en profondeur.

Pour la protection d'informations Confidentiel-Défense, les deux principes particuliers suivants sont retenus.

1) Inscription du système d'information dans une zone sécurisée définie par un ensemble de barrières physiques et logiques, avec possibilité de substitution d'un des trois niveaux de barrière physique par un ou plusieurs moyens de protection logique.

Conformément à [IGI 1300], le système de niveau Confidentiel-Défense doit être déployé dans une zone sécurisée ; la présence de trois barrières physiques (matérielles) doit systématiquement être recherchée. La protection physique des informations et supports protégés doit ainsi être conforme aux

[4] Les différentes activités (audit, contrôle, inspections, …) désignées dans la présente instruction sous le terme d'audits de sécurité sont explicitées en annexe.

exigences de la directive n°1223/SGDN/SSD/DR [D 1223], associant trois barrières physiques (matérielles) cohérentes, inclusives et successives, des fonctions de détection et des fonctions d'intervention

Cependant, les contraintes opérationnelles, techniques (architecture, technologie, disponibilité de produits matériels ou logiciels), ou bien d'exploitation des systèmes d'information, conduisent souvent à la présence permanente ou transitoire d'informations ou de supports protégés en dehors d'un meuble, voire d'un local ou bâtiment. Elles peuvent amener à mettre en œuvre, en lieu et place d'une barrière physique, des moyens de protection logique. Dans ce cas, les moyens[5] de protection logique et les procédures d'exploitation associées doivent constituer autant d'obstacles conçus de manière à ce que leur franchissement illégitime soit gêné, retardé et détecté.

2) Dans l'état actuel de la technologie, les équipements constituant le système d'information sont conçus pour le traitement d'informations jusqu'au niveau Confidentiel-Défense, en mode d'exploitation dominant ou exclusif : une protection similaire de toutes les informations traitées par le système, qu'elles soient de niveau Confidentiel-Défense ou de niveau inférieur, est offerte.

Ce principe découle de l'absence de solutions multi-niveaux de confiance notamment dans la gestion de l'interconnexion de systèmes d'information de niveaux différents.

On considère donc que l'ensemble du système fait l'objet d'une homologation au niveau Confidentiel-Défense, que l'ensemble des utilisateurs est habilité, et que l'exportation d'informations Confidentiel-Défense ou non à partir du système est maîtrisé.

En outre, il est possible de faire circuler les informations Confidentiel-Défense en clair ou chiffrées par des moyens non agréés (par exemple pour séparer le besoin d'en connaître), sur des circuits approuvés conformément à cette instruction. En particulier, ces circuits ne partagent pas de ressources avec des réseaux de niveau inférieur (équipements actifs des réseaux locaux, câbles, armoires de brassage le cas échéant, imprimantes, sauvegardes, …).

Article 4

DONNÉES PERSONNELLES ET CORRESPONDANCE PRIVÉE

La politique de sécurité du système d'information détermine, en conformité avec les dispositions du règlement intérieur de l'organisme, si le système peut être utilisé à des fins de correspondance privée ou de traitement de données personnelles, et en définit les conditions d'emploi afférentes.

[5] Le niveau d'implémentation (applicatif, réseau) des moyens de protection logique étant notamment à définir au vu des menaces et du niveau de confiance de l'environnement technique d'exploitation (systèmes d'exploitation, famille de protocoles, …).

TITRE I

EXIGENCES EN MATIÈRE DE RESPONSABILITÉS ET DE PROCESSUS DE SÉCURISATION DU SYSTÈME D'INFORMATION

Article 5

RÉFÉRENTIEL MINISTÉRIEL DE SSI

L'article 47 de [IGI 1300] dispose que :

"*Face à la complexité croissante et au niveau d'intégration et d'interconnexion élevé des systèmes d'information, il est nécessaire de mettre en œuvre une gestion globale des risques de sécurité pour l'ensemble du système d'information tout au long de son cycle de vie et impliquant les différents acteurs concernés. Une telle approche, dite "démarche d'homologation de sécurité", doit permettre d'identifier, d'atteindre puis de maintenir un niveau de risques de sécurité acceptable pour le système d'information considéré, compte tenu du niveau de protection requis*."

Le référentiel ministériel de la SSI (PSSI, textes interministériels déclarés applicables au niveau du ministère, …) définit la méthode de prise en compte de la sécurité tout au long du cycle de vie des systèmes d'information et la procédure de désignation des différents responsables vis-à-vis de la SSI du système. Cette méthode, applicable aux systèmes d'information traitant des informations Confidentiel-Défense et à leurs éventuels segments d'interconnexion, doit mener à la décision d'homologation de sécurité et à la décision formelle d'emploi.

Article 6

RESPONSABILITÉS SSI

L'autorité qualifiée assume les responsabilités SSI décrites dans [II 900].

Dès lors que le système d'information dépend de plusieurs autorités qualifiées de la SSI, celles-ci désignent, par un protocole d'accord, celle qui endosse la responsabilité pour l'ensemble du système, afin d'être garante de la cohérence de la politique de sécurité et de la coordination des mesures à mettre en œuvre.

Les responsables vis-à-vis de la SSI du système d'information doivent être explicitement désignés, à savoir, conformément [II 900] et [IGI 1300] :

- l'autorité d'homologation, qui s'appuie pour l'instruction de l'homologation et le contrôle permanent de l'état de sécurité du système sur la voie fonctionnelle SSI, représentée par l'agent de sécurité du système d'information (ASSI) conformément à [II 900]. Dès lors que le système concerne plusieurs ASSI, l'autorité d'homologation désigne un coordinateur de ces ASSI ;
- l'autorité responsable de la décision d'emploi du système, qui s'appuie pour la mise en œuvre des conditions d'emploi de sécurité du système découlant de l'homologation sur les administrateurs du système : administrateur de sécurité du système, administrateurs système et réseaux.

Les tâches de l'ASSI sont définies dans [II 900]. Il est également responsable de l'organisation et du contrôle de la mise en œuvre effective des actions correctrices identifiées suite aux audits de sécurité.

L'administrateur de sécurité est responsable devant l'ASSI :
- du paramétrage de la sécurité (application des correctifs de sécurité, des politiques de gestion des mots de passe au niveau des systèmes d'exploitation et des applicatifs, de filtrage au niveau des pare-feu, de chiffrement au niveau des chiffreurs, …) ou de la transmission et du contrôle de la mise en place des paramètres de sécurité applicables à des moyens partagés avec d'autres systèmes ;
- de la gestion des comptes et des droits utilisateurs conformément aux autorisations délivrées par l'autorité responsable de la décision d'emploi du système, ou du contrôle de ces opérations lorsqu'elles sont effectuées par l'administrateur système ;
- de l'exploitation des alertes et journaux de sécurité.

Il constitue le point de contact des utilisateurs et autres administrateurs pour toutes questions relevant de la sécurité « opérationnelle » du système (renouvellement des certificats, des mots de passe, …) et assure la sensibilisation vis-à-vis des risques techniques sur le système.

Quand un événement pouvant mettre en péril la sécurité du système survient, ou quand il détecte une vulnérabilité du système ou de nouveaux risques créés par une évolution dans l'usage du système d'information, l'administrateur de sécurité en rend compte immédiatement à l'ASSI.

Le partage effectif des rôles entre ASSI et administrateurs est précisé dans le dossier de sécurité du système.

L'administrateur de sécurité du système est de préférence distinct de l'administrateur système et réseaux ; cette prescription devient obligatoire dès lors que l'administration du système est externalisée.

La fonction d'auditeur de sécurité est dans la mesure du possible distincte de celle d'administrateur de sécurité.

Article 7

GESTION DES RISQUES

Les informations[6] essentielles doivent être identifiées et leurs besoins de sécurité en termes de disponibilité, intégrité et confidentialité exprimés. C'est pourquoi, il est recommandé, pour la gestion globale des risques sur les systèmes d'information, d'utiliser la méthode EBIOS de la DCSSI, afin que chaque système dispose d'une analyse cohérente et comparable entre systèmes d'information.

Les éléments menaçants tant internes qu'externes doivent être pris en compte. Le risque de niveau stratégique est à considérer, même si la valeur des informations à protéger est Confidentiel-Défense et pas Secret-Défense. De même, les éléments menaçants d'origine terroriste doivent également être pris en compte.

La confrontation des besoins de sécurité aux menaces doit mettre en évidence les risques pesant sur le système d'information étudié. Les objectifs de sécurité indiqueront les risques à traiter.

La présente instruction énonce des mesures de sécurité permettant de répondre de façon concrète à des objectifs de sécurité liés à certaines méthodes d'attaque sur le système d'information :
- l'écoute passive :
  - à l'intérieur d'un bâtiment ;

[6] sans oublier les objets et processus qui participent à la sécurité du système.

  - à l'intérieur d'un site ;
  - entre sites distincts ;
- le vol de matériel (comprenant l'accès illégitime aux supports) ;
- l'accès illégitime aux locaux ;
- l'usurpation de droits ;
- l'altération des données ;
- l'utilisation illicite du matériel ;
- l'interception de signaux compromettants ;
- le piégeage du logiciel.

Cependant, une réflexion doit être menée sur toutes les autres méthodes d'attaque afin de les retenir ou de les écarter explicitement au cours de la démarche de gestion des risques.

Article 8

POLITIQUE DE SÉCURITÉ DU SYSTÈME D'INFORMATION

L'organisme qui met en œuvre un système d'information traitant d'informations de niveau Confidentiel-Défense définit et applique une politique de sécurité du système d'information conformément à [II 900].

Cette politique doit respecter la politique des systèmes d'information de l'organisme.

Elle peut être réalisée à partir du guide d'élaboration d'une PSSI de la DCSSI. Les principes et exigences organisationnels, de mise en œuvre, et techniques doivent garantir que le dispositif de sécurité est crédible et cohérent au regard des objectifs de sécurité identifiés, en particulier qu'il est confié à des personnes ayant les compétences et les moyens d'assurer leur mission, et qu'il est auditable et contrôlable.

Elle est approuvée par l'autorité d'homologation.

Article 9

CONCEPTION ET DÉVELOPPEMENT

La sécurité est indissociable des autres exigences requises pour le système d'information (fonctionnalités, performances, …). Elle doit être prise en compte dans sa conception.

Le système est conçu de manière à protéger également les informations utiles à son fonctionnement, en particulier les informations qui concourent à sa sécurité : paramètres de configuration, droits , traces, …

En complément des moyens de sécurité pour lesquels un agrément au niveau Confidentiel-Défense est requis, la sélection des moyens de sécurité du commerce est effectuée sur la base :

- de leur cohérence avec les objectifs de sécurité exprimés dans la FEROS du système ;
- du résultat positif à une évaluation conduite par un tiers, se traduisant par une certification selon des critères reconnus (Critères Communs, notamment) et par une qualification du produit par la DCSSI au niveau requis pour le besoin de sécurité exprimé ;
- ou à défaut, sur l'avis d'un centre d'expertise technique SSI étatique ou sous contrat.

Le choix des constituants du système prend en compte les éventuels guides (bonnes pratiques, guides de paramétrage et de configuration, …) disponibles auprès des centres d'expertise technique SSI.

Dans le cadre de l'agrément au niveau Confidentiel-Défense, les moyens de sécurité pour lesquels une protection spécifique est requise reçoivent la mention ACSSI et sont gérés conformément aux prescriptions de l'instruction N°910/SGDN/SSD/DR. L'analyse des risques peut conduire à faire porter cette mention ACSSI sur d'autres moyens.

Les mesures de sécurité applicables à l'industriel en charge de l'étude et du développement du système sont définies conformément à l'instruction interministérielle n°2000/SGDN/SSD/DR [II 2000] relative aux conditions de protection du secret et des informations concernant la défense nationale et la sûreté de l'État dans les contrats.

Le passage de marchés au minimum sensibles est requis.

Au-delà des fournitures industrielles attendues en vue de la conduite de l'homologation, par exemple :

- les procédures d'exploitation de la sécurité ;
- les dossiers pour l'évaluation des moyens de sécurité ;

le contrat doit également prévoir la fourniture des moyens (dossiers de conception, code source, résultats de tests, …) permettant de s'assurer que l'autorité d'emploi a bien la maîtrise des accès au système lors de la mise en service, notamment qu'il ne subsiste pas d'accès non documentés constituant des portes dérobées potentielles (mots de passe constructeur, possibilités d'accès distant sans passer par les fonctions de sécurité, journaux des événements non documentés, …).

Article 10

HOMOLOGATION DE SÉCURITÉ ET DÉCISION D'EMPLOI

La procédure générale d'homologation de sécurité décrite dans les textes ministériels est appliquée ; les guides de la DCSSI peuvent servir de trame à la démarche d'homologation de sécurité.

Conformément à [IGI 1300], la décision d'homologation de sécurité s'appuie sur un dossier d'homologation de sécurité. Ce dossier comprend notamment :

- la FEROS ;
- la politique de sécurité du système ;
- les procédures d'exploitation de la sécurité ;
- les certificats des produits (qualifications, agréments, …) ;
- les résultats des tests (comprenant ceux relatifs aux signaux compromettants) et audits menés pour établir la conformité du système avec sa politique de sécurité et ses procédures d'exploitation, et le plan des actions correctrices ;
- le dossier des risques résiduels, établi à partir :
  - de l'analyse de cohérence entre la politique de sécurité du système et les objectifs de sécurité décrits dans la FEROS ;
  - des vulnérabilités résiduelles constatées dans les tests et audits et non corrigées.

La décision d'homologation de sécurité d'un système d'information Confidentiel-Défense est prononcée pour une durée maximale de cinq ans, et est adressée au haut fonctionnaire de défense / fonctionnaire de sécurité des systèmes d'information (HFD/FSSI) du ministère.

Le système d'information fait l'objet d'une décision formelle d'emploi prise par l'autorité responsable de la décision d'emploi du système en s'appuyant sur l'homologation de sécurité du système.

Lorsque l'urgence opérationnelle le requiert, l'homologation de sécurité peut être prononcée postérieurement à la décision d'emploi, qui est alors dite provisoire.

Une décision provisoire d'exploitation peut être donnée pour une durée de six mois, renouvelable une fois seulement : cette décision doit s'accompagner d'un plan d'actions visant à obtenir l'homologation.

Le dossier d'homologation de sécurité est détenu par l'autorité d'homologation, et est accessible à l'ASSI et à l'autorité responsable de la décision d'emploi du système.

Le dossier des risques résiduels est classifié de défense, au minimum au niveau Confidentiel-Défense, et porte la mention Spécial France.

Article 11

RENOUVELLEMENT DE L'HOMOLOGATION DU SYSTÈME D'INFORMATION

En complément des conditions prévues par la PSSI, un système de niveau Confidentiel-Défense fait l'objet d'un renouvellement d'homologation dès lors que :

- celle-ci arrive à échéance;
- le système est amené à traiter des informations de nature différente (par exemple, traitement d'informations de niveau Confidentiel-UE sur un système traitant initialement du Confidentiel-Défense, …) ;
- les conditions d'exploitation du système sont modifiées par rapport au cadre défini par l'homologation (notamment : transfert de responsabilité entre autorités qualifiées, passage d'un mode exclusif à un mode dominant, utilisation en dehors du territoire national d'un système précédemment en usage sur le territoire national, recours à l'externalisation non prévue initialement, extensions, interconnexions, …) ;
- le système a fait l'objet d'une compromission avérée ou d'un incident grave de disponibilité ou d'intégrité ;
- l'autorité d'homologation est informée de résultats d'une inspection ou d'un audit qui remettent en cause l'homologation délivrée.

Article 12

EXPLOITATION ET MAINTIEN EN CONDITION OPÉRATIONNELLE DE LA SÉCURITÉ DU SYSTÈME

Le recours à des prestations externes à l'organisme détenteur des informations Confidentiel-Défense pour l'exploitation ou la maintenance du système, de sa sécurité, ou pour la conduite des actions d'audit, d'inspection de la sécurité du système, est soumis à la décision explicite de l'autorité d'homologation.

Les conditions (contractuelles, techniques, humaines, …) associées sont analysées dans le cadre de la procédure d'homologation de la sécurité.

Des procédures d'exploitation de la sécurité (PES) du système sont définies :

- pour sa gestion courante, notamment :
  - gestion de la configuration matérielle et logicielle ;
  - gestion des supports ;
  - gestion de l'archivage;
  - application des sauvegardes et tests de restauration ;
- pour la gestion et l'exploitation des moyens de sécurité, notamment :
  - gestion des comptes ;
  - gestion des politiques de chiffrement, de filtrage, … ;

- suivi continu des vulnérabilités liées aux technologies de l'information et de leur impact sur la sécurité du système, notamment par le suivi et l'application des avis du CERTA ;
- suivi de l'état de l'art des produits de sécurité et l'actualisation des outils concourant au maintien en condition de sécurité ;
- suivi des opérations de maintenance des constituants du système d'information offrant des fonctions de sécurité ;

- pour la gestion de procédures particulières, notamment :
  - audits de sécurité, à conduire au minimum à l'occasion du renouvellement d'homologation du système, et dont les plans d'action doivent être respectés ;
  - intégration du système dans le champ d'application d'un réseau de veille et d'alerte ;
  - application des plans gouvernementaux VIGIPIRATE et PIRANET si le niveau de criticité du système l'impose ;
  - traitement des incidents et la liaison avec le réseau d'alerte ;
  - processus de retrait de service de constituants du système voire du système complet (inventaire des supports, destruction, …).

Les PES, comprenant les fiches réflexes, sont accessibles aux utilisateurs et aux acteurs concernés par la mise en œuvre du système (administrateurs,…). Le niveau de protection des procédures d'exploitation et de la documentation décrivant les éléments concourant directement à la sécurité du système d'information (paramétrage des dispositifs de sécurité, …) est déterminé par l'ASSI.

Article 13

GESTION DES INCIDENTS

La PSSI du système, ou si elle existe, de l'organisme, définit la politique d'alerte et de traitement des incidents, et en particulier :

- les conditions d'information des niveaux supérieurs (autorité hiérarchique, autorité qualifiée, HFD/FSSI, …) et, quand elles existent, des cellules de veille SSI ;
- les modalités d'instruction des événements : recherche de l'origine des incidents, application de correctifs, …

Cette politique est déclinée en procédures d'exploitation de sécurité du système, qui se traduisent de préférence par des fiches réflexes, actualisées en particulier en fonction du retour d'expérience et du traitement des incidents déjà rencontrés.

Les personnels travaillant sur les systèmes Confidentiel-Défense doivent être sensibilisés et faire preuve d'une vigilance permanente : il doit être rendu compte immédiatement de tout événement de sécurité (incident, découverte de compromission possible sur le système ou dans son environnement d'exploitation immédiat, …).

Dans le cas d'interconnexions entre plusieurs ministères, les modalités du protocole d'accord pour l'interconnexion sont appliquées pour l'information mutuelle et le traitement des événements.

Si un système d'information multinational (UE, OTAN, , …) est concerné, le SGDN est également informé sans délai.

Article 14

GESTION DES COMPROMISSIONS

L'atteinte à la protection des informations de niveau Confidentiel-Défense relève du code pénal qui sanctionne la destruction, la soustraction, l'altération, le détournement et la divulgation. La disparition de supports protégés d'information est traitée comme une compromission possible. En complément aux procédures de traitement des incidents, les compromissions possibles ou avérées font l'objet des mesures prescrites à l'article 88 de [IGI 1300].

Les investigations en vue de détecter une éventuelle compromission doivent respecter la notion de « preuves informatiques ». Elles imposent en général de procéder à des mesures conservatoires adéquates[7] de constituants du système d'information, à l'analyse de journaux d'événements, …, et peuvent conduire à suspendre le fonctionnement de tout ou partie du système.

Toute investigation susceptible de détruire des éléments de preuves et de compromettre la valeur des traces est formellement proscrite.

[7] Pour l'analyse après incident d'une machine que l'on craint compromise.

TITRE II

EXIGENCES DE SÉCURITÉ PHYSIQUE

Article 15

PRINCIPES DE PROTECTION PHYSIQUE

Les moyens de protection physique, définis dans [D 1223], portent sur :

- l'environnement du système d'information : les sites, les zones ou les bâtiments, les locaux, les meubles ;
- les constituants du système d'information :
  - serveurs,
  - postes de travail,
  - équipements et supports de transmission,
  - terminaux inscrivant des supports amovibles (imprimantes, baies de stockage ou de sauvegarde, traceurs, ...),
  - moyens de sécurité et documents ou dispositifs associés (clés, dispositifs d'authentification, …),
  - supports de données ou de programmes, …
- les personnels accédant, en permanence ou non, au système d'information ou à son environnement immédiat (comprenant la documentation du système).

Les mesures de protection physique doivent respecter le principe de la défense en profondeur, fondé sur l'adoption d'un ensemble de mesures de protection, de détection, d'alarme et d'intervention. Pour cela, on adopte, conformément aux pratiques internationales en vigueur (OTAN et UE), les trois niveaux d'environnement suivants :

- l'environnement de sécurité physique global (désigné dans la suite de la présente instruction par GSE[8]), qui désigne l'environnement physique général dans lequel est situé le système, par exemple : la base aérienne, le commissariat, le consulat ou l'ambassade ;
- l'environnement de sécurité local (désigné dans la suite de la présente instruction par LSE), inclus dans le GSE, qui recouvre l'environnement de sécurité physique, du personnel, documentaire et procédurale relevant du domaine de l'autorité d'homologation ;
- l'environnement de sécurité électronique (ESE), inclus dans le LSE, qui désigne les mesures techniques de sécurité mises en place au niveau du système.

Les mesures liées au troisième niveau relèvent ici de la protection logique et sont définies au Titre III, en fonction notamment des mesures apportées au niveau physique.

Conformément à [IGI 1300] :

- si les informations Confidentiel-Défense sont traitées dans une zone réservée[9], elle-même incluse dans une zone protégée[10], les règles définies dans [IGI 1300] s'appliquent strictement;
- sinon, elles doivent être traitées dans un local ou une zone sécurisée[11], dont la présente instruction définit les caractéristiques minimales en les répartissant sur les GSE et LSE.

---

[8] Les acronymes GSE, LSE et ESE sont basés sur la terminologie anglo-saxonne (voir le glossaire), car ils n'ont malheureusement pas été traduits dans les versions françaises des documents internationaux les utilisant.

[9] La zone réservée peut accueillir plusieurs LSE.

[10] La zone protégée est incluse dans une GSE.

[11] Ce local ou cette zone sécurisée peut être situé ou non dans une zone protégée. Une zone sécurisée peut englober plusieurs LSE ; a contrario, un local sécurisé peut être créé pour chaque LSE.

La protection physique des informations ou supports protégés respecte [D 1223], le niveau minimum des classes applicables étant défini ci-après selon les types d'environnement (GSE et LSE).

Les mesures de protection contre les signaux compromettants définies dans l'instruction n°300/SGDN/TTS/SSI/DR du 20 juin 1997 sont appliquées. Il doit être impossible, au-delà de la zone de sécurité de l'organisme, de capter des informations par le biais des signaux compromettants :

- la directive n°495/SGDN/TTS/SI/DR est appliquée de manière à ce que la zone de sécurité ne dépasse pas les limites du GSE ;
- le choix des pièces abritant les LSE est déterminé notamment à partir des résultats du zonage des locaux conformément à la directive n°495/SGDN/TTS/SI/DR, afin de faciliter le recours à des matériels commerciaux conformément aux règles de la directive n°485/SGDN/DISSI/SCSSI/DR.

Dans le cas où le système Confidentiel-Défense cohabite avec un système de niveau inférieur ou un système étranger, une analyse de vulnérabilité des signaux compromettants est menée pour évaluer les risques résiduels liés à la proximité des équipements, et adapter la nature des moyens de protection (catégorie des équipements, recours à une cage de Faraday, …) à la menace.

Les circonstances exceptionnelles (urgence, sécurité incendie, intervention sur le système, …) ou les événements planifiés (travaux d'infra, visites officielles, ...) conduisant des personnes étrangères au service à accéder aux locaux hébergeant un système d'information de niveau Confidentiel-Défense sont également prévues et formalisées dans les procédures d'exploitation de la sécurité.

Dès lors qu'un constituant du système ne bénéficie plus de la protection offerte par les niveaux d'environnement GSE et LSE, des conditions particulières d'emploi sont définies :

- l'exploitation de matériels en transit en vue du traitement de données Confidentiel-Défense est a priori interdite, ces équipements étant alors considérés et traités comme des supports ;
- les exigences particulières pour les postes nomades sont définies au titre VI.

Les informations relatives à la configuration physique et aux mécanismes de protection physique du système d'information ne doivent être accessibles qu'aux personnes autorisées.

Article 16

MESURES AU NIVEAU DU GSE

MESURES DE PROTECTION

Le GSE est délimité par une barrière physique correspondant au minimum aux bâtiments ou emprises de la classe 3 de [D 1223].

Un contrôle d'accès est mis en œuvre ; seules les personnes autorisées entrent dans le GSE, et des dispositions permanentes sont prises pour qu'aucun moyen d'interception ou d'écoute ne puisse être installé de manière illicite dans le GSE.

En fonction des objectifs de disponibilité requis pour le système, les locaux hébergeant les équipements d'environnement nécessaires au bon fonctionnement du site (climatisation, alimentation électrique, protection incendie...) font l'objet de mesures propres à assurer leur protection, notamment s'il n'a pas été possible de les placer en zone réservée ou sécurisée.

MESURES DE DÉTECTION

Les mesures de détection au sein du GSE sont assurées :

- soit par des rondes de surveillance ;
- soit par un dispositif de surveillance (télévision en circuit fermé, …) ou de détection d'intrusion (détecteur de mouvement, …) relié à une équipe d'intervention.

Si ces prestations sont externalisées, elles font l'objet d'un marché classé ou à clause de sécurité. Les instructions d'emploi et le plan des dispositifs sont considérés comme des documents protégés.

MESURES DE REACTION

Des mesures de réaction sont définies localement, en fonction de la nature juridique (zone protégée, …) du GSE.

Article 17

MESURES AU NIVEAU DU LSE

MESURES DE PROTECTION

L'accès au LSE est protégé par une barrière physique supplémentaire à celle du GSE, établie au niveau de la zone sécurisée ou du local sécurisé et correspondant au minimum aux locaux de la classe d de [D 1223].

Un contrôle d'accès est mis en œuvre, pour ne laisser entrer que les personnes autorisées dans le LSE.

Si le LSE est tel que le fait de pénétrer dans cet environnement équivaut en pratique à avoir accès aux informations Confidentiel-Défense (correspondant à une zone de classe ou catégorie I[12]), seules les personnes habilitées et ayant besoin d'en connaître peuvent y accéder.

Pour un LSE dans lequel des contrôles internes d'accès aux informations sont possibles (correspondant à une zone de classe ou catégorie II), les personnes non habilitées doivent être accompagnées en permanence.

Les périphériques (clavier, souris, …), et les protocoles et technologies de communication sans fil susceptibles d'induire des signaux compromettants sont interdits d'emploi au sein du LSE, sauf autorisation explicite selon les conditions d'emploi (cohérence avec la limite de sécurité définie par le zonage, et moyennant des procédures d'exploitation de la sécurité adaptées) définies dans le cadre de l'homologation. Des procédures d'acquisition, de configuration et de contrôle programmé ou inopiné des équipements sont identifiées dans les PES afin de vérifier le respect dans le temps de cette exigence.

Les constituants d'autres systèmes d'information de niveau de protection différent, de téléphonie, de télécopie, … co-localisés avec les constituants du système au sein du LSE, ne doivent pas remettre en cause le niveau de protection conféré au système d'information Confidentiel-Défense.

MESURES DE DÉTECTION

Les mesures de détection prévues par l'article 16 s'appliquent également au sein du LSE.

En complément, tout accès et ouverture d'une ressource critique (équipement de sécurité, serveur, routeur, …) du système d'information doit être détectable.

[12] Au niveau de l'OTAN et de l'Union européenne, le LSE s'appuie sur des zones de classe (ou catégorie) I ou II telles que décrites dans les documents CM (2002)49 sur la sécurité dans l'organisation de l'Atlantique Nord, et les règlements de sécurité du Conseil et de la Commission de l'Union européenne.

MESURES DE RÉACTION

Des mesures de réaction sont définies localement, en fonction de la nature juridique du LSE.

Conformément à [IGI 1300], un plan d'évacuation d'urgence et un plan de destruction d'urgence sont tenus à jour au niveau de chaque LSE par l'officier de sécurité.

MESURES SPÉCIFIQUES POUR LES SERVEURS

Les serveurs ou autres équipements en fonctionnement permanent, manipulant de l'information Confidentiel-Défense en clair hors de la présence de personnel, sont intégrés dans un LSE soumis à des mesures de protection renforcées, correspondant au minimum aux locaux de la classe c de [D 1223].

Article 18

MESURES COMPLÉMENTAIRES POUR L'INFRASTRUCTURE DE COMMMUNICATION

CÂBLAGE

L'installation du câblage réseau doit respecter les exigences de la directive n°485/SGDN/DISSI/SCSSI/DR, en s'appuyant sur les recommandations de la DCSSI.

Le câblage véhiculant en clair les informations classifiées Confidentiel-Défense est confiné à l'intérieur de l'environnement de sécurité local (LSE), il est réalisé de manière à permettre un contrôle visuel rapide de son ensemble :

- il permet de constituer des réseaux physiquement dissociés dans la zone sécurisée ;
- l'infrastructure de câblage est facilement inspectable.

Seuls les câbles sortant d'équipements de chiffrement agréés et véhiculant de l'information chiffrée peuvent sortir du LSE.

Dans le cas où l'autorité qualifiée prend la responsabilité d'utiliser des circuits approuvés entre différents LSE implantés au sein de la même emprise (GSE), en remplacement de la mise en œuvre de moyens de chiffrement agréés, une cartographie précise du câblage est détenue par l'ASSI, et des procédures spécifiques d'exploitation de la sécurité sont établies (contrôles d'intégrité aléatoires du câblage,…).

Dans tous les cas, les règles d'installation permettent la vérification visuelle d'intégrité du câblage.

Les procédures d'exploitation du système prévoient une inspection visuelle périodique de l'ensemble du câblage, au moins annuelle.

LOCAUX TECHNIQUES

Les locaux techniques abritant les éléments actifs de réseau (routeurs, commutateurs, …), les armoires de brassage le cas échéant, les systèmes d'administration, de supervision et les dispositifs de filtrage et de chiffrement assurant l'interface avec les réseaux extérieurs (réseau de transit ou réseau de desserte d'un niveau inférieur) sont spécifiques, et leur accès est limité aux personnels habilités justifiant d'un besoin spécifique d'y pénétrer.

Les mesures de protection des LSE correspondants sont conformes aux locaux de la classe c de [D 1223].

Article 19

MESURES COMPLÉMENTAIRES POUR LES SUPPORTS PHYSIQUES

Les supports physiques considérés peuvent être à base de cartes (carte à puce, ...), magnétiques de transfert (disques amovibles, disquette, ZIP, cassette à bandes, ...), magnétiques de masse (disque dur, carte mémoire, ...), optiques (CD-ROM, CD Réinscriptibles, DVD, ...), à base de composants électroniques (clé USB, PDA, …), …

RÈGLES D'ACQUISITION

Les actes contractuels d'approvisionnement et de maintenance d'équipements qui intègrent des supports physiques pour traiter d'informations Confidentiel-Défense comprennent des clauses de non retour de ces supports chez les fournisseurs, applicables dès lors que ces supports sont entrés en service dans le système.

RÈGLES DE GESTION

Les supports physiques contenant ou ayant contenu des informations Confidentiel-Défense sont marqués physiquement, manipulés et stockés de la même façon que les documents papiers classifiés de niveau Confidentiel-Défense, conformément aux règles de [IGI 1300].

Les supports amovibles ainsi marqués sont mis en armoire forte en dehors des horaires de travail ou en cas d'absence prolongée du détenteur.

Toutes les opérations sur les supports de données (accès, mouvement, modification, entretien, maintenance, ...) sont effectuées par des personnes habilitées.

Des supports physiques spécifiquement marqués permettent les importations sur le système à partir d'autres systèmes, et les exportations depuis le système vers d'autres systèmes. Ces supports sont audités périodiquement afin de s'assurer qu'ils ne contiennent pas d'informations Confidentiel-Défense.

Les moyens (lecteurs de disquettes, graveurs, imprimantes, …) permettant la gestion de ces supports spécifiques sont identifiés et font l'objet de procédures d'exploitation visant à assurer qu'ils sont:

- explicitement autorisés ;
- explicitement attribués à des utilisateurs identifiés ou mutualisés dans le cadre des procédures d'exploitation de sécurité du système.

Tous les moyens non explicitement autorisés dans les procédures d'exploitation de sécurité sont verrouillés physiquement ou logiquement, selon le besoin et les possibilités techniques.

Dès lors qu'un support a traité de l'information Confidentiel-Défense, on lui applique de manière permanente les règles de protection définies dans cette instruction : par défaut, ce composant n'est pas réaffecté à un système de niveau différencié (exemples : niveau inférieur, système interallié, éventuellement besoin d'en connaître distinct).

DESTRUCTION DES SUPPORTS D'INFORMATION

En l'absence de moyen d'effacement agréé, les supports ne sont pas déclassifiés ou requalifiés. Dès lors qu'ils ne sont plus utiles ou utilisables sur le système, ils sont détruits. Les moyens de destruction sont adaptés aux types de supports à détruire conformément à la directive n°36/SGDN/SSD/DR.

Les supports à détruire sont stockés dans un local sécurisé jusqu'à leur destruction.

La destruction des supports est réalisée par des personnes habilitées et toute destruction est enregistrée.

TITRE III

EXIGENCES DE SÉCURITÉ LOGIQUE

Article 20

COHÉRENCE DES MESURES DE PROTECTION PHYSIQUE ET LOGIQUE ET GESTION DU BESOIN D'EN CONNAÎTRE

Dès lors que sont mis en œuvre, en lieu et place d'une barrière physique, des moyens de protection logique :

- un ou des moyens de détection, qui peuvent être des dispositifs logiques internes au système d'information, sont alors associés à chaque barrière logique, et provoquent les interventions prévues dans les procédures d'exploitation de la sécurité ;
- cette répartition et le choix des moyens de protection, de détection et de réaction sont décrits et justifiés dans le dossier de sécurité du système d'information.

Un même dispositif ne permet de franchir un ensemble de barrières que s'il met en jeu des mécanismes ou paramètres différents[13].

Les procédures d'exploitation de sécurité décrivent précisément les modalités d'accès physique et logique de l'ensemble des catégories de personnels à l'environnement et aux différents constituants du système, en fonction notamment de leur habilitation et de leur besoin d'en connaître. L'accès doit s'appuyer au minimum sur des identifiants personnels et nominatifs, afin de permettre une imputabilité des accès et des actions. Il doit être géré de manière harmonisée entre les responsables des environnements physiques et logiques.

Des profils, auxquels sont associés des privilèges, dissocient les prérogatives de chacune des catégories précédentes, selon le principe du moindre privilège.

Article 21

PROTECTION DES POSTES DE TRAVAIL, DES SERVEURS ET DES RÉSEAUX LOCAUX

L'analyse de sécurité définit les zones dans lesquelles l'information classifiée peut être traitée en clair.

La configuration et la gestion des postes de travail, des serveurs et des réseaux locaux s'appuient sur les guides de la DCSSI ou ministériels.

Le démarrage des postes utilisateurs ou des serveurs ne s'effectue que sur des médias contrôlés, et les opérations de démarrage ("boot") sur disquette, bande, CD-ROM, …, sont strictement réglementées et encadrées par les PES, y compris pour la maintenance. L'utilisateur n'a pas accès à la configuration matérielle du poste de travail (BIOS, carte mère).

Chaque utilisateur s'identifie et s'authentifie pour toute utilisation d'un poste de travail.

Les moyens d'authentification ne doivent pas permettre le rejeu : en particulier, les éléments d'authentification associés sont protégés par les utilisateurs et le système.

---

[13] Exemple : une même carte à puce peut servir au franchissement de plusieurs barrières, mais avec des jeux de clés et d'authentifiants différents.

Les sessions sont limitées en durée : la périodicité de ré-authentification et/ou la durée d'inactivité au-delà de laquelle l'utilisateur est déconnecté sont spécifiées dans les PES.

Les sessions authentifiées sont tracées. De même, les tentatives d'authentification se soldant par un échec sont tracées, et elles génèrent une alerte et un verrouillage des postes concernés au-delà d'un nombre d'échecs spécifié dans les PES.

Le système informe l'utilisateur que seuls les utilisateurs autorisés peuvent accéder au système et que celui-ci est surveillé pour détecter les utilisations non autorisées.

Seuls les équipements mobiles (PDA, téléphones et ordinateurs portables, clés USB, appareils photo numériques, ...) mis à disposition par l'autorité d'emploi dans le cadre du service sont autorisés au sein du LSE, selon les procédures d'exploitation de la sécurité définies dans le cadre de l'homologation ; en revanche il est interdit de connecter les équipements personnels avec le système.

Article 22

PROTECTION DES ÉCHANGES D'INFORMATION

La protection des échanges entre les zones dans lesquelles l'information peut être traitée en clair est offerte :

- par des moyens de chiffrement agréés[14] au niveau Confidentiel-Défense au minimum, dès lors que les échanges se font entre deux GSE ;
- selon les résultats d'une analyse de risques, dès lors que les échanges se font entre deux LSE situés dans une même GSE : dans ce cas, une formalisation consistant en l'approbation du circuit (voir article 18) est prononcée par l'autorité qualifiée, qui peut en outre demander un renforcement de la protection physique par l'utilisation de moyens de protection logiques complémentaires non nécessairement agréés mais préférablement qualifiés.

Article 23

MARQUAGE

Le marquage de l'information et des supports classifiés est conforme aux règles de [IGI 1300].

L'objectif des mesures ci-après est que l'utilisateur ait toujours conscience du niveau de classification des informations qu'il traite.

Ainsi, le niveau de l'information, même à l'état de document de travail, apparaît à tout accédant au système :

- par marquage du niveau de classification de l'information, de la durée de validité correspondante si elle est connue, des mentions d'appartenance et de manipulation au plus près de l'information : en-tête et pied de page, enregistrement pour une base de données, en-tête ou corps d'un message, …;
- ou à défaut par dépôt de l'information dans des supports logiques (fichier, répertoire, …), ostensiblement dédiés à ce niveau ;
- la consultation et l'impression d'informations Confidentiel-Défense font apparaître le niveau de classification de l'information, conformément aux modèles de timbre figurant à la fin de la présente instruction (couleur, …).

Le nom du support logique des informations (nom de fichier, titre d'un message, …), comprenant le marquage, ne doit pas constituer en soi une information Confidentiel-Défense.

[14] voir l'annexe I.

Il est conseillé de marquer également les informations sensibles non classifiées de défense et les informations non protégées (par exemple : «explicitement autorisé à sortir sur Internet »).

Les outils et méthodes de marquage doivent permettre de requalifier l'information prévue pour être transmise aux alliés, conformément aux accords de sécurité, en conservant par défaut le niveau de protection initial.

Article 24

DROIT D'ACCÈS AUX DONNÉES DE CONFIGURATION, DE GESTION ET D'ADMINISTRATION

Les informations relatives à la topologie du système d'information (adresses des serveurs, des postes, des éléments actifs de réseau, annuaires, éléments de routage,…) ne sont accessibles qu'aux personnes autorisées identifiées dans les PES.

Les données d'administration et de sécurité, comme elles sont vitales pour le système d'information (authentification, droits d'accès, comptes administrateurs, données de filtrage des gardes de sécurité, …), ne doivent être accessibles qu'aux personnes autorisées, via des canaux sécurisés[15] garantissant l'authenticité et la confidentialité des opérations sur ces données.

Sauf cas exceptionnel, les utilisateurs ne sont pas administrateurs du système.

Article 25

DROIT D'ACCÈS AUX INFORMATIONS

Les droits d'accès à chaque fichier ou collection de données (répertoire, base de données, …) Confidentiel-Défense sont gérés. À toute personne accédant au système est associé un profil définissant ses droits d'accès aux différentes ressources limité à son seul besoin d'en connaître.

Les comptes sont affectés individuellement ; dans le cas contraire, des mesures organisationnelles doivent permettre d'identifier l'utilisateur.

Lorsque plusieurs personnes doivent accéder à l'information, il est conseillé de la conserver dans une ressource partagée et gérée afin d'éviter les copies multiples.

Article 26

IMPUTATION DES ACTIONS, JOURNALISATION, ALARMES

L'imputation des actions doit permettre de tracer les actions conformément à la politique de sécurité du système et de disposer de suffisamment de traces pour mener les investigations dans le cas d'une compromission.

[15] Le niveau de sécurité requis pour les différents mécanismes dépend de l'architecture du système et des conditions de mise en œuvre de l'administration (locale, distante, …). En première approche, il doit être identique au minimum à celui requis pour la protection des données des utilisateurs sur le système, mais l'analyse des risques peut amener à modifier ce niveau.

Les actions qui doivent être imputées individuellement (éventuellement par le rapprochement de traces élémentaires) sont au minimum :

- les ouvertures et échecs d'ouvertures de sessions ;
- la modification des droits d'accès à l'information Confidentiel-Défense ;
- l'accès aux données de configuration, de gestion et d'administration ;
- l'exportation d'informations Confidentiel-Défense sur tous types de périphériques (imprimante, support amovible, réseau, …).

En complément, il est souhaitable d'imputer l'accès à chaque information Confidentiel-Défense, ainsi que les échanges d'information Confidentiel-Défense.

Les événements de sécurité sont journalisés.

Les journaux qui conservent les informations d'imputation et les événements de sécurité sont protégés en intégrité et en disponibilité. Ils font l'objet d'une procédure d'archivage approuvée dans le cadre de l'homologation, la durée de conservation minimale recommandée étant d'un an.

Ils ne sont accessibles qu'aux personnes autorisées.

Les événements de sécurité remontent à l'administrateur sécurité du système d'information, qui en rend compte à l'ASSI. Certains événements traduisant une violation potentielle de la sécurité font l'objet d'alarmes de sécurité remontant immédiatement à l'administrateur sécurité, et peuvent, le cas échéant, impliquer une réaction automatique du système.

Les journaux doivent pouvoir constituer des éléments de preuve dans le cadre d'une enquête : cela doit être réalisé par des mesures organisationnelles (conservation dans des armoires fortes à accès contrôlé, …) et/ou technique (signature électronique, …), définies selon les analyses de risques et actualisées selon la jurisprudence.

Article 27

PROTECTION CONTRE LES CODES ET PROGRAMMES MALICIEUX

Tout système d'information traitant des informations Confidentiel-Défense est équipé d'au moins un moyen d'un moyen de surveillance de l'intégrité des données et du système (anti-virus,…), mis à jour conformément aux directives des systèmes de veille et alerte.

Dès lors qu'une information est importée depuis un environnement non déclaré de confiance par l'autorité qualifiée, un contrôle additionnel (exemples : second anti-virus, filtrage des types de fichiers autorisés à être importés, blocage ou contrôle de la signature des codes mobiles, …) est effectué, afin de s'assurer que les données importées ne sont pas susceptibles de mettre en cause la sécurité du système.

Les systèmes d'exploitation et autres logiciels sont mis à jour selon des processus prévus dans les PES.

Les utilisateurs sont informés des risques liés aux codes et programmes malicieux.

Article 28

MAÎTRISE DE LA CONFIGURATION DU SYSTÈME D'INFORMATION

Les composants du système (systèmes d'exploitation, …) utilisés pour le traitement de données Confidentiel-Défense sont configurés :

- selon le strict besoin fonctionnel et technique du système (exemple : droits d'accès, services, ports, …) ;
- selon les guides de configuration et recommandations interministériels et ministériels en vigueur.

Toutes les fonctions qui ne sont pas nécessaires au bon fonctionnement du système d'information sont désactivées dans la mesure du possible.

Tous les éléments et composants du système sont gérés en configuration et documentés.

Un contrôle de l'intégrité des logiciels du système et de leurs paramètres de configuration par rapport à une version de référence est effectué périodiquement.

Les mises à jour ou correctifs des logiciels, ainsi que l'ajout de nouveaux logiciels, l'installation ou la modification de tout matériel ou périphérique, ne peuvent être effectués qu'avec l'accord d'un administrateur du système. Dans tous les cas, une analyse de la non-régression des fonctions de sécurité et de la sécurité globale du système est effectuée, ses résultats pouvant conduire au lancement d'une procédure de renouvellement d'homologation.

Des mesures particulières peuvent être définies pour des logiciels qui nécessitent par nature une mise à jour fréquente (anti-virus, correctifs de sécurité, …) ; les modalités de mise à jour sont alors formalisées dans les PES.

Le raccordement de machines non explicitement prévues comme faisant partie des constituants du système est interdit par des mesures techniques, ou à défaut contrôlé par des mesures organisationnelles.

Article 29

SAUVEGARDE ET RESTAURATION

Des sauvegardes périodiques sont effectuées et leurs restaurations régulièrement testées.

Les sauvegardes effectuées sur un système traitant d'informations Confidentiel-Défense sont protégées au moins au niveau Confidentiel-Défense.

TITRE IV

EXIGENCES SUR LE PERSONNEL

Article 30

POUR L'UTILISATION ET L'EXPLOITATION DU SYSTÈME

Les personnes accédant au système d'information sont habilitées selon le besoin du service en fonction du catalogue des emplois et du poste effectivement tenu, à savoir :

- les utilisateurs, au niveau Confidentiel-Défense ;
- les administrateurs système, réseau et sécurité, au niveau Secret-Défense.

Les règles spécifiques relatives aux ACSSI définies par l'instruction interministérielle n°910/SGDN/SSD/DR s'appliquent aux personnes qui manipulent les constituants ayant reçu cette mention.

Les utilisateurs étrangers habilités au niveau Confidentiel-Défense ne doivent pas pouvoir accéder à des informations et supports protégés Spécial France, ou faisant l'objet de restriction de diffusion au titre d'accords de sécurité avec d'autres pays ou organisations.

L'utilisateur est tenu responsable des importations et des exportations d'informations via des supports physiques sur le système. Les exportations d'informations, quel que soit le procédé retenu, ne sont autorisées qu'à des utilisateurs spécifiquement désignés, et sont réalisées sous la responsabilité de l'émetteur de l'information qui doit déclarer le niveau de classification de l'information.

Article 31

RÉALISATION ET MAINTENANCE DU SYSTÈME

Les prescriptions de [II 2000] concernant les sociétés intervenant au titre de marchés et autres contrats de maintenance des matériels et logiciels ou de marchés d'études (informatique, télécommunication, électronique, …) et les types de marchés passés s'appliquent. Des conditions sont prévues pour le remplacement des personnes au sein des équipes constituées.

Les personnes de ces sociétés qui ont, dans le cadre de leurs interventions, accès à des informations ou supports protégés, doivent être habilitées au niveau Confidentiel-Défense.

Toute intervention de maintenance des matériels et logiciels ou d'études est effectuée sous contrôle d'une personne mandatée par l'entité d'emploi du système, habilitée et qualifiée, apte à s'assurer que l'intervenant :

- n'accède qu'à l'information dont il a besoin de connaître pour son opération ;
- ne procède pas à l'export d'informations ou supports protégés, sauf si cela est explicitement prévu par le contrat ;
- ne modifie pas indûment la configuration ou les données du système et de son environnement physique de sécurité (LSE).

Le recours à des spécialistes non habilités pour effectuer une opération de maintenance des matériels et logiciels ou d'études doit être exceptionnel (urgence opérationnelle, savoir-faire exclusif, …) et se faire exclusivement après accord écrit de l'autorité d'emploi et de l'ASSI.

Toutes mesures doivent être prises pour que ces spécialistes ne puissent avoir connaissance, même fortuitement, d'informations Confidentiel-Défense.

De même que pour les personnes dûment habilitées, leurs interventions sont effectuées sous contrôle d'une personne mandatée par l'entité d'emploi du système, habilitée et qualifiée, apte à s'assurer que l'intervenant :

- n'accède qu'à l'information dont il a besoin de connaître pour son opération ;
- ne procède pas à l'export d'informations ou supports protégés, sauf si cela est explicitement prévu par le contrat ;
- ne modifie pas indûment la configuration ou les données du système et de son environnement physique de sécurité (LSE).

De manière générale, les équipements, documents et informations mis à la disposition de ces intervenants externes doivent être strictement limités à ceux nécessaires à leur intervention.

Des dispositions techniques accompagnent également leurs opérations : dans la mesure du possible, une sauvegarde initiale et une vérification sont réalisées.

Les clauses contractuelles des marchés de soutien doivent prévoir :

- que les équipes d'interventions externes ne puissent pas introduire dans le système des matériels et logiciels ne faisant pas partie de la configuration approuvée du système ou susceptibles d'exporter des informations classifiées ;
- l'approvisionnement ou la fourniture par l'administration des équipements et outils nécessaires.

Seule la télémaintenance depuis une zone de sécurité respectant des mesures physiques et logiques offrant un niveau de protection global équivalent à celle du système et faisant partie du périmètre d'homologation du système est autorisée : les procédures et les réseaux utilisés doivent être maîtrisés et faire partie des spécifications du système d'information. Un suivi des opérations et leur imputation à une personne sont obligatoires.

Article 32

AUDITS ET INSPECTIONS DE SÉCURITÉ DU SYSTÈME

Les personnes en charge des audits et inspections de sécurité sont habilitées au niveau Secret-Défense. Les résultats des audits et inspections de sécurité sont classifiés au minimum au niveau Confidentiel-Défense Spécial France.

Conformément à [IGI 1300], les rapports de synthèses comprenant les mesures préconisées pour rectifier les déficiences constatées et leur planification sont adressés aux autorités responsables des organismes contrôlés et aux autorités ministérielles de tutelle.

Préalablement à l'audit ou l'inspection de sécurité, le contrat ou une convention établie entre le commanditaire et l'équipe d'audit définit notamment :

- le système cible ;
- les modalités d'intervention ;
- le mode de diffusion et de conservation des résultats.

Dans le cas où il est fait appel à une société pour ce type de prestation, outre les exigences précédentes :

- cette société est habilitée au niveau Secret-Défense ;
- le marché passé est classé ou à clause de sécurité ;

- les résultats des audits et inspections de sécurité ne sont pas conservés par le prestataire, qui ne pourra en outre faire publicité de son intervention qu'avec l'accord écrit du commanditaire au titre du contrat ;
- les interventions sont effectuées sous contrôle d'une personne mandatée par l'entité d'emploi du système ou par une autorité de contrôle, habilitée et qualifiée, apte à s'assurer que l'intervenant :
  - n'accède qu'à l'information dont il a besoin de connaître pour son opération ;
  - ne procède pas à l'export d'informations ou supports protégés, sauf si cela est explicitement prévu par le contrat ;
  - ne modifie pas indûment la configuration ou les données du système et de son environnement physique de sécurité (LSE).

Afin de permettre d'affiner les spécifications de systèmes, les vulnérabilités techniques ou procédurales apparues à l'occasion des audits sont adressées, après démarquage, au centre d'expertise technique SSI du ministère.

Article 33

MESURES CONCERNANT LE PERSONNEL D'ENTRETIEN OU DE MAINTENANCE

Les personnes chargées de l'entretien ou de la réparation et de la maintenance des bâtiments, des équipements non informatiques, du nettoyage, peuvent ne pas être habilitées : dans ce cas elles interviennent uniquement sous contrôle permanent.

TITRE V

EXIGENCES POUR LES INTERCONNEXIONS

Article 34

CONDITIONS REQUISES POUR L'INTERCONNEXION

Toute interconnexion est soumise à l'application d'une démarche de sécurité spécifique, conformément aux directives d'interconnexion en vigueur.

Pour un système Confidentiel-Défense devant être interconnecté avec un système de même niveau, ayant lui-aussi ayant fait l'objet d'une homologation, l'architecture d'interconnexion est analysée en fonction de la cohérence des politiques de sécurité des systèmes à interconnecter :

- si les politiques des deux systèmes sont différentes, l'architecture d'interconnexion basée sur une zone tampon s'applique strictement ;
- sinon, l'analyse de risque doit justifier la possibilité de simplifier cette architecture, en s'appuyant sur des moyens de gestion du besoin d'en connaître (VLAN, …).

Dès lors que l'interconnexion impose le transit d'informations Confidentiel-Défense entre des GSE distinctes, alors ces informations sont chiffrées par des moyens agréés.

Si le système Confidentiel-Défense doit être interconnecté avec un système de niveau inférieur :

- on utilise des moyens agréés permettant de garantir que :
  - seules les informations de niveau inférieur au niveau Confidentiel-Défense et susceptibles d'être échangées avec le niveau inférieur peuvent sortir du système Confidentiel-Défense;
  - les sorties d'information sont réalisées sous la volonté et le contrôle de l'émetteur ;
  - ces actions sont toujours journalisées et imputées à l'émetteur ;
- sinon, seules les importations d'informations à partir du système de niveau inférieur sont autorisées, via une architecture homologuée mettant en œuvre une zone tampon sous la responsabilité de l'autorité d'emploi du système Confidentiel-Défense et en s'appuyant sur un/des moyen(s) agréés de transfert unidirectionnel d'informations ; ces importations sont journalisées.

L'application de la démarche doit permettre à toute autorité qualifiée de juger de l'intérêt et du risque d'interconnexion du système Confidentiel-Défense dont elle est responsable en matière de sécurité.

Cette démarche, pour être appliquée efficacement, doit être planifiée et gérée. En particulier, le choix des architectures et des moyens est très critique pour autoriser ou non les interconnexions, notamment vis-à-vis des systèmes étrangers ou de coalition.

Le HFD/FSSI est informé des interconnexions des systèmes Confidentiel-Défense de son ministère.

Pour un système traitant exclusivement d'informations nationales ayant un besoin d'interconnexion avec des partenaires étrangers, cette transition est subordonnée à une approbation ministérielle formelle préalable, sur la base des spécifications des besoins d'échange exprimées.

Article 35

PROTECTION DES MOYENS D'INTERCONNEXION

Les différents composants de l'interconnexion (zone tampon, …) disposent au minimum du même niveau de protection (physique, …) que le système de niveau Confidentiel-Défense à interconnecter.

TITRE VI

EXIGENCES SPÉCIFIQUES POUR LES POSTES NOMADES

Article 36

SPÉCIFICITÉS DES POSTES NOMADES

Les postes nomades se caractérisent principalement par un usage temporaire en dehors d'une GSE conforme aux exigences de l'article 16.

En conséquence, il convient d'obtenir une protection équivalente par l'application des exigences des articles suivants.

Le traitement d'informations Confidentiel-Défense sur des postes nomades doit rester exceptionnel.

Article 37

EXIGENCES SPÉCIFIQUES EN MATIÈRE DE RESPONSABILITÉS ET DE PROCESSUS DE SÉCURISATION DU SYSTÈME D'INFORMATION

Le poste nomade et ses supports classifiés sont gérés comme des documents Confidentiel-Défense : les exigences de la section 3 de [IGI 1300] s'appliquent. Il est notamment rappelé que l'on ne peut pas sortir du territoire avec un poste nomade Confidentiel-Défense sans respecter les prescriptions de l'article 67 de [IGI 1300].

Les procédures d'exploitation de la sécurité prévoient des conditions de soutien adaptées aux contraintes liées à la mobilité.

Article 38

EXIGENCES SPÉCIFIQUES DE SÉCURITÉ PHYSIQUE

Le poste nomade et ses supports classifiés sont sous la surveillance permanente de l'utilisateur, à défaut ils sont stockés dans une armoire forte conformément à [D 1223].

A l'étranger, cette protection est systématiquement recherchée, par le dépôt du poste dans une représentation française (consulat, ambassade, coopération, opération extérieure, …).

Par mesure de précaution, des solutions physiques (étiquettes ou enveloppes de sécurité, …) permettent de détecter une tentative d'accès frauduleux au poste ou une atteinte à son intégrité.

L'exploitation d'informations classifiées sur un poste nomade est conditionnée par l'existence d'une zone permettant de respecter le besoin d'en connaître de l'information traitée. En conséquence, elle est interdite dans un espace ouvert au public (aéroport, train, …).

Un poste nomade fait l'objet de vérifications régulières de sa configuration physique, en particulier avant qu'il soit reconnecté sur le système d'information homologué de son organisme d'appartenance.

Les périphériques (clavier, souris, …), et les protocoles et technologies de communication sans fil susceptibles d'induire des signaux compromettants sont interdits dès lors que le poste nomade est exploité hors d'une GSE.

Les bonnes pratiques suivantes sont à respecter par l'utilisateur :
- fonctionnement du poste sur batterie et non sur secteur ;
- éloignement (un mètre) des sources de conduction (radiateurs, réseaux électriques, réseaux informatiques , téléphone fixe ou mobile, …).

Article 39

EXIGENCES SPÉCIFIQUES DE SÉCURITÉ LOGIQUE

L'utilisateur ne peut pas modifier les paramètres de configuration de démarrage du poste nomade.

Un poste nomade fait l'objet de vérifications régulières de sa configuration logique, en particulier avant qu'il soit reconnecté sur le système d'information homologué de son organisme d'appartenance.

La présence d'informations Confidentiel-Défense en clair sur les supports du poste nomade augmente les risques : les informations sur les supports sont chiffrées par des produits agréés.
À défaut, il est demandé :
- de limiter la présence d'informations classifiées sur les supports (utilisation de clients légers, de supports amovibles, …) ;
- et de rendre plus difficile leur accès sur les supports par l'utilisation d'outils de sécurité non forcément agréés, de préférence qualifiés (chiffrement, authentification par moyen physique, …).

Article 40

EXIGENCES SPÉCIFIQUES SUR LE PERSONNEL

Un utilisateur ne peut se voir attribuer un poste nomade pour le traitement d'informations Confidentiel-Défense qu'après avoir pris formellement connaissance des règles de sécurité à respecter pour l'utilisation de ce type d'équipement.

Article 41

EXIGENCES SPÉCIFIQUES SUR LES INTERCONNEXIONS

Les exigences d'interconnexion de l'article 34 pour le raccordement d'un poste nomade, se traduisent de la manière suivante :
- le raccordement d'un poste nomade à un système ou réseau non homologué au niveau Confidentiel-Défense est interdit ;
- toutefois, le raccordement d'un poste nomade à un système de niveau Confidentiel-Défense via un réseau non homologué au niveau Confidentiel-Défense est autorisé au travers d'un dispositif agréé et dans la mesure où l'homologation du système le prévoit.

GLOSSAIRE

Note : les éléments figurant dans ce glossaire, s'ils constituent des citations *verbatim* d'autres documents, sont en italique et échappent donc à toute révision dans ce document.
L'origine des définitions si elle n'est pas citée est propre à ce document.

Accord de sécurité *: [IGI 1300] accord intergouvernemental conclu entre deux ou plusieurs États ou au sein d'une alliance multinationale et ayant pour objet la protection d'informations ou de supports protégés. Ces accords comprennent l'identification et la reconnaissance mutuelle des autorités nationales de sécurité, la correspondance des niveaux de classification, la reconnaissance mutuelle des habilitations de personnes, les modalités d'échange et de protection des informations et matériels classifiés.*

Administrateur de sécurité *: [IGI 1300] est chargé de la mise en œuvre, du maintien, du contrôle et de l'évolution des mesures de sécurité à appliquer à tout système d'information contenant des informations ou supports protégés classifiés au niveau Secret-Défense et Confidentiel-Défense.*

Administrateur réseaux : est chargé de la mise au point, de l'exploitation, de la maintenance, du contrôle et des évolutions des réseaux.

Administrateur système *: [IGI 1300] est chargé de la mise au point, de l'exploitation, de la maintenance, du contrôle et des évolutions du système informatique.*

Agrément d'un produit de sécurité ***:*** *[II 900] reconnaissance formelle que le produit de sécurité évalué peut protéger des informations jusqu'à un niveau spécifié dans les conditions d'emploi définies.*

Archivage *: [IGI 1300] opération consistant à verser à un service d'archives des supports d'information lorsqu'ils ne sont plus d'utilisation habituelle. Les supports faisant encore l'objet d'une classification ne peuvent être archivés que dans certaines conditions et dans des services habilités à les recevoir.*

Audit de sécurité : regroupe dans la présente instruction :
- l'inspection : action conduite par une entité indépendante de l'autorité responsable du système, elle consiste essentiellement à réaliser un examen qualitatif et à vérifier l'adéquation des moyens et mesures avec les objectifs de sécurité, la réglementation et les directives en vigueur.
- le contrôle : action consistant à réaliser un examen limité et précis afin de vérifier l'application des procédures et de la réglementation. Les contrôles peuvent indifféremment porter sur des systèmes d'information, les sites hôtes ou les organisations concernées.
- l'audit : démarche d'investigation conduite sur un système en exploitation à partir d'un référentiel. Elle comprend un diagnostic et conduit à des recommandations ou des conseils. Les audits, effectués sur tout ou partie d'un système d'information, ont pour objet :
  - de vérifier, voire d'évaluer, la qualité, l'efficacité et la cohérence, des dispositifs, mesures et procédures de sécurité ;
  - de mettre en évidence les vulnérabilités résiduelles ;
  - de qualifier les risques effectifs ou d'en quantifier le niveau ;
  - de proposer les éventuelles actions correctives.

Authenticité *: [IGI 1300] propriété d'une information ou d'un traitement qui garantit son identité, son origine et éventuellement sa destination.*

Authentification / Identification : l'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement, l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. S'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.

Besoin d'en connaître *: [IGI 1300] nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée et pour la bonne exécution d'une mission précise.*

Catalogue des emplois *: [IGI 1300] dans un organisme, liste des emplois qui peuvent nécessiter l'accès aux informations ou supports protégés. Le catalogue est dressé sur le seul critère du besoin d'en connaître.* Seules les personnes occupant un emploi recensé au catalogue sont habilitées à prendre connaissance d'informations ou supports protégés.

Circuit approuvé *: [II 500bis] circuit sur lequel peuvent être transmises en clair, de façon permanente, des informations classifiées dont la mention de protection est inférieure ou égale à un niveau de protection choisi par une autorité et constituant le degré d'approbation de ce circuit.* L'approbation du circuit est de la responsabilité de l'autorité d'homologation du système d'information comprenant ce circuit.

Compromission *: [IGI 1300] prise de connaissance, certaine ou probable, d'une information ou support protégé par une ou plusieurs personnes non autorisées.*

Confidentialité *: [IGI 1300] caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés.*

Cycle de vie : le cycle de vie de l'information comprend les phases de planification, recueil, création ou production de l'information, son organisation, extraction, utilisation, accessibilité et transmission, son stockage et sa protection, et, finalement son élimination par transfert aux archives, effacement ou destruction du support associé.

Décision d'habilitation provisoire *: [IGI 1300] décision exceptionnelle et provisoire prise au vu d'un avis de sécurité provisoire et permettant l'accès d'une personne aux informations ou supports protégés. Cette autorisation prend fin lors de la délivrance de l'autorisation définitive ou au plus tard six mois après avoir été accordée.*

Déclassification *: [IGI 1300] suppression de tout niveau de classification d'informations ou supports protégés.*

Disponibilité : *[IGI 1300] propriété d'une information ou d'un traitement d'être, à la demande, utilisable par une personne ou un système.*

Donnée *: [IGI 1300] toute représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement.*

Environnement de sécurité électronique (ESE) : les mesures techniques de sécurité (mises en place au niveau du système (Electronic Security Environment en terminologie anglaise).

Environnement de sécurité local (LSE) : l'environnement de sécurité physique, du personnel, documentaire et procédurale relevant du domaine de l'autorité d'homologation (Local Security Environment en terminologie anglaise). La LSE est typiquement un local au sens de la directive n°1223/SGDN/SSD/DR.

Environnement de sécurité physique global (GSE) : l'environnement général de sécurité physique dans lequel est situé le système, par exemple : la base aérienne, le commissariat, le consulat ou l'ambassade, ... (Global Security Environment en terminologie anglaise).

Équipement mobile : support d'information mobile (ex : PDA, ordinateur portable, téléphone portable, appareil de prise de vue, …) disposant de capacité propre de traitement.

Fonctionnaire de sécurité de défense *: [IGI 1300] assiste le HFD et contrôle sous sa direction notamment l'exécution des mesures de protection des informations ou supports protégés.*

GSE (Global Security Environment) : voir Environnement de sécurité physique global.

Haut fonctionnaire de défense (HFD) *: [IGI 1300] est chargé, dans les ministères autres que celui de la Défense, d'assister le ministre dans l'exercice de ses attributions de sécurité de défense et de protection du secret. Dans la présente instruction, désigne le haut fonctionnaire de défense ou le fonctionnaire de sécurité de défense dans le cas d'un secrétariat d'Etat, ou l'autorité déléguée par le ministre de la défense.*

Homologation de sécurité *: [IGI 1300] déclaration par l'autorité d'homologation, au vu du dossier d'homologation, que le système d'information considéré est apte à traiter des informations d'un niveau de classification donné conformément aux objectifs de sécurité visés, et que les risques de sécurité résiduels induits sont acceptés et maîtrisés.*

L'homologation de sécurité reste valide tant que le SI opère dans les conditions approuvées par l'autorité d'homologation.

Information *: [IGI 1300] tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement.*

Information ou support protégé *: [IGI 1300] renseignement, procédé, objet, document, donnée informatisée ou fichier présentant un caractère de secret de la défense nationale (cf. art.1er du décret du 17 juillet 1998).*

Information sensible non classifiée de défense : information dont la confidentialité, la disponibilité et l'intégrité ne procèdent pas du secret de la défense nationale tel que défini par les articles 413-9 à 413-12 du code pénal et le décret 98-608, mais des dispositions spécifiques prévues dans la loi, notamment l'atteinte au secret professionnel (CP 226-13 et 226-14), les atteintes aux droits de la personne résultant des fichiers et des traitements informatiques (CP 226-16 à 226-24), et d'autres obligations légales ou contractuelles.
Les informations sensibles ne rentrent pas dans le champ de l'instruction 920.
La mention Diffusion Restreinte peut servir à marquer du sensible non classifié de défense : un récapitulatif figure dans l'article 4 de la recommandation 901 qui peut être utilisée dans le règlement intérieur d'administrations ou d'établissements publics ou privés.

Intégrité *: [IGI 1300] propriété assurant qu'une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée.*

LSE (Local Security Environment) : voir Environnement de sécurité local.

Marquage *: [IGI 1300] opération consistant à apposer sur un support classifié les mentions précisant son niveau de classification, la destination exclusivement nationale le cas échéant, le numéro d'exemplaire, le numéro d'enregistrement et la pagination pour un document papier.*

Matériel classifié *: [IGI 1300] objet, équipement, installation, système ou substance présentant un caractère de secret de la défense nationale et qui nécessitent une protection appropriée Très Secret-Défense, Secret-Défense ou Confidentiel-Défense.*

Modes d'exploitation de sécurité : les différents ratios entre le niveau d'habilitation du personnel, son besoin d'en connaître et le niveau maximum des informations auxquelles il a accès.
Trois modes de fonctionnement sont envisageables : exclusif, dominant ou multi-niveaux

- mode exclusif : les personnes ayant accès au système sont toutes habilitées au plus haut niveau de classification des informations stockées, traitées ou transmises dans le système et ont un besoin commun d'en connaître pour toutes les informations stockées, traitées ou transmises dans le système.
- mode dominant (ou compartimenté) : les personnes ayant accès au système sont toutes habilitées au plus haut niveau de classification des informations stockées, traitées ou transmises dans le système mais n'ont pas toutes un besoin commun d'en connaître pour toutes les informations stockées, traitées ou transmises dans le système.
- mode multi-niveaux : les personnes ayant accès au système ne sont pas toutes habilitées au plus haut niveau de classification des informations stockées, traitées ou transmises dans le système, et n'ont pas toutes un besoin commun d'en connaître pour toutes les informations stockées, traitées ou transmises dans le système.

Non-répudiation *: [IGI 1300] impossibilité de nier la participation au traitement d'une information.*

Périphérique à mémoire rémanente : photocopieur numérique, imprimante, …

Poste nomade : dispositif numérique mobile doté d'un système de traitement et de mémoire permanente (exemple : ordinateur portable, téléphone portable, PDA, appareils photo numériques, …) .

PES : procédures d'exploitation de la sécurité.

Protection physique *: (extrait de la directive 1223) ensemble des mesures de sécurité destinées à garantir l'intégrité des bâtiments, des locaux spécifiquement dédiés aux informations ou supports protégés et la fiabilité des meubles où ils sont conservés, afin d'éviter toute perte ou compromission. Le degré de sécurité physique à mettre en œuvre pour*

assurer leur protection doit être proportionnel au niveau de classification, à la capacité des supports et à la menace à laquelle ils sont exposés.

PSSI : politique de sécurité du système d'information.

Requalification : transformation de la mention d'appartenance d'une information classifiée, par exemple, requalification d'un document Confidentiel-Défense en Confidentiel-UE. Information **requalifiée** : information classifiée dont la mention d'appartenance a été modifiée.

Risque : *[Glossaire EBIOS] combinaison d'une menace et des pertes qu'elle peut engendrer, c'est à dire de l'opportunité de l'exploitation d'une ou plusieurs vulnérabilités d'une ou plusieurs entités par un élément menaçant employant une méthode d'attaque et de l'impact sur les éléments essentiels et sur l'organisme.*

Sensibilisation *: [IGI 1300] instruction périodiquement prodiguée aux personnes habilitées ou susceptibles d'être habilitées et destinée à leur faire prendre conscience des enjeux de la protection du secret de la défense nationale, des sanctions judiciaires et administratives encourues et de la nécessité d'appliquer les mesures de sécurité prescrites.*
Plus généralement : instruction périodiquement prodiguée aux personnes responsables (habilitées ou susceptibles d'être habilitées, ou détentrices d'informations sensibles) et destinée à leur faire prendre conscience des enjeux de la protection du secret (de la défense nationale ou des éléments sensibles), du caractère vital de la disponibilité de l'intégrité et de la confidentialité des informations et de leurs traitements, des sanctions judiciaires et administratives encourues et de la nécessité d'appliquer les mesures de sécurité prescrites (dont les comptes-rendus d'incidents).

Spécial France *: [IGI 1300] mention figurant sur des supports d'information et précisant leur destination exclusivement nationale.*

Sorties versus échanges au sein du système :
- **sortie** : tout dépôt d'information sur un support permanent ou sur un système situé hors du système d'information considéré : impression, enregistrement sur support amovible, enregistrement sur un support fixe hors de la zone de sécurité, communication avec un système externe ; on exclut la visualisation (sur écran, afficheur, projecteur) traitée comme une consultation de document.
- **échange** : tout transfert d'information à l'intérieur du système.

Support *: [IGI 1300] tout moyen matériel, quel qu'en soit la forme ou les caractéristiques physiques, permettant de recevoir, conserver ou restituer des informations ou des données.*

Support amovible : support d'information ne disposant pas de capacité autonome de traitement.

Système d'information *: [IGI 1300] ensemble des moyens humains et matériels ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire l'information.*

Système informatique *: [IGI 1300] ensemble des moyens informatiques et de télécommunication ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire des données.*

Timbre *: [IGI 1300] mention figurant sur un support d'information précisant son niveau de classification et, le cas échéant, son usage national exclusif. Le timbre possède des caractéristiques définies (dimensions, aspect).*

Traitement co-localisé : coexistence de plusieurs systèmes d'information de mentions d'appartenance distinctes, dans la même zone sécurisée.

Vulnérabilité : *[Glossaire EBIOS] caractéristique d'une entité qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information.*

Zone protégée *: [IGI 1300] zone créée par arrêté des ministres compétents et faisant l'objet d'une interdiction de pénétration sans autorisation, sanctionnée pénalement en cas d'infraction (articles 413-7 et R. 413-1 à R 413-5 du Code pénal qui ont institué de telles zones et décret d'application n° 73-389 du 27 mars 1973).*

Zone réservée *: [IGI 1300] locaux et emplacements qui font l'objet de mesures de protection matérielle particulières et dont l'accès est réglementé et subordonné à des conditions spéciales.*
Ces mesures et conditions sont définies dans [IGI 1300].

Zone sécurisée : locaux et emplacements qui font l'objet de mesures de protection matérielle particulières et dont l'accès est réglementé et subordonné à des conditions spéciales. Ces mesures et conditions sont définies dans la présente instruction.

INSTRUCTIONS INTERMINISTÉRIELLES DE RÉFÉRENCE sur la protection du secret de la défense nationale

---

- Instruction générale interministérielle n°1300/SGDN/PSE/SSD du 25 août 2003 sur la protection du secret de la défense nationale.

- Instruction interministérielle n°2100/SGDN/SSD du 1er décembre 1975 pour l'application en France du système de sécurité de l'organisation du traité de l'Atlantique nord.

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

- Instruction interministérielle n°2101/SGDN/SSD/DR du 22 mai 1995 pour l'application en France du système de sécurité de l'Union de l'Europe occidentale.

- Directive n°1223/SGDN/SSD/DR (en cours de modification) sur la protection physique des informations ou supports protégés.

- Directive n°485/SGDN/DISSI/SCSSI/DR du 15 décembre 1988 relative à l'installation des sites et systèmes d'information. Protection contre les signaux compromettants.

- Directive n°495/SGDN/TTS/SI/DR du 19 septembre 1997 de zonage TEMPEST. Protection contre les signaux compromettants.

- Instruction interministérielle n°2000/SGDN/SSD/DR relative aux conditions de protection du secret et des informations concernant la défense nationale et la sûreté de l'État dans les contrats.

- Instruction interministérielle n°1310/SGDN/DEN/SSD/DR du 18 octobre 1996 pour l'enregistrement du courrier classifié.

- Directive n°36/SGDN/SSD/DR du 15 janvier 1985 relative à la protection du secret de défense : déclassification et destruction des documents secret défense et confidentiel défense.

- Instruction interministérielle n°500 bis /SGDN/TTS/SSI/DR du 18 octobre 1996 relative au chiffre dans la sécurité des systèmes d'information.

- Instruction interministérielle n°910/SGDN/SSD/DR du 19 décembre 1994 relative aux articles contrôlés de la sécurité des systèmes d'information.

MODÈLES DE TIMBRE POUR LES DOCUMENTS ÉLECTRONIQUES

_____

I – Entête et pied de page de la 1ère page du document

CONFIDENTIEL DEFENSE
Ce document ne doit être communiqué qu'aux personnes qualifiées pour le connaître

SPECIAL FRANCE

II – Entête et pied de page des pages internes du document

CONFIDENTIEL DEFENSE

SPECIAL FRANCE

III – Pied de page de la 1ère page du document, pour prévoir la déclassification une information ou un support

A déclassifier à compter du :

A déclassifier sur ordre de l'autorité émettrice