

REPUBLIQUE FRANCAISE

PREMIER MINISTRE

**SECRETARIAT GENERAL
DE LA DEFENSE NATIONALE**

DEFENSE ET NATION

N° 1310/SGDN/DEN/SSD/DR

Paris, le 18 octobre 1996.

51, bd de Latour-Maubourg
75700 PARIS

INSTRUCTION INTERMINISTERIELLE PROVISoire
POUR L'ENREGISTREMENT INFORMATISE DU COURRIER CLASSIFIE

DIFFUSION RESTREINTE

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

DIFFUSION RESTREINTE

Version CD.SD.02

SOMMAIRE

INTRODUCTION	1
<u>Article premier</u> : Objet de l'instruction	1
<u>Article 2</u> : Définitions	1
<u>Article 3</u> : Champ d'application	1
<u>Article 4</u> : Organisation réglementaire	2
CHAPITRE I : CONDITIONS D'APPLICATION	4
<u>Article 5</u> : Les fonctions assurées par le système d'enregistrement informatisé du courrier	4
<u>Article 6</u> : Modalités d'utilisation opérationnelle du système	5
<u>Article 7</u> : Modalités d'application de la présente instruction	6
CHAPITRE II : LES BESOINS DE SÉCURITÉ	7
<u>Article 8</u> : La confidentialité	7
<u>Article 9</u> : L'intégrité	8
<u>Article 10</u> : La disponibilité	8
CHAPITRE III : ÉNONCÉ DES PRESCRIPTIONS	9
<u>Article 11</u> : Établissement d'un dossier de sécurité	9
<u>Article 12</u> : L'agrément	9
<u>Article 13</u> : Conformité avec la réglementation sur la cryptologie	9
<u>Article 14</u> : Responsabilités des intervenants	10
<u>Article 15</u> : Répartition des rôles et des responsabilités	10
<u>Article 16</u> : Choix des intervenants	12
<u>Article 17</u> : Protection des locaux et contrôle d'accès	12
<u>Article 18</u> : Protection du système et des supports d'information classifiés associés	13

DIFFUSION RESTREINTE

Version CD.SD.02

<u>Article 19</u>	: Protection contre les signaux parasites compromettants	14
<u>Article 20</u>	: Procédures d'exploitation	14
<u>Article 21</u>	: Cohabitation avec d'autres applications	16
<u>Article 22</u>	: Extension de l'application	16
<u>Article 23</u>	: Installation de l'application sur un réseau	17
<u>Article 24</u>	: La validation des données d'enregistrement	18
<u>Article 25</u>	: Impression des fiches d'enregistrement	19
<u>Article 26</u>	: Impression des fiches de suivi	19
<u>Article 27</u>	: Impression d'historiques	21
<u>Article 28</u>	: Impression de la liste des positions	21
CHAPITRE IV	: PRESCRIPTIONS RELATIVES AUX FONCTIONS DE SÉCURITÉ A IMPLANTER	23
<u>Article 29</u>	: Évaluation des fonctions de sécurité	23
<u>Article 30</u>	: Fonctions d'identification et d'authentification	23
<u>Article 31</u>	: Fonction de contrôle d'accès	24
<u>Article 32</u>	: Cas particuliers pour le contrôle d'accès	25
<u>Article 33</u>	: Fonction d'imputation	27
<u>Article 34</u>	: Fonction d'audit	28
<u>Article 35</u>	: Réutilisation d'objet	28
<u>Article 36</u>	: Fidélité	28
<u>Article 37</u>	: Fiabilité de service	29
<u>Article 38</u>	: L'échange de données	29
CHAPITRE V	: SYNTHÈSE	30
<u>Article 39</u>	: Tableaux récapitulatifs	31
ANNEXE A	: GLOSSAIRE	
ANNEXE B	: RÉFÉRENCES RÉGLEMENTAIRES	

DIFFUSION RESTREINTE

INTRODUCTION

Article premier

Objet de l'instruction

L'objet de la présente instruction provisoire est de fixer les règles relatives aux systèmes d'enregistrement informatisé du courrier*¹ classifié de défense, compatibles avec la législation et la réglementation en vigueur sur la protection des secrets de la défense nationale.

Cette instruction ne s'applique qu'au seul courrier classifié aux niveaux CONFIDENTIEL DÉFENSE* et SECRET DÉFENSE*².

Elle ne s'applique pas à la transmission automatisée et à la mémorisation des supports d'information classifiés de défense, ainsi qu'à la transmission de courrier électronique.

Article 2

Définitions

Est dénommé système d'enregistrement informatisé du courrier classifié de défense, tout système assurant par voie informatique tout ou partie des fonctions définies à l'article 5.

Il peut se substituer à l'enregistrement manuel du courrier, tel que celui-ci est prévu aux articles 27, 28 et 33 de l'I.G.I. 1300. Il exerce les mêmes fonctions et permet les mêmes contrôles et recherches que le registre imposé par cette IGI.

Article 3

Champ d'application

La présente instruction s'applique à toutes les administrations et aux services déconcentrés de l'État.

¹ Les termes suivis d'une * font l'objet d'une définition dans le glossaire joint en annexe A de l'instruction. Le symbole * ne figurera qu'à la première apparition des mots concernés dans chaque paragraphe.

² Les prescriptions qui ne s'adressent qu'aux systèmes d'enregistrement du courrier classifié au niveau Confidentiel Défense sont indiquées par un simple trait en marge.

Les prescriptions qui ne s'adressent qu'aux systèmes d'enregistrement du courrier classifié au niveau Secret Défense sont indiquées par un double trait en marge.

DIFFUSION RESTREINTE

Ses dispositions doivent, en outre, faire l'objet de clauses particulières dans les marchés et autres contrats soumis aux dispositions de l'instruction interministérielle n° 2000/SGDN/SSD/DR du 1er octobre 1986 sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'État, ainsi que dans tous les autres contrats administratifs qui entraînent la mise en oeuvre de systèmes d'information faisant l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées.

Cette instruction s'applique notamment aux établissements publics nationaux placés sous l'autorité d'un ministre. Chaque ministre doit, par ailleurs, veiller à ce que les établissements ou organismes dépendant de lui ou soumis au régime de la tutelle, appliquent la présente instruction.

Article 4

Organisation réglementaire

La présente instruction est établie en cohérence avec la réglementation en vigueur et les directives diffusées :

1. Instruction générale interministérielle N°1300/SGDN/SSD du 12 mars 1982 sur la protection du secret et des informations concernant la Défense nationale et la sûreté de l'État,

Directive N°036/SGDN/SSD du 15 janvier 1985 pour l'application de l'article 22 de l'IGI 1300/SGDN/SSD,

Directive N°1223/SGDN/SSD du 17 décembre 1984 modifiée le 20 novembre 1990, sur la protection matérielle des documents classifiés,

2. Instruction générale interministérielle N°900/SGDN/SSD, N°900/DISSI/SCSSI 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,
3. Avis relatif à la délivrance de certificats pour la sécurité offerte par les produits informatiques vis-à-vis de la malveillance. Journal officiel de la République Française, vendredi 1er septembre 1995, pages 12981 et 12982 (Avis Divers / Premier Ministre)
4. Instruction interministérielle N°2000/SGDN/SSD du 1er octobre 1986, sur la protection du secret et des informations concernant la Défense nationale et la sûreté de l'État dans les marchés et autres contrats,
5. Recommandation N° 600/SGDN/DISSI/SCSSI de mars 1993 sur la protection des informations sensibles ne relevant pas du secret de Défense dans les postes de travail informatiques,
6. Guide de protection contre les signaux compromettants : N°480 SGDN/DISSI/SCSSI du 15 mai 1990,
7. Directive d'installation des sites et systèmes d'information. Protection contre les signaux compromettants : N°485 SGDN/DISSI/SCSSI du 15 décembre 1988,

DIFFUSION RESTREINTE

8. Directive de zonage Tempest - Protection contre les signaux compromettants
N°495 SGDN/DISSI/SCSSI du 20 décembre 1990,
9. Article 413-9 du Code Pénal.

Les extraits de la réglementation, qui s'appliquent directement à l'enregistrement informatisé du courrier classifié*, sont donnés en annexe B.

DIFFUSION RESTREINTE

CHAPITRE I : CONDITIONS D'APPLICATION

Article 5

Les fonctions assurées par le système d'enregistrement du courrier classifié

Les fonctions assurées par le système d'enregistrement du courrier classifié sont listées ci-après. Parmi celles-ci, les fonctions minimum permettant de remplacer le registre imposé par l'I.G.I. 1300 sont indiquées en caractères gras ; les autres fonctions restent facultatives.

1. Mémorisation des données d'enregistrement [Réf. 3 à 5, 7, 10, 20, 22 annexe B] :

a) Identification du support d'information :

- **N° d'enregistrement départ* ou arrivée***,
- **N° d'enregistrement du service émetteur dans le cas d'un support d'information à l'arrivée,**
- **Auteur ou service* émetteur,**
- **Date de création,**
- Domaine (rubrique utilisée pour gérer le besoin d'en connaître, le cas échéant),
- Titre ou objet,
- **Mode* de déclassification prévu** (sur ordre de l'émetteur ou à terme fixé) et le cas échéant, **date prévue,**
- **Nombre d'exemplaires gérés par le service*.**

b) Événements concernant les exemplaires du support d'information :

- **Nature du ou des événement(s) :**
 - **arrivée***,
 - **départ***,
 - **mouvement***,
 - **reproduction** (obligatoire pour le SD, conseillé pour le CD),
 - **archivage***,
 - **destruction,**
 - **déclassification***,
- **Numéro de référence du ou des événements** (ce numéro sera porté sur la fiche de suivi* établie à l'issue de la mémorisation du ou des événements concernés, cf. article 26, Impression des fiches de suivi)),
- **Date du ou des événement(s),**
- **Référence individuelle des exemplaires** (obligatoire pour le SD, conseillée pour le CD) [Réf. 5, annexe B],
- **Nom et fonction du ou des détenteur(s) physique(s) de chaque exemplaire concerné.**

c) Modifications éventuelles des données précédentes.

DIFFUSION RESTREINTE

2. Recherches sur les supports d'information :

- **Recherche des détenteurs successifs d'un exemplaire d'un support d'information à partir de son numéro d'enregistrement** [Réf. 9, annexe B],
- Autres recherches sur les supports d'information (date de création, nom du service émetteur...) à partir des données d'enregistrement.

3. Fourniture d'inventaires de supports d'information :

- **Liste des positions*** [Réf. 9, annexe B],
- Inventaires divers (par meuble de sécurité, par détenteur).

4. Fourniture d'états relatifs aux actions effectuées sur les supports d'information :

- **Historiques***,
- Fiches d'enregistrement* et **fiches de suivi*** (obligatoires pour le SD, conseillées pour le CD),
- **Bordereaux d'envoi** (obligatoires pour le SD, conseillés pour le CD) [Réf. 7, annexe B],
- **Procès verbaux de destruction** (obligatoires pour le SD, conseillés pour le CD) [Réf. 10, annexe B],
- Avis de déclassification*,
- Archivages, reproductions,...

Article 6

Modalités d'utilisation opérationnelle du système

Les systèmes d'enregistrement du courrier classifié au niveau Confidentiel Défense pourront être mis à la disposition des secrétariats ou des responsables de l'enregistrement du courrier classifié ou, plus largement, de certains détenteurs de supports d'information classifiés, en fonction de leur besoin d'en connaître.

Les systèmes d'enregistrement du courrier classifié au niveau Secret Défense seront mis à la disposition exclusive des bureaux Secret Défense*.

Les systèmes mis en place ne pourront réaliser à part entière l'enregistrement du courrier classifié que s'ils offrent toutes les fonctions indiquées en gras dans la liste donnée à l'article 5, avec les exigences de confidentialité, d'intégrité et de disponibilité définies au chapitre II.

Si une de ces fonctions n'est pas réalisée, alors le système mis en place ne devra pas être utilisé pour gérer le courrier classifié : il ne pourra être qu'un complément d'un enregistrement traditionnel réalisé au moyen d'un registre de type "papier".

DIFFUSION RESTREINTE

Article 7

Modalités d'application de la présente instruction

Le courrier classifié de défense peut ne pas faire l'objet d'un système d'enregistrement informatisé. Dans ce cas, l'enregistrement est soumis aux seules règles relatives à la protection du secret de défense et notamment aux dispositions de l'I.G.I. n° 1300.

Lorsqu'un tel système est adopté, il est le plus souvent mis en place dans les services* ou les bureaux Secret Défense* où le flux annuel de courrier classifié de défense reçu, émis ou diffusé est jugé important.

Cette instruction est applicable dès qu'une des fonctions énoncées à l'article 5 est mise en oeuvre par un système* informatisé.

DIFFUSION RESTREINTE

CHAPITRE II : LES BESOINS DE SÉCURITÉ

Les systèmes d'enregistrement informatisé du courrier classifié doivent répondre à des besoins de sécurité. Ils doivent, à ce titre, apporter un niveau de sécurité suffisant compte tenu de leur environnement d'exploitation et de la sensibilité des informations qu'ils traitent.

À cet effet, ces systèmes doivent faire l'objet de mesures de protection techniques ou non techniques garantissant un niveau de sécurité équivalent à celui offert par un enregistrement traditionnel fait au moyen d'un registre "papier", tel que cela résulte de l'I.G.I. n° 1300.

Ce niveau de sécurité se traduit en termes d'exigences de confidentialité, d'intégrité et de disponibilité.

Article 8

La confidentialité

Les données d'enregistrement mémorisées par les systèmes d'enregistrement du courrier classifié au niveau Confidentiel Défense devront recevoir le niveau de classification adéquat : ce niveau peut atteindre le Confidentiel Défense en particulier dans le cas où les données d'enregistrement incluent le titre ou l'objet des supports d'information.

Les supports* d'information Confidentiel Défense ne peuvent être enregistrés que par des personnes ayant fait l'objet d'une décision d'admission au niveau requis. Les responsables de l'enregistrement ne devront avoir accès qu'aux données pour lesquelles ils ont le besoin d'en connaître.

Les secrétariats et les détenteurs de supports d'information classifiés habilités au niveau requis peuvent bénéficier d'un droit d'accès aux données d'enregistrement des supports d'information Confidentiel Défense : cet accès sera impérativement limité à la consultation et ne pourra concerner que les données d'enregistrement pour lesquelles ils ont le besoin d'en connaître.

Les données d'enregistrement mémorisées par les systèmes d'enregistrement du courrier classifié au niveau Secret Défense devront recevoir le niveau de classification adéquat : ce niveau peut atteindre le Secret Défense en particulier dans le cas où les données d'enregistrement incluent le titre ou l'objet des supports d'information. De même, il convient de noter que la liste des destinataires d'un support d'information peut constituer en soi un secret de défense.

Les systèmes d'enregistrement du courrier classifié au niveau Secret Défense sont réservés à l'usage exclusif des membres des bureaux Secret Défense*, qui sont les seuls habilités pour enregistrer le courrier classifié Secret Défense et doivent avoir fait l'objet d'une décision d'admission au niveau Secret Défense [Réf. 6, annexe B]. De plus, ils ne devront avoir accès qu'aux données d'enregistrement pour lesquelles ils ont le besoin d'en connaître.

DIFFUSION RESTREINTE

Article 9

L'intégrité

Un état des informations suivantes :

- données d'enregistrement actualisées,
- historique des modifications de ces données depuis leur première validation ou correspondant à une période définie,

est exigible pour chaque support d'information enregistré, avec une garantie d'intégrité maximum, c'est-à-dire conforme aux données validées successivement par les utilisateurs autorisés.

Un numéro d'enregistrement ne doit pas pouvoir être supprimé ni modifié.

Les données d'enregistrement peuvent être modifiées par les utilisateurs chargés de l'enregistrement du courrier sous réserve de constituer une trace de l'historique des modifications successives.

Article 10

La disponibilité

Les informations ci-dessus doivent pouvoir être fournies, à la demande, aux responsables de l'enregistrement du courrier, afin de permettre au minimum les mêmes types de contrôle que ceux effectués sur le registre imposé par l'IGI 1300.

L'enregistrement du courrier doit pouvoir être effectué sans interruption, informatiquement ou, par défaut, manuellement : la continuité de fonctionnement du système lui-même n'est pas exigée.

Par ailleurs, conformément à l'IGI 1300, il est souhaitable d'intégrer les systèmes d'enregistrement informatisé du courrier classifié au niveau Confidentiel Défense dans une organisation garantissant la **non-répudiation des échanges de supports d'information** avec des services* extérieurs et à l'intérieur même du service concerné.

La **non-répudiation des échanges de supports d'information** doit, en revanche, être obligatoirement garantie lorsqu'il s'agit de supports d'information classifiés au niveau Secret Défense.

DIFFUSION RESTREINTE

CHAPITRE III : ÉNONCÉ DES PRESCRIPTIONS

Article 11

Établissement d'un dossier de sécurité

Un dossier de sécurité*, qui explicite la politique de sécurité du système, doit être rédigé et tenu à jour. Les éléments suivants y sont détaillés :

Les objectifs de sécurité*, qui doivent être exprimés dans la FEROS, Fiche d'expression rationnelle des objectifs de sécurité [Réf. 25, annexe B],

Les menaces* susceptibles de porter atteinte aux biens sensibles* traités par le système à chaque phase de son cycle de vie (développement du système, utilisation opérationnelle, maintenance...). Les biens sensibles comprennent au minimum l'ensemble des données d'enregistrement*, qui peuvent être classifiées jusqu'au niveau Secret Défense. Les biens sensibles peuvent aussi couvrir, entre autres, l'environnement matériel et logiciel nécessaire à l'application et les mesures de protection techniques associés ;

Les contre-mesures* techniques et non techniques qui permettent de répondre aux objectifs de sécurité, compte tenu des menaces retenues.

Ces contre-mesures doivent être conformes aux prescriptions de ce guide.

Le dossier de sécurité ainsi constitué constitue la base pour l'établissement de la cible de sécurité*, au sens des ITSEC*.

Article 12

L'agrément

Les systèmes d'enregistrement informatisé du courrier classifié traitent d'informations qui peuvent être classifiées jusqu'au niveau Secret Défense. Conformément à l'IGI 900 du 20 juillet 1993, ils peuvent de ce fait nécessiter l'utilisation de moyens de sécurité informatique agréés ou de produits informatiques agréés. Selon cette instruction, "cet agrément* est prononcé par le SCSSI à l'issue d'une évaluation* effectuée sous la responsabilité du ministère de la défense ou du SCSSI et financée par le ministère demandeur" [Réf. 24, annexe B].

Article 13

Conformité avec la réglementation sur la cryptologie

Les fonctions de sécurité mises en place pour protéger les biens sensibles* pourront éventuellement mettre en oeuvre des moyens de chiffrement. Dans ce cas, il convient de s'assurer que les algorithmes et/ou les équipements concernés sont mis en place et utilisés conformément aux dispositions de l'IGI 900 (chapitre 2 préambule et article-7).

DIFFUSION RESTREINTE

Article 14

Responsabilité des intervenants

Selon l'instruction générale interministérielle n° 900/SGDN/SSD, n° 900/DISSI/SCSSI (Article 19, page 17), "La sécurité des systèmes d'information relève de la responsabilité de chaque **ministre**, pour le département dont il a la charge." Il en va ainsi en ce qui concerne plus particulièrement la sécurité des systèmes d'enregistrement informatisé du courrier classifié.

L'IGI N°900/SGDN/SSD, N°900/DISSI/SCSSI précise de plus que :

..."Dans chaque département ministériel, à l'exception de celui de la défense, le ministre est assisté pour l'exercice de ses responsabilités de défense par un ou, exceptionnellement, plusieurs **hauts fonctionnaires de défense**"...

..."Dans les départements ministériels qui utilisent des systèmes d'information justifiant une protection ou qui assurent la tutelle d'organismes ou d'entreprises utilisant de tels systèmes, le ministre désigne un **fonctionnaire de sécurité des systèmes d'information (FSSI)**, placé sous l'autorité du haut fonctionnaire de défense."

..."Les **autorités qualifiées** sont les autorités responsables de la sécurité des systèmes d'information dans les administrations centrales et les services déconcentrés de l'État, ainsi que dans les établissements publics...et dans les organismes et entreprises ayant conclu avec l'administration des marchés ou des contrats visés par ce même texte."

Les autorités qualifiées doivent prononcer l'homologation du système au niveau de classification approprié. Leur responsabilité ne peut se déléguer.

Article 15

Répartition des rôles et des responsabilités

Pour l'ensemble du cycle de vie du système d'enregistrement du courrier classifié, les rôles et responsabilités de chaque intervenant devront être explicités.

Ces rôles devront, dans la mesure du possible, être dissociés.

L'Agent de sécurité des systèmes d'information³ a pour mission d'assurer la protection des personnes, la protection des informations et la sécurité des systèmes, sous l'autorité de l'agent de sécurité de l'organisme.

Il doit veiller à la cohérence de l'organisation mise en place avec les **objectifs de sécurité***, compte tenu des **menaces*** retenues.

Il a en charge l'établissement du dossier de sécurité* et contrôle la mise en oeuvre de la politique de sécurité pour chaque phase du cycle de vie du système (spécifications, développement, utilisation opérationnelle, maintenance, mise au rebut).

³ Selon l'I.G.I. n° 900/SGDN/SSD, n° 900/DISSI/SCSSI, pages 19 et 20.

DIFFUSION RESTREINTE

Pour ce qui concerne la sécurité, il peut s'appuyer sur les personnes suivantes :

- Administrateur du système : Il est responsable des moyens matériels et logiciels nécessaires au développement et à l'exploitation du système. En particulier, c'est lui qui définit et met en oeuvre les procédures de sauvegardes, en conformité avec la politique de sécurité établie dans le dossier de sécurité*.
- Gestionnaire de l'informatique local : Il est chargé de la gestion des configurations matérielles et logicielles et de la maintenance de premier niveau.
- Équipe de développement : L'équipe de développement devra se conformer à la politique de sécurité établie dans le dossier de sécurité. En particulier, lorsque le système lui-même a un caractère secret, le personnel chargé du développement devra être habilité au niveau adéquat.

- Utilisateurs du système :

Les utilisateurs d'un système d'enregistrement du courrier classifié au niveau Confidentiel Défense sont les personnes chargées de l'enregistrement du courrier et éventuellement les secrétariats et les détenteurs de supports d'information classifiés.

Les utilisateurs d'un système d'enregistrement du courrier classifié au niveau Secret Défense sont exclusivement les membres désignés des bureaux Secret Défense*, chargés de l'enregistrement du courrier classifié*.

Les utilisateurs devront respecter les procédures techniques ou non techniques introduites pour garantir la sécurité.

En particulier, dans le cadre de l'enregistrement du courrier de niveau Secret Défense, ils sont responsables de la circulation des supports d'information et devront faire signer les fiches de suivi* par les détenteurs des supports d'information concernés [Réf. 6, annexe B].

Leurs droits d'accès aux fonctions du système seront établis en fonction de leur besoin d'en connaître.

Les utilisateurs ont une **responsabilité équivalente** à celle qu'ils auraient pour la tenue d'un registre classique de type papier.

- Techniciens de maintenance : La maintenance doit être effectuée en présence et sous la surveillance d'un agent qualifié de l'organisme, en conformité avec la réglementation des marchés intéressant la défense nationale.

En particulier, tout support susceptible de contenir des informations classifiées et accessible à l'opérateur lors de la maintenance, doit être géré selon les dispositions de l'IGI N° 1300, notamment en ce qui concerne l'habilitation et le besoin d'en connaître.

- Contrôleur : Il est mandaté par les autorités de tutelle de l'organisme et chargé du contrôle réglementaire de la protection des activités et des informations classifiées [Réf. 9 et 21, annexe B].

La liste précédente ne doit pas être considérée comme exhaustive. Le nombre des personnes ayant une fonction concernant la sécurité dépend essentiellement de la taille de l'organisme : des fonctions supplémentaires pourront s'avérer nécessaires dans les

DIFFUSION RESTREINTE

organismes de grande taille (administrateur de la sécurité, administrateur de données, responsable des sauvegardes, par exemple).

En tout état de cause, les intervenants ayant accès au système doivent impérativement respecter la confidentialité des informations auxquelles ils pourraient accéder, même fortuitement, pendant l'accomplissement de leurs fonctions [Réf. 1, annexe B].

Article 16

Choix des intervenants

Seuls peuvent être autorisés à accéder aux données d'enregistrement* ou aux fonctions du système les utilisateurs ou les intervenants **habilités** pour le niveau de classification le plus élevé des informations auquel le système est susceptible de leur donner accès. Leur **besoin d'en connaître** doit avoir, en outre, été explicitement reconnu. À cet effet, ils seront soumis aux règles découlant des instructions ministérielles :

- n° 1300/SGDN/SSD du 12 mars 1982 sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'état,
- n° 2000/SGDN/SSD du 1er octobre 1986 sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'état dans les marchés et autres contrats.

Article 17

Protection des locaux et contrôle d'accès

Dans le cas des systèmes d'enregistrement du courrier classifié au niveau Confidentiel Défense, il est nécessaire de protéger les locaux sensibles, c'est-à-dire :

- les locaux abritant les éléments constituant le système d'enregistrement du courrier (poste de travail, serveurs de fichiers, serveurs de communication,...),
- les locaux où se traitent directement les informations relevant de la classification de défense,
- les locaux réservés à la conservation des supports et des sauvegardes,
- les locaux techniques associés (servitudes : alimentation électrique, onduleurs, les passages de câbles, les équipements d'interface de communication,...),

afin de préserver la confidentialité et l'intégrité et la disponibilité des informations traitées et du système.

Les systèmes d'enregistrement du courrier classifié au niveau Secret Défense (les ordinateurs et leurs périphériques) doivent être installés exclusivement dans les bureaux Secret Défense*, érigés en Zone Réservée Secret Défense [Réf. 6, 16, 19, annexe B]. Cette zone réservée ne peut s'étendre au-delà d'un bâtiment d'emprise géographique limitée.

DIFFUSION RESTREINTE

Les mesures de protection et de contrôle d'accès aux locaux devront être conformes à l'I.G.I. 1300 ainsi qu'à la directive n° 1223/SGDN/SSD/DR du 17 décembre 1984 sur la protection matérielle des documents classifiés [Réf. 17 et 18, annexe B].

L'administration des droits d'accès aux locaux sensibles ou aux bureaux Secret Défense doit prendre en compte le niveau d'habilitation, le statut et le besoin d'en connaître des agents ainsi que les plages horaires.

Article 18

Protection du système et des supports d'information classifiés associés

La mise en oeuvre d'un système d'enregistrement informatisé du courrier classifié implique la création de supports spécifiques pour les données d'enregistrement, qui peuvent être classifiées (documents, supports magnétiques, optiques, films, microfiches ou composants électroniques,...).

Il convient de noter que, dans certains cas particuliers, le système lui-même (hors données d'enregistrement) peut présenter un caractère de secret de la défense nationale. Sa divulgation à un agresseur peut être en effet de nature à nuire à celle-ci ou à conduire à la découverte d'un secret de la défense nationale. Aussi peut-il être classifié.

Les supports visés au premier alinéa, incluant le cas échéant le matériel informatique supportant l'application⁴, doivent faire l'objet de mesures de protection en conformité avec l'I.G.I. n° 1300 [Réf. 8, 19, annexe B] ainsi qu'avec la directive n° 1223/SGDN/SSD/DR du 17 décembre 1984 sur la protection matérielle des documents classifiés.

Un plan d'évacuation et de destruction d'urgence doit être élaboré, chaque fois que des circonstances exceptionnelles mettent en péril la sécurité des bâtiments, des documents et des matériels.

Les prescriptions de l'article 47 de l'I.G.I. n° 1300 doivent être intégralement appliquées.

Prise en compte du besoin d'en connaître : Lorsque les supports d'information gérés au sein du bureau d'enregistrement portent sur des domaines devant être cloisonnés, les responsables de l'enregistrement peuvent être amenés à reconnaître des besoins d'en connaître différents.

Pour rendre les données d'enregistrement inaccessibles aux personnes n'ayant pas le besoin d'en connaître, une des deux mesures suivantes doit obligatoirement être mise en oeuvre au sein de la zone réservée :

- Enregistrements des différents domaines sur des systèmes informatiques physiquement indépendants et, pour chaque système, rangement du matériel informatique support du logiciel d'application et des données d'enregistrement dans des armoires fortes différentes.

⁴ y compris les portables et les supports adaptés

DIFFUSION RESTREINTE

Dans ce cas, les utilisateurs de chaque système auront un besoin d'en connaître homogène.

- Cloisonnement informatique au sein d'un même système et prise en compte du domaine sur lequel portent les supports d'information par la fonction de contrôle d'accès (cf. articles 31 et 32).

La première solution, qui équivaut à des cahiers d'enregistrement différents, sera toujours préférée à la seconde, qui est techniquement plus contraignante.

Article 19

Protection contre les signaux parasites compromettants

[Réf. 14 et 23, annexe B]

Conformément à l'IGI 900, "Tout matériel ou système qui traite des informations sous forme électrique est le siège de perturbations électromagnétiques..."

"... Les matériels ou systèmes qui traitent des informations classifiées de défense doivent être protégés contre cette menace. L'une des méthodes de protection consiste à utiliser des matériels dits TEMPEST..."

"...D'autres méthodes telles que l'utilisation de cages de Faraday ou le zonage TEMPEST, peuvent être utilisées. Il convient alors de s'assurer du maintien de leur efficacité dans le temps".

Les mesures de protection contre les signaux parasites compromettants, si elles sont nécessaires, devront être conformes à :

- la Directive d'installation des sites et systèmes d'information - Protection contre les signaux compromettants : N°485 SGDN/DISSI/SCSSI du 15 décembre 1988,
- la Directive de zonage Tempest - Protection contre les signaux compromettants N°495 SGDN/DISSI/SCSSI du 20 décembre 1990

Article 20

Procédures d'exploitation

Les procédures d'exploitation doivent être conformes à la politique de sécurité fixée et respecter, en particulier, les points suivants.

Si l'intégrité des données d'enregistrement n'est pas contrôlée par une fonction de sécurité technique (cf. article 36) :

- La liste des positions* et les historiques d'enregistrement* utilisés pour les contrôles réglementaires devront être vérifiés comme suit :
 - vérification qu'aucun numéro d'enregistrement ne manque (les supports d'information sont listés dans l'ordre d'enregistrement : les numéros

DIFFUSION RESTREINTE

doivent se suivre et correspondre aux numéros des fiches d'enregistrement*),

- pour chaque support d'information, vérification qu'aucun numéro de fiche de suivi* ne manque (les événements sont listés pour chaque support d'information dans l'ordre de validation : les numéros doivent se suivre et correspondre aux numéros des fiches de suivi).

Pour cette vérification, les fiches d'enregistrement et les fiches de suivi tiennent lieu de référence ; leur impression devient dans ce cas obligatoire⁵ à l'issu de l'enregistrement de chaque événement concernant un support d'information.

- Des procédures de sauvegarde de l'ensemble des informations mémorisées devront être effectuées avec une fréquence suffisante pour limiter les risques d'altération des données d'enregistrements. Ces sauvegardes devront faire l'objet de tests de restauration.

Si la continuité de fonctionnement du système n'est pas assurée par des mesures techniques, la continuité de l'enregistrement doit être assurée comme suit par des mesures à caractère organisationnel :

A la suite d'une défaillance du système ne permettant plus d'effectuer les enregistrements ou le suivi des supports d'information, les utilisateurs poursuivent les enregistrements et le suivi manuellement sur des fiches d'un format similaire aux fiches d'enregistrement et aux fiches de suivi fournies par le système.

Après la restauration du système, les utilisateurs ont la responsabilité d'effectuer à nouveau les enregistrements nécessaires, à partir :

- des fiches d'enregistrement et des fiches de suivi effectuées entre la dernière sauvegarde et la défaillance du système,
- des fiches renseignées manuellement depuis la défaillance du système.

La mise en oeuvre de cette procédure rend l'impression des fiches d'enregistrement et des fiches de suivi⁶ obligatoire à l'issu de l'enregistrement de chaque événement concernant un support d'information.

Dans le cas de l'enregistrement du courrier Secret Défense, l'utilisateur doit, après chaque action qu'il valide sur un enregistrement :

faire viser la fiche de suivi par le(s) détenteur(s) de supports d'information concernés (cf. article 26 Impression des fiches de suivi).

- classer ces fiches dans un registre qui constitue les éléments de preuve utilisables lors des contrôles réglementaires.

L'émargement des fiches de suivi dans le cadre de l'enregistrement du courrier classifié Confidentiel Défense, bien que non obligatoire, est vivement conseillé.

⁵ L'impression des fiches de suivi est toujours obligatoire pour l'enregistrement du courrier Secret Défense.

⁶ L'impression des fiches de suivi est toujours obligatoire pour l'enregistrement du courrier Secret Défense.

DIFFUSION RESTREINTE

Article 21

Cohabitation avec d'autres applications

La cohabitation informatique, y compris par l'intermédiaire d'un réseau informatique, d'un système* d'enregistrement du courrier classifié* au niveau Confidentiel Défense avec d'autres applications est déconseillée [Réf. 11, annexe B].

Si toutefois, cela est le cas, il est obligatoire d'adopter une politique de sécurité extrêmement rigoureuse en mettant en place des fonctions de sécurité techniques pour cloisonner les traitements informatiques et les fichiers mémorisés, qui peuvent être de niveaux de classification différents (cf. chapitre IV, fonctions de sécurité à implanter).

Remarque : La prise en compte de niveaux de classification multiples par la fonction de contrôle d'accès est techniquement très contraignante. Il est de ce fait préférable de gérer les enregistrements de niveaux de classification différents sur des systèmes informatiques physiquement indépendants.

La cohabitation informatique d'un système d'enregistrement du courrier classifié au niveau Secret Défense avec d'autres applications est interdite.

Article 22

Extension de l'application

L'extension de l'application d'enregistrement du courrier classifié au niveau Confidentiel Défense :

- à d'autres utilisations comme, par exemple, l'enregistrement du courrier de diffusion restreinte ou non classifié,
- à d'autres fonctions très limitées comme, par exemple, la gestion du fichier des habilitations du personnel (ce type de fichier peut, en effet, être exploité utilement pour le contrôle de l'accès à l'application d'enregistrement du courrier classifié),

est déconseillée.

Les éventuelles fonctions auxquelles est étendue l'application ne devront en aucun cas élever le niveau de classification de l'application au-delà du niveau Confidentiel Défense.

L'extension de l'application d'enregistrement du courrier classifié Secret Défense à l'enregistrement du courrier du niveau Confidentiel Défense est la seule extension tolérée. Toute autre extension est interdite.

Dans l'éventualité d'une extension du système, il est obligatoire d'adopter une politique de sécurité extrêmement rigoureuse en mettant en place des fonctions de sécurité techniques pour cloisonner les traitements informatiques et les fichiers mémorisés, qui peuvent être de niveaux de classification différents (cf. chapitre IV, fonctions de sécurité à implanter).

DIFFUSION RESTREINTE

Les exigences concernant les systèmes réalisant conjointement l'enregistrement du courrier Confidentiel Défense et l'enregistrement du courrier Diffusion Restreinte (DR) et, éventuellement, non classifié (NC) sont celles qui correspondent au **niveau de classification Confidentiel Défense**.

Les exigences concernant les systèmes réalisant conjointement l'enregistrement du courrier Confidentiel Défense et du courrier Secret Défense sont celles qui correspondent au **niveau de classification Secret Défense** : les prescriptions qui ne s'adressent qu'aux systèmes d'enregistrement du courrier classifié au niveau Confidentiel Défense (un trait simple en marge) ne s'appliquent pas à ce type de systèmes.

Les extensions possibles et le niveau des exigences correspondantes sont résumées dans le tableau suivant :

Système d'enregistrement	Extensions autorisées	Prescriptions applicables
Enregistrement CD	Enregistrement DR et/ou Enregistrement NC et/ou Autres fonctions jusqu'à CD	Prescriptions non spécifiques (pas de trait en marge) + Prescriptions spécifiques CD (trait simple en marge).
Enregistrement SD	Enregistrement CD	Prescriptions non spécifiques (pas de trait en marge) + Prescriptions spécifiques SD (trait double en marge).

Remarque : La prise en compte de niveaux de classification multiples par la fonction de contrôle d'accès est techniquement très contraignante. Il est de ce fait préférable de gérer les enregistrements de niveaux de classification différents sur des systèmes informatiques physiquement indépendants.

Article 23

Installation de l'application sur un réseau

Pour des besoins opérationnels, il peut être nécessaire d'installer l'application d'enregistrement du courrier classifié au niveau Confidentiel Défense sur un réseau. Dans ce cas, ce réseau doit être, dans la mesure du possible, un réseau local réservé à l'usage exclusif de l'enregistrement du courrier classifié et installé dans les locaux protégés (tels que définis dans l'article 17), sans connexion informatique à l'extérieur de cette zone protégée.

Si une de ces conditions n'est pas respectée, alors des fonctions de sécurité techniques devront impérativement être mises en oeuvre pour protéger l'échange de données entre

DIFFUSION RESTREINTE

deux postes distants ainsi que l'accès à l'application d'enregistrement du courrier (cf. chapitre IV, Fonctions de sécurité à implanter).

Toutefois il convient de noter qu'aucune disposition de l'IGI 1300 n'impose un tel type de configuration : en particulier, la tenue du cahier d'enregistrement doit être faite de façon indépendante dans chacun des sites d'un organisme. L'implantation d'un système d'enregistrement du courrier classifié sur un réseau reliant différents sites n'est donc pas recommandée et devra être justifiée dans le dossier de sécurité*.

Pour des besoins opérationnels, il peut aussi être nécessaire d'installer l'application d'enregistrement du courrier classifié au niveau Secret Défense sur un réseau. Dans ce cas, ce réseau doit être un réseau local impérativement réservé à l'usage exclusif de l'enregistrement du courrier classifié et installé dans le bureau Secret Défense [Réf. 6 et 16, annexe B]. Le réseau local sera dédié et desservira cette zone réservée sans concerner une autre zone. Aucune connexion informatique à l'extérieur de cette zone réservée n'est permise.

Article 24

La validation des données d'enregistrement

Une fonction de validation des données d'enregistrement* est obligatoire. Cette fonction est destinée à figer les données d'enregistrement pour éviter les modifications abusives ou illicites.

La fonction de validation doit respecter les caractéristiques suivantes :

- les données d'identification d'un support d'information prévues par le système (conformes à l'article 5) forment un tout et doivent faire l'objet d'une validation globale,

la validation d'un enregistrement Confidentiel Défense (départ* ou arrivée*) déclenche l'attribution d'un numéro d'enregistrement et, si nécessaire, l'impression des fiches de suivi* et de la fiche d'enregistrement* correspondantes (voir rubriques suivantes),

la validation d'un enregistrement Secret Défense (départ ou arrivée) déclenche l'attribution d'un numéro d'enregistrement, l'impression des fiches de suivi correspondantes et, si nécessaire, d'une fiche d'enregistrement (voir rubriques suivantes).

- les événements concernant les exemplaires d'un support d'information (mouvement*, archivage*, destruction, déclassification*) doivent être validés individuellement,

la validation d'un ou plusieurs événements sur un support d'information Confidentiel Défense déclenche, si nécessaire, l'impression des fiches de suivi correspondantes (voir rubriques suivantes),

la validation d'un ou plusieurs événements sur un support d'information Secret Défense déclenche l'impression des fiches de suivi correspondantes (voir rubriques suivantes).

DIFFUSION RESTREINTE

Les numéros d'enregistrement attribués ne doivent pouvoir être ni modifiés ni supprimés.

Les autres données d'enregistrement peuvent faire l'objet de modifications par les utilisateurs autorisés : chaque modification de ces données, depuis la validation initiale, devra être mémorisée par le système (date et nature de la modification).

La mémorisation des données d'enregistrement et leurs modifications successives doit être définitive et impossible sans validation par l'utilisateur.

Article 25

Impression des fiches d'enregistrement

Si l'intégrité des données d'enregistrement ou la continuité de fonctionnement ne sont pas contrôlées par des fonctions techniques, le système doit obligatoirement fournir à **chaque validation** d'un enregistrement (départ* ou arrivée* d'un support d'information) un compte-rendu papier de l'enregistrement, où figurent au minimum les informations suivantes :

- le numéro d'enregistrement chronologique (départ ou arrivée), qui est attribué par le système de façon unique à chaque support d'information,
- les données d'enregistrement* actualisées suite à la validation,
- la nature de l'action qui vient d'être réalisée :
 - enregistrement départ,
 - enregistrement arrivée.

Cette fiche doit être vérifiée par l'utilisateur : elle constitue une trace intègre de chaque enregistrement qui fera référence lors des contrôles réglementaires.

Les fiches d'enregistrement doivent être rassemblées dans un registre unique.

Article 26

Impression des fiches de suivi

L'impression d'une fiche de suivi à **chaque validation** d'un événement concernant un support d'information (départ, arrivée, mouvement, reproduction, archivage, destruction, déclassification) est obligatoire dans les cas suivants :

- si l'intégrité des données d'enregistrement ou la continuité de fonctionnement ne sont pas contrôlées par des fonctions techniques pour les systèmes d'enregistrement du courrier classifié au niveau Confidentiel Défense,
- dans tous les cas pour les systèmes d'enregistrement du courrier Secret Défense.

DIFFUSION RESTREINTE

Les fiches de suivi des supports d'information doivent indiquer au minimum les informations suivantes :

- un double numéro de référence chronologique, qui est attribué par le système de façon unique à chaque événement (numérotation commune à l'ensemble des supports d'information + numérotation propre à chaque support d'information),
- la date du ou des événements,
- le numéro d'enregistrement du support concerné.

Et, pour chaque exemplaire concerné :

- la nature de l'action qui vient d'être réalisée :
 - départ*,
 - arrivée*,
 - mouvement*,
 - reproduction,
 - archivage*,
 - destruction,
 - déclassification*,
- l'éventuelle référence individuelle de l'exemplaire [Réf. 5, Annexe B],
- le nom et la fonction du détenteur de l'exemplaire concerné par l'action.

Pour les supports d'information Confidentiel Défense, les fiches de suivi sont rassemblées dans un registre et constituent, si nécessaire, les éléments de référence utilisables lors des contrôles réglementaires.

Pour les supports d'information Secret Défense, les fiches de suivi, visées par les détenteurs de supports d'information concernés, sont rassemblées dans un registre et constituent les éléments de preuve utilisables lors des contrôles réglementaires.

Dans le cas d'un départ correspondant à l'émission ou la transmission du support d'information, il est souhaitable que le système fournisse automatiquement les bordereaux d'envoi nécessaires, afin qu'ils soient cohérents avec les enregistrements.

La fourniture de ces bordereaux d'envoi est obligatoire pour les systèmes d'enregistrement du courrier Secret Défense [bordereaux A, B, B' : Réf. 7, annexe B].

Dans le cas d'un mouvement de support d'information Secret Défense, la fiche de suivi tient lieu de procès verbal de prise en compte.

Dans le cas d'une destruction, la fiche de suivi tient lieu de procès verbal de destruction et fait apparaître dans ce cas toutes les rubriques relatives à la destruction.

DIFFUSION RESTREINTE

Article 27

Impression d'historiques

Afin d'assurer une fonction de contrôle équivalente à celle offerte par le registre de type "papier", une fonction d'impression d'un historique des données d'enregistrement est obligatoire.

Pour chaque support d'information, cette fonction doit faire apparaître au minimum les informations suivantes :

- état actualisé des données d'enregistrement,
- nombre total d'exemplaires gérés par le service,
- historique des événements subis par chaque exemplaire au cours de la période demandée :
 - enregistrement arrivée*,
 - enregistrement départ*
 - mouvement*,
 - reproduction,
 - destruction,
 - déclassification*,
 - archivage*.

et, pour chaque événement, référence de la fiche de suivi associée.

Lorsque le système nécessite une fonction d'imputation* (cf. article 33), l'historique devra pouvoir, sur demande de la part d'un utilisateur autorisé, inclure les informations d'imputation correspondantes.

Article 28

Impression de la liste des positions

De même, une fonction d'impression de la liste des positions* des supports d'information est obligatoire. Cette fonction fera apparaître, sur demande, dans l'ordre des numéros d'enregistrement arrivée puis départ, au minimum les informations suivantes :

- N° d'enregistrement,
- Identification du support d'information (voir § 2.1),
- Référence de l'exemplaire,
- Position de l'exemplaire :
 - Nom du détenteur,
 - ou Nom du service extérieur auquel il a été émis ou transmis,
 - ou "Détruit",
 - ou "Déclassifié",
 - ou "Archivé".

DIFFUSION RESTREINTE

- Le cas échéant, référence de la dernière fiche de suivi* concernant cet exemplaire.

Le système doit pouvoir fournir, sur demande, la liste des supports d'information détenus par un individu.

DIFFUSION RESTREINTE

CHAPITRE IV : PRESCRIPTIONS RELATIVES AUX FONCTIONS DE SÉCURITÉ À IMPLANTER

Ce chapitre décrit les fonctions de sécurité indispensables [Réf. 24, annexe B] pour répondre aux exigences de sécurité décrites au chapitre 2 "Besoins de sécurité".

Dans tous les cas, il est indispensable d'**identifier les menaces* spécifiques au système** pour déterminer si des fonctions de sécurité supplémentaires sont **nécessaires**. Cette démarche s'inscrit dans le cadre de l'établissement du dossier de sécurité* (cf. article 11).

Les fonctions de sécurité sont regroupées selon les huit rubriques génériques des ITSEC* :

Identification et authentification,
Contrôle d'accès,
Imputation*,
Audit,
Réutilisation d'objet,
Fidélité,
Fiabilité de service,
Échange de données.

Article 29

Évaluation des fonctions de sécurité

Lorsque le système d'enregistrement nécessite la mise en place de fonctions de sécurité techniques⁷ celles-ci doivent obligatoirement faire l'objet d'une évaluation de leur sécurité selon les critères d'évaluation préconisés par le schéma national d'évaluation et de certification des technologies de l'information.

Cette évaluation s'inscrit dans la procédure d'agrément (article 12) et permet de s'assurer que les fonctions de sécurité offrent une protection suffisante.

Article 30

Fonctions d'identification et d'authentification

Des fonctions d'identification et d'authentification sont obligatoires dans chacun des cas suivants :

- le système est physiquement accessible à des personnes n'ayant pas le besoin d'en connaître sur certaines données d'enregistrement*,
- l'application est étendue à l'enregistrement du courrier de niveaux de classification différents et les utilisateurs ne sont pas tous habilités pour le niveau de classification le plus élevé des informations traitées.

⁷

Les conditions qui rendent les fonctions de sécurité obligatoires sont indiquées pour chacun des cas dans les articles 30 à 38.

DIFFUSION RESTREINTE

Dans le cas d'un système d'enregistrement du courrier classifié au niveau Confidentiel Défense, une fonction d'identification et d'authentification est aussi obligatoire dans chacun des autres cas suivants :

- l'accès aux données d'enregistrement est étendu aux secrétariats ou aux détenteurs de supports d'information classifiés,
 - d'autres applications cohabitent sur le même système (cf. article 21), et, éventuellement, des données de niveaux de classification multiples cohabitent sur le même système,
 - l'application est étendue à d'autres fonctions (cf. article 22), et, éventuellement, des données de niveaux de classification multiples sont gérées par l'application alors que les utilisateurs ne sont pas tous habilités pour le niveau de classification le plus élevé des informations traitées.
- l'application est installée sur un réseau ne respectant pas les caractéristiques indiquées à l'article 23,

Ces fonctions doivent identifier et authentifier les utilisateurs de façon unique.

Une identification et une authentification réussies doivent avoir lieu avant toute autre interaction entre le système et l'utilisateur.

Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles, pour création ou destruction, aux responsables désignés.

Cas des systèmes d'enregistrement du courrier classifié au niveau Confidentiel Défense installés sur un réseau :

Si l'application est installée sur un réseau ne respectant pas les caractéristiques indiquées à l'article 23, alors :

- la connexion au système d'enregistrement depuis un poste éloigné doit être précédée de son identification et de son authentification établies de façon unique,
- à la réception de données par le système, il doit être possible d'identifier et d'authentifier de façon unique leur émetteur (poste de travail et utilisateur).

Article 31

Fonction de contrôle d'accès

Une fonction de contrôle d'accès est obligatoire dans chacun des cas suivants :

- le système est physiquement accessible à des personnes n'ayant pas le besoin d'en connaître sur certaines données d'enregistrement*,
- l'application est étendue à l'enregistrement du courrier de niveaux de classification différents et les utilisateurs ne sont pas tous habilités pour le niveau de classification le plus élevé des informations traitées.

DIFFUSION RESTREINTE

Dans le cas d'un système d'enregistrement du courrier classifié au niveau Confidentiel Défense, une fonction de contrôle d'accès est aussi obligatoire dans chacun des autres cas suivants :

- l'accès aux données d'enregistrement est étendu aux secrétariats ou aux détenteurs de supports d'information classifiés,
- d'autres applications cohabitent sur le même système (cf. article 21), et, éventuellement, des données de niveaux de classification multiples cohabitent sur le même système,
- l'application est étendue à d'autres fonctions (cf. article 22), et, éventuellement, des données de niveaux de classification multiples sont gérées par l'application, alors que les utilisateurs ne sont pas tous habilités pour le niveau de classification le plus élevé des informations traitées,
- l'application est installée sur un réseau ne respectant pas les caractéristiques indiquées à l'article 23.

Dans chacune de ces éventualités :

- la fonction de contrôle d'accès doit vérifier la validité de la demande lors de toute tentative de connexion,
- les tentatives d'accès non autorisés doivent être rejetées et journalisées,
- le nombre d'échecs successifs lors d'une tentative d'accès doit être limité à trois et provoquer l'éviction automatique de l'utilisateur,
- seul l'administrateur des droits d'accès doit pouvoir introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants ; il doit disposer de contrôles pour limiter la propagation des droits d'accès.

Par ailleurs, une déconnexion automatique doit être déclenchée par le système en cas d'abandon d'un poste de travail, c'est-à-dire lorsque le système ne perçoit aucune interaction de la part de l'utilisateur pendant une durée jugée excessive, compte tenu de l'environnement.

Article 32

Cas particuliers pour le contrôle d'accès

Prise en compte d'une catégorie d'utilisateurs unique :

Si une fonction de contrôle d'accès est obligatoire (voir conditions indiquées ci-dessus) et si les conditions suivantes sont conjointement réunies :

- le système est accessible uniquement au personnel affecté à l'enregistrement du courrier classifié⁸,
- le personnel chargé de l'enregistrement a un besoin d'en connaître homogène sur l'ensemble des données d'enregistrement,

⁸ Ceci est toujours le cas pour les systèmes d'enregistrement du courrier Secret Défense

DIFFUSION RESTREINTE

alors les utilisateurs autorisés ont un droit d'accès global et sans restriction à toutes les fonctions du système et à l'ensemble des données d'enregistrement. Leur nombre doit être dans ce cas strictement limité.

La fonction de contrôle d'accès doit pouvoir distinguer et administrer les droits d'accès au niveau de chaque utilisateur individuel.

Prise en compte de différentes catégories d'utilisateurs :

S'il est nécessaire de distinguer plusieurs catégories d'utilisateurs sur un même système, c'est-à-dire dans un des cas suivants :

- les utilisateurs ont des besoins d'en connaître différents sur les données d'enregistrement,
- dans le cas de l'enregistrement du courrier classifié au niveau Confidentiel Défense :
 - plusieurs applications cohabitent sur le même système,
 - l'accès au système est étendu aux secrétariats ou aux détenteurs de supports d'information classifiés,

alors la fonction de contrôle d'accès du système doit être conforme aux exigences spécifiées pour la classe de fonctionnalité F-C2 des ITSEC* (contrôle d'accès discrétionnaire*).

Les droits d'accès doivent être alloués comme suit :

1. Le personnel affecté à l'enregistrement du courrier classifié a un droit d'accès global et sans restriction à toutes les fonctions du système et aux données d'enregistrement pour lesquelles ils ont besoin d'en connaître. Le nombre d'utilisateurs de cette catégorie doit être strictement limité.

Et pour les systèmes d'enregistrement du courrier classifié au niveau Confidentiel Défense :

2. Les détenteurs de supports d'information et les secrétariats n'ont pas le droit d'accès aux fonctions d'enregistrement mais uniquement aux fonctions de consultation et de recherche sur les données d'enregistrement.

Le droit d'accès accordé à cette catégorie d'utilisateurs doit respecter le besoin d'en connaître. A cet effet, il peut être nécessaire de distinguer plusieurs groupes parmi ces utilisateurs, auxquels seront affectés des domaines autorisés pour les fonctions de consultation des données d'enregistrement.

3. Les utilisateurs des éventuelles autres applications qui cohabitent sur le même système ne doivent avoir aucun droit d'accès à l'application d'enregistrement.

Il ne doit pas être possible à quelqu'un qui n'est pas un responsable autorisé d'accorder ou de retirer des droits d'accès à un enregistrement ou à un groupe d'enregistrements.

Prise en compte de niveaux de classification multiples :

Lorsque des niveaux de classification différents sont gérés sur un même système (cf. article 22) et si les utilisateurs ne sont pas tous habilités pour le niveau de classification le plus élevé des informations traitées, la fonction de contrôle d'accès du système doit être conforme au minimum aux exigences spécifiées pour la classe de fonctionnalité F-B1 des ITSEC* (contrôle d'accès par mandats*).

DIFFUSION RESTREINTE

Cas des systèmes d'enregistrement du courrier classifié au niveau Confidentiel Défense installés sur un réseau :

Si l'application est installée sur un réseau ne respectant pas les caractéristiques indiquées à l'article 23, alors :

- le système doit vérifier la validité de la demande lors de toute tentative de connexion depuis un poste de travail éloigné. Les tentatives d'accès non autorisées doivent être rejetées, journalisées et entraîner l'invalidation du poste et de l'utilisateur après trois tentatives infructueuses,
- tout poste de travail doit être déconnecté automatiquement du réseau en cas d'abandon par son utilisateur, c'est-à-dire lorsque le système ne perçoit aucune interaction de la part de l'utilisateur pendant une durée jugée excessive compte tenu de l'environnement.

Article 33

Fonction d'imputation*

Une fonction d'imputation* est obligatoire lorsque des mécanismes d'identification, d'authentification et de contrôle d'accès sont nécessaires. Cette fonction d'imputation doit être capable, pour chacun des événements suivants, d'enregistrer cet événement avec les données exigées :

- Utilisation du mécanisme d'identification et d'authentification :

Données exigées : date ; heure ; identité fournie par l'utilisateur ; identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé (par exemple identificateur du terminal) .

- Actions d'utilisateurs autorisés affectant la sécurité ; ces actions, telles que, par exemple, les tentatives de suppression ou de modification d'un enregistrement, d'accès à des données d'enregistrement* sur lesquelles l'utilisateur n'a pas le besoin d'en connaître, les tentatives de modification des droits d'accès ou des données d'imputation, doivent être identifiées et figurer dans le dossier de sécurité* :

Données exigées : date ; heure ; identité de l'utilisateur ; type de l'action ; référence des données sur lesquelles porte l'action.

Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation.

La fonction d'imputation doit être mise en oeuvre systématiquement pour l'ensemble des utilisateurs, y compris l'administrateur.

DIFFUSION RESTREINTE

Article 34

Fonction d'audit

Lorsque une fonction d'imputation* (cf. article 33) est nécessaire, il doit exister des outils pour examiner et maintenir les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions des utilisateurs, y compris l'administrateur.

De plus, il est souhaitable de mettre en oeuvre un mécanisme pour surveiller l'apparition d'événements qui, soit touchent particulièrement à la sécurité, soit, en raison de leur fréquence, peuvent devenir une menace* critique pour la sécurité. Ce mécanisme doit pouvoir notifier sans délai au responsable de l'enregistrement du courrier classifié l'apparition de tels événements. Il doit mettre en oeuvre l'action la moins perturbatrice pour mettre fin à de tels événements. Il peut enfin exploiter les résultats d'audits effectués sur une partie plus vaste du système, dans laquelle est intégrée, le cas échéant, l'application.

Dans le cas d'un système d'enregistrement du courrier classifié au niveau Secret Défense, ce mécanisme est obligatoire.

Article 35

Réutilisation d'objet

Tous les objets de stockage utilisés par le système (mémoire vive, disquettes, disques...) doivent, avant d'être réutilisés à un autre usage, être traités d'une manière telle qu'aucune conclusion ne puisse être tirée concernant leur contenu précédent.

Article 36

Fidélité

Le système doit garantir que les données d'enregistrement* mémorisées ne peuvent pas être modifiées de manière non autorisée. Les conditions de modification autorisées sont les suivantes :

- les numéros d'enregistrement attribués ne doivent pouvoir être ni modifiés ni supprimés,
- les autres données d'enregistrement peuvent faire l'objet de modifications par les utilisateurs autorisés : chaque modification de ces données, depuis la validation initiale, devra être mémorisée par le système (date et nature de la modification).

Il est souhaitable que le système identifie toute altération des données d'enregistrement et en informe le responsable de l'enregistrement du courrier classifié ou l'administrateur du système, afin de mettre en oeuvre la procédure permettant de restaurer les informations altérées. Cette fonction sera mise en oeuvre conjointement à une fonction d'imputation.

DIFFUSION RESTREINTE

Cas des systèmes d'enregistrement du courrier classifié au niveau Confidentiel Défense installés sur un réseau :

Si l'application est installée sur un réseau ne respectant pas les caractéristiques indiquées à l'article 23, alors le système doit permettre de déceler toute perte, tout ajout ou toute modification des données échangées entre deux postes et rendre impossible toute modification de la source ou de la destination réelles du transfert de données.

Article 37

Fiabilité de service

La continuité de fonctionnement du système n'est pas exigée : la continuité des fonctions d'enregistrement du courrier et d'accès aux données d'enregistrement, qui en revanche est exigée, peut en effet être assurée par des mesures à caractère organisationnel (cf. article 20).

Article 38

Échange de données

Dans le cas où l'application d'enregistrement du courrier Confidentiel Défense est installée sur un réseau ne respectant pas les caractéristiques indiquées à l'article 23, alors les points suivants doivent obligatoirement être respectés :

- le système doit offrir la possibilité d'un chiffrement de bout en bout qui garantisse la confidentialité des données d'enregistrement* transmises entre deux postes du réseau [Réf. 15, annexe B],
- le besoin concernant la confidentialité du flux de trafic et la non répudiation des échanges doit faire l'objet d'une analyse dont les conclusions figurent dans le dossier de sécurité*; le cas échéant, les mécanismes appropriés devront être implantés,
- des méthodes de détection et de correction d'erreurs doivent être appliquées en cas d'échange de données d'enregistrement entre deux postes du réseau. Ces mécanismes doivent être conçus de manière à permettre d'identifier les manipulations intentionnelles ou non des champs d'adresse et des données de l'utilisateur. La connaissance seule des algorithmes utilisés dans les mécanismes ne doit pas permettre une manipulation non reconnue des données d'enregistrement. La connaissance supplémentaire indispensable pour le faire doit être protégée de telle façon que seul un nombre restreint d'utilisateurs autorisés puisse y avoir accès.
- des mécanismes qui identifient de façon sûre et unique comme une erreur la réémission non autorisée de données doivent être utilisés.

Dans le cas d'un système d'enregistrement du courrier classifié au niveau Secret Défense, si l'application est installée sur un réseau, celui-ci devra respecter les règles énoncées à l'article 23. La mise en oeuvre de fonctions techniques pour sécuriser les échanges de données entre postes n'est alors pas nécessaire.

DIFFUSION RESTREINTE

CHAPITRE V : SYNTHÈSE

Une synthèse des prescriptions contenues dans cette directive est proposée dans les tableaux pages suivantes.

Pour chaque prescription figure :

- son intitulé,
- la page où elle est énoncée,
- les modalités d'application des mesures prescrites pour l'enregistrement du courrier classifié au niveau Confidentiel Défense d'une part, Secret Défense d'autre part.

DIFFUSION RESTREINTE

Article 39

Tableaux récapitulatifs

PRESCRIPTION	Page	MODALITÉ D'APPLICATION DES MESURES PRESCRITES	
		Enregistrement du courrier classifié au niveau Confidentiel Défense	Enregistrement du courrier classifié au niveau Secret Défense
Dossier de sécurité	9	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Agrément	9	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Réglementation cryptologie	9	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Responsabilités	10	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Répartition des rôles et des responsabilités	10	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Choix des intervenants	12	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Protection des locaux et contrôle d'accès	12	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Protection du système et des supports d'information classifiés - IGI 1300 + Directive 1223 - Besoin d'en connaître	13	Les mesures prescrites sont obligatoires Les mesures prescrites sont obligatoires si des besoins d'en connaître différents doivent être gérés.	Les mesures prescrites sont obligatoires Les mesures prescrites sont obligatoires si des besoins d'en connaître différents doivent être gérés.
Protection contre les signaux parasites compromettants	14	Selon l'environnement.	Selon l'environnement.

DIFFUSION RESTREINTE

PRESCRIPTION	Page	MODALITÉ D'APPLICATION DES MESURES PRESCRITES	
		Enregistrement du courrier classifié au niveau Confidentiel Défense	Enregistrement du courrier classifié au niveau Secret Défense
Procédures d'exploitation - Vérification de l'intégrité de la liste des positions et des historiques - Sauvegardes - Continuité de fonctionnement - Visa des fiches de suivi	14	Les mesures prescrites sont obligatoires si l'intégrité des données d'enregistrement n'est pas garantie par des fonctions de sécurité techniques. Les mesures prescrites sont obligatoires si l'intégrité des données d'enregistrement n'est pas garantie par des fonctions de sécurité techniques. Les mesures prescrites sont obligatoires si la continuité de fonctionnement n'est pas garantie par des fonctions de sécurité techniques. Les mesures prescrites sont conseillées	Les mesures prescrites sont obligatoires si l'intégrité des données d'enregistrement n'est pas garantie par des fonctions de sécurité techniques. Les mesures prescrites sont obligatoires si l'intégrité des données d'enregistrement n'est pas garantie par des fonctions de sécurité techniques. Les mesures prescrites sont obligatoires si la continuité de fonctionnement n'est pas garantie par des fonctions de sécurité techniques. Les mesures prescrites sont obligatoires
Cohabitation avec d'autres applications	16	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Extension de l'application	16	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Installation de l'application sur un réseau	17	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Validation des données d'enregistrement	18	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Impression des fiches d'enregistrement	19	Les mesures prescrites sont obligatoires si l'intégrité des données d'enregistrement ou la continuité de fonctionnement ne sont pas assurées par des fonctions de sécurité techniques.	Les mesures prescrites sont obligatoires si l'intégrité des données d'enregistrement ou la continuité de fonctionnement ne sont pas assurées par des fonctions de sécurité techniques.
Impression des fiches de suivi	19	Les mesures prescrites sont obligatoires si l'intégrité des données d'enregistrement ou la continuité de fonctionnement ne sont pas assurées par des fonctions de sécurité techniques.	Les mesures prescrites sont obligatoires
Impression d'historiques	21	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Impression de la liste des positions	21	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires

DIFFUSION RESTREINTE

PRESCRIPTION	Page	MODALITÉ D'APPLICATION DES MESURES PRESCRITES	
		Enregistrement du courrier classifié au niveau Confidentiel Défense	Enregistrement du courrier classifié au niveau Secret Défense
Évaluation des fonctions de sécurité	23	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Identification et authentification	23	Les mesures prescrites sont obligatoires : - si le système est physiquement accessible à des personnes n'ayant pas le besoin d'en connaître sur certaines données d'enregistrement gérées, - si l'accès aux données d'enregistrement est étendu aux secrétariats ou aux détenteurs de supports d'information classifiés, - d'autres applications cohabitent sur le même système, - l'application est étendue à d'autres fonctions, - l'application est installée en réseau ne respectant pas les caractéristiques indiquées à l'article 23.	Les mesures prescrites sont obligatoires: - si le système est physiquement accessible à des personnes n'ayant pas le besoin d'en connaître sur certaines données d'enregistrement gérées, - si le système est étendu à l'enregistrement du courrier Confidentiel Défense.
- Enregistrement du courrier CD sur réseau	24	Les mesures prescrites sont obligatoires si l'application est installée sur un réseau ne respectant pas les caractéristiques indiquées à l'article 23.	Sans objet
Contrôle d'accès			
- Fonction de contrôle d'accès	24	Les mesures prescrites sont obligatoires dans les mêmes cas que l'identification et l'authentification.	Les mesures prescrites sont obligatoires dans les mêmes cas que l'identification et l'authentification.
- Catégorie d'utilisateurs unique	25	Les mesures prescrites sont obligatoires si une fonction de contrôle d'accès est nécessaire et si le système n'est accessible qu'aux personnes chargées de l'enregistrement et si ces personnes ont un besoin d'en connaître homogène sur les données d'enregistrement.	Les mesures prescrites sont obligatoires si une fonction de contrôle d'accès est nécessaire et si le système n'est accessible qu'aux personnes chargées de l'enregistrement et si ces personnes ont un besoin d'en connaître homogène sur les données d'enregistrement.
- Différentes catégories d'utilisateurs (contrôle d'accès FC2)	26	Les mesures prescrites sont obligatoires : - si les utilisateurs ont des besoins d'en connaître différents sur les données d'enregistrement, - si plusieurs applications cohabitent sur le même système, - si l'accès aux données d'enregistrement est étendu aux secrétariats ou aux détenteurs de supports d'information classifiés.	Les mesures prescrites sont obligatoires si les utilisateurs ont des besoins d'en connaître différents sur les données d'enregistrement.
- Niveaux de classification multiples (contrôle d'accès FB1 ou plus)	26	Les mesures prescrites sont obligatoires si le système doit gérer des données de niveaux de classification multiples et si les utilisateurs ne sont pas tous habilités au niveau le plus élevé.	Les mesures prescrites sont obligatoires si le système doit gérer des données de niveaux de classification multiples et si les utilisateurs ne sont pas tous habilités au niveau le plus élevé.
- Enregistrement du courrier CD sur réseau	27	Les mesures prescrites sont obligatoires si l'application est installée sur un réseau ne respectant pas les caractéristiques indiquées à l'article 23.	Sans objet

DIFFUSION RESTREINTE

PRESCRIPTION	Page	MODALITÉ D'APPLICATION DES MESURES PRESCRITES	
		Enregistrement du courrier classifié au niveau Confidentiel Défense	Enregistrement du courrier classifié au niveau Secret Défense
Imputation*	27	Les mesures prescrites sont obligatoires si une identification et une authentification sont nécessaires.	Les mesures prescrites sont obligatoires si une identification et une authentification sont nécessaires.
Audit - Outils d'audits - Surveillance de l'apparition d'événements critiques.	28	Les mesures prescrites sont obligatoires si une fonction d'imputation est nécessaire. La mesure prescrite est recommandée	Obligatoire si une fonction d'imputation est nécessaire. La mesure prescrite est obligatoire
Réutilisation d'objet	28	Les mesures prescrites sont obligatoires	Les mesures prescrites sont obligatoires
Fidélité - Restriction et mémorisation des modifications des données d'enregistrement - Identification de l'altération des données d'enregistrement - Enregistrement du courrier CD sur réseau	28	Les mesures prescrites sont obligatoires Les mesures prescrites sont recommandées Les mesures prescrites sont obligatoires si l'application est installée sur un réseau ne respectant pas les caractéristiques indiquées à l'article 23.	Les mesures prescrites sont obligatoires Les mesures prescrites sont recommandées Sans objet
Fiabilité de service	29	Les mesures prescrites sont facultatives	Les mesures prescrites sont facultatives
Échange de données	29	Les mesures prescrites sont obligatoires si l'application est installée sur un réseau ne respectant pas les caractéristiques indiquées à l'article 23.	Fonction sans objet

DIFFUSION RESTREINTE

La présente instruction interministérielle provisoire entre en vigueur à dater de ce jour.

Fait à Paris, **le 18 octobre 1996.**

Le Secrétaire général de la défense nationale



Jean PICQ

DIFFUSION RESTREINTE

Annexe A : Glossaire

ANNEXE A : Glossaire

DIFFUSION RESTREINTE

Annexe A : Glossaire

Les définitions retenues sont conformes aux références indiquées aux § 1.2 de l'instruction et à la terminologie employée dans les ITSEC : Critères d'évaluation de la sécurité des systèmes informatiques.

Arrivée d'un support d'information : Réception par un service d'un support d'information issu d'un service extérieur.

Un support d'information "arrivée" peut provenir de la déclassification, au sein d'un service, d'un support d'information. Par exemple, un document initialement enregistré au niveau de classification Secret Défense, devra à nouveau faire l'objet d'un enregistrement "arrivée" au niveau Confidentiel Défense lors de sa déclassification.

Agrément : Reconnaissance formelle que le produit ou le système évalué peut protéger les informations jusqu'à un niveau spécifié dans des conditions d'emploi définies (Instruction interministérielle n° 900, page 23).

Archivage : "Dès qu'ils ne font plus l'objet d'une utilisation habituelle, les documents classifiés présentant un intérêt administratif et historique doivent être versés aux dépôts d'archives suivants : soit les services historique des armées pour le département ministériel de la Défense et les services rattachés, soit les archives du ministère des Relations extérieures, pour ce qui les concerne, soit la direction des Archives de France - Archives Nationales - pour toutes les administrations et organismes civils gérant des archives publiques, ces services étant seuls équipés, en effet, pour recevoir des documents classifiés, jusqu'au niveau Secret Défense inclus..." (IGI N°1300, Article 46)

Biens sensibles : Éléments du système qu'il est indispensable de protéger pour satisfaire les objectifs de sécurité. Ils sont identifiés par une analyse propre à chaque système, qui prend en compte en particulier les conditions d'environnement et les menaces auxquelles celui-ci est soumis. Les résultats de cette analyse sont consignés dans le dossier de sécurité et doivent préciser si les biens sensibles font l'objet d'une classification.

Dans le cas présent, les biens sensibles incluent au minimum les données d'enregistrement.

Bureaux Secret Défense : Bureaux situés en zone de sécurité dite zone réservée, composés exclusivement de personnels ayant fait l'objet d'une décision d'admission au Secret Défense (cf article 27 de l'I.G.I. n° 1300).

Cible de sécurité¹ : Spécification de la sécurité qui est exigée d'une cible d'évaluation et qui sert de base pour l'évaluation. La cible de sécurité doit spécifier les fonctions dédiées à la sécurité de la cible d'évaluation. Elle spécifiera aussi les objectifs de sécurité, les menaces qui pèsent sur ces objectifs ainsi que les mécanismes de sécurité particuliers qui seront employés.

Contre-mesures : Mesures non techniques (telles que choix de personnels habilités, protection des locaux) ou techniques (telles que contrôle d'accès automatique pour une application, mécanismes d'authentification, logiciels antivirus) mises en place pour protéger un système des menaces auxquelles il est exposé.

¹ cf. ITSEC, § 6.8, page 111

DIFFUSION RESTREINTE

Annexe A : Glossaire

Contrôle d'accès discrétionnaire² : Moyen de restreindre l'accès à des objets, en donnant à des sujets identifiés qui ont une permission d'accès, l'autorisation de transmettre cette permission à tout autre sujet sauf restriction imposée par un contrôle d'accès obligatoire.

Contrôle d'accès par mandats³ : Moyen de restreindre l'accès aux objets en fonction de la sensibilité, telle qu'elle est représentée par un label, des informations contenues dans les objets et, en fonction de l'autorisation formelle des sujets, d'accéder aux informations d'une telle sensibilité.

Courrier classifié : La notion de courrier classifié recouvre l'ensemble des supports d'information classifiés émis ou reçus par un service. Ceci comprend les supports d'information créés par un service à son seul profit.

Déclassification d'un document (Directive N°036/SGDN/SSD/DR du 15 janvier 1985) : Le terme général de déclassification recouvre deux notions :

- l'abaissement de classification, qui consiste à attribuer au document la mention de protection immédiatement inférieure (déclassement),
- la suppression de classification, qui consiste à ôter toute mention au document qui devient alors non protégé (déclassification proprement dite).

La notion de déclassification doit être étendue à tout support d'information.

Départ d'un support d'information : Émission ou retransmission d'un support d'information par un service :

- vers un autre service,
- pour le compte du service émetteur avec ou non diffusion interne.

Données d'enregistrement : Données mémorisées lors de l'enregistrement d'un événement concernant un support d'information (départ, arrivée, mouvement, déclassification, destruction, archivage).

Les données d'enregistrement d'un support d'information classifié incluent obligatoirement les informations suivantes :

a) Identification du support d'information :

- N° d'enregistrement départ ou arrivée,
- N° d'enregistrement du service émetteur dans le cas d'un support d'information à l'arrivée,
- Auteur ou service émetteur ,
- Date de création,
- Mode de déclassification prévu (sur ordre de l'émetteur ou à terme fixé) et, le cas échéant, date prévue,
- Nombre d'exemplaires gérés par le service.

² Glossaire Informatique OTAN 08.NN.85

³ Glossaire Informatique OTAN 08.NN.111

DIFFUSION RESTREINTE

Annexe A : Glossaire

b) Événements concernant les exemplaires du support d'information :

- Nature du ou des événement(s) :
 - arrivée,
 - départ
 - mouvement,
 - reproduction
 - archivage,
 - destruction,
 - déclassification.

- Double numéro de référence du ou des événement(s) (voir fiche de suivi),
- Date,
- Référence(s) individuelle(s) de(s) exemplaire(s) (obligatoire uniquement pour le niveau Secret Défense),
- Nom et fonction du ou des détenteur(s) physique(s) de chaque exemplaire concerné,

c) Les éventuelles modifications successives de ces données.

Les données d'enregistrement d'un support d'information classifié peuvent aussi inclure, de façon facultative, les informations suivantes :

- Domaine (rubrique utilisée pour gérer le besoin d'en connaître, le cas échéant),
- Titre ou objet.

Il convient de noter que la réunion de ces informations est susceptible d'élever le niveau de classification des données d'enregistrement.

Dossier de sécurité : Dossier qui explicite la politique de sécurité du système. Les éléments suivants y sont détaillés :

- Les objectifs de sécurité,
- Les menaces susceptibles de porter atteinte aux biens sensibles traités par le système en conditions opérationnelles,
- Les contre-mesures techniques et non techniques qui permettent de répondre aux objectifs de sécurité, compte tenu des menaces retenues.

L'établissement d'un dossier de sécurité est obligatoire pour les systèmes d'enregistrement du courrier classifié (voir § 4.1. Prescriptions générales découlant de la réglementation).

Évaluation⁴ : Estimation de la sécurité d'un produit ou d'un système par rapport à des critères d'évaluation définis.

Fiche d'enregistrement : Fiche imprimée systématiquement à l'issue de chaque enregistrement lorsque l'intégrité des données d'enregistrement mémorisées ou la continuité de fonctionnement du système ne sont pas assurées par des fonctions de sécurité techniques.

Des modèles de fiches sont donnés ci-après à titre indicatif :

⁴ cf. IISEC, § 6.35, page 113

DIFFUSION RESTREINTE

Annexe A : Glossaire

**FICHE D'ENREGISTREMENT
DÉPART**

Référence enregistrement :

- Numéro d'enregistrement départ
- Date de l'enregistrement

Identification du support d'information :

- Référence du service émetteur (dans le cas d'un support d'information issu d'un service extérieur)
- Auteur ou service émetteur
- Date de création
- Domaine
- Titre ou objet
- Mode de déclassification prévu
Date prévue

Enregistrement :

Référence Individuelle de l'exemplaire	Nature du départ ⁵	Nom/fonction du détenteur

**FICHE D'ENREGISTREMENT
ARRIVÉE**

Référence enregistrement :

- Numéro d'enregistrement arrivée
- Date de l'enregistrement

Identification du support d'information :

- Référence du service émetteur
- Auteur ou service émetteur
- Date de création
- Domaine
- Titre ou objet
- Mode de déclassification prévu
Date prévue

Enregistrement :

Référence Individuelle de l'exemplaire	Nom/fonction du détenteur

5 -Diffusion interne au service
-Transmission ou émission à l'extérieur du service

DIFFUSION RESTREINTE

Annexe A : Glossaire

Fiche de suivi : Fiche imprimée par le système à l'issue de chaque validation d'un ou plusieurs événements concernant les supports d'information :

- arrivée,
- départ,
- mouvement,
- reproduction,
- destruction,
- archivage,
- déclassification.

Dans le cas de l'enregistrement du courrier Confidentiel Défense, l'impression systématique des fiches de suivi n'est obligatoire que lorsque l'intégrité des données d'enregistrement ou la continuité de fonctionnement ne sont pas assurées par des fonctions de sécurité techniques.

Dans le cas de l'enregistrement du courrier Secret Défense, l'impression des fiches de suivi est obligatoire ; elles doivent être visées par les détenteurs de supports d'information concernés et constituent les éléments de preuve utilisables lors des contrôles réglementaires.

Un modèle de fiche est donné ci-après à titre indicatif (auquel il convient de rajouter, le cas échéant, les rubriques spécifiques à chaque type d'évènement) :

FICHE DE SUIVI

Références fiche :

- Double numéro de référence chronologique
- Date

Identification du support d'information :

- Numéro d'enregistrement

Nature de l'évènement	Référence de l'exemplaire	Nom/fonction du détenteur	Emargement

Enregistrement :

DIFFUSION RESTREINTE

Annexe A : Glossaire

Historique d'enregistrement : Document fourni par le système concernant un support d'information, qui sert de base de référence lors des contrôles réglementaires. Il indique au minimum les informations suivantes :

- état actualisé des données d'enregistrement,
- nombre total d'exemplaires gérés par le service
- historique des événements subis par chaque exemplaire au cours de la période demandée :
 - enregistrement arrivée,
 - enregistrement départ,
 - mouvement,
 - reproduction,
 - destruction,
 - déclassification,
 - archivage.

et, pour chaque événement, référence de l'événement ou numéro d'enregistrement associée.

Lorsque le système nécessite une fonction d'imputation, l'historique des enregistrements devra pouvoir, sur demande, inclure les informations d'imputation correspondantes.

Pour chaque donnée, les éventuelles modifications successives seront systématiquement indiquées.

Un modèle d'historique est donné ci-après, à titre indicatif :

FICHE D'HISTORIQUE

Identification du support d'information :

- N° d'enregistrement départ et/ou arrivée
- Référence du service émetteur dans le cas d'un support d'information issu d'un service extérieur
- Auteur ou service émetteur
- Date de création
- Domaine
- Titre
- Mode de déclassification prévu
- Date prévue
- Nombre total d'exemplaires gérés par le service

Enregistrements :

Référence individuelle de l'exemplaire	Nature des événements successifs	Nom/fonction du détenteur	Date	Référence de la fiche de suivi ou d'enregistrement

DIFFUSION RESTREINTE

Annexe A : Glossaire

Imputabilité : Propriété qui garantit "l'enregistrement des informations pertinentes sur les actions soit d'un utilisateur, soit d'un processus agissant pour le compte de celui-ci, de façon que les conséquences de ces actions puissent être ultérieurement associées à l'utilisateur en question et qu'on puisse le tenir pour responsable"⁶.

ITSEC : Information Technology Security Evaluation Criteria, soit, en français, Critères d'évaluation de la sécurité des systèmes informatiques.

Les ITSEC sont des critères préparés par quatre pays européens dont la France et diffusés à l'ensemble de la CEE par la Commission des Communautés en 1991. Leur application a été rendue obligatoire pour les administrations de l'État par la lettre N° 106 SGDN/DISSI/26007 du 11 mars 1992.

Liste des positions : Liste qui doit pouvoir être imprimée sur demande par le système et qui fait apparaître, dans l'ordre des numéros d'enregistrements arrivée puis départ, les informations suivantes :

- N° d'enregistrement,
- Identification du support d'information (voir § 2.1)
- Référence de l'exemplaire,
- Position de l'exemplaire :
 - Nom du détenteur,
 - ou Nom du service extérieur auquel il a été émis ou transmis,
 - ou "Détruit",
 - ou "Déclassifié",
 - ou "Archivé".
- Référence de la dernière fiche de suivi concernant cet exemplaire.

Menace⁷ : Action ou événement susceptible de porter préjudice à la sécurité.

Modes de déclassification : (Directives N°036/SGDN/SSD/DR pour l'application de l'article 22 de l'instruction générale interministérielle N°1300/SGDN/SSD du 12 mars 1982, pages 2 et 3).

- **À terme fixé** : Il s'agit de documents :
 - a) soit qui, en raison de la sensibilité temporaire des informations qu'ils contiennent, peuvent voir leur classification "Secret Défense" ou "Confidentiel Défense" abaissée sans inconvénient ou même supprimée totalement dans un délai assez proche qu'il est possible d'apprécier dès l'émission. Leur déclassification pourra donc intervenir à un "terme fixé".
 - b) soit qui sont considérés comme pouvant systématiquement faire l'objet d'un abaissement de niveau à l'issue des délais de principe suivants :...
 - ...5 ans après leur émission (ou leur déclassement en "Confidentiel Défense" pour les documents "Secret Défense") les documents "Confidentiel Défense" sont déclassifiés ou reçoivent la mention "Diffusion Restreinte".

⁶ cf. ITSEC § 2.40, page 26

⁷ cf. ITSEC, § 6.49, page 115

DIFFUSION RESTREINTE

Annexe A : Glossaire

- Sur ordre :

Les documents pour lesquels la déclassification ne peut intervenir systématiquement à une date précise ou à l'issue des délais de principes d'abaissement de niveau sont à déclassifier exclusivement sur ordre de l'autorité émettrice. Toutes les précautions doivent alors être prises pour que l'ensemble des détenteurs soit avisé de la déclassification et de son niveau résiduel..."

Cette définition doit être étendue à tout support d'information.

Mouvement d'un support d'information : Changement de détenteur dans le cas d'un support d'information Confidentiel Défense, sortie ou réintégration au bureau Secret Défense dans le cas d'un support d'information Secret Défense.

Niveau de classification Confidentiel Défense : "...La mention CONFIDENTIEL DÉFENSE est réservée aux informations qui ne présentent pas en elles-mêmes un caractère secret mais dont la connaissance, la réunion ou l'exploitation peuvent conduire à la divulgation d'un secret intéressant la Défense nationale et la sûreté de l'État..." (Décret N° 81-514 du 12 mai 1981, relatif à l'organisation de la protection des secrets et des informations concernant la défense nationale et la sûreté de l'État, Article 5).

Niveau de classification Secret Défense : "...La mention SECRET DÉFENSE est réservée aux informations dont la divulgation est de nature à nuire à la Défense nationale et à la sûreté de l'État..." (Décret N° 81-514 du 12 mai 1981, relatif à l'organisation de la protection des secrets et des informations concernant la défense nationale et la sûreté de l'État, Article 5).

Objectifs de sécurité⁸ : Contribution à la sécurité qu'une cible d'évaluation est destinée à apporter.

Service : Le terme "service" est utilisé de façon générique dans ce guide pour désigner l'entité organisationnelle au sein de laquelle est implanté le système d'enregistrement du courrier classifié.

Dans la pratique, le terme "service", pourra s'appliquer à un organisme, un établissement, une entreprise ou toute autre entité organisationnelle nécessitant un enregistrement autonome du courrier classifié.

Support d'information classifié : Support d'information qui présente un caractère de secret de la Défense Nationale. Dans les nouvelles dispositions du code pénal, l'article 413-9 dispose que :

"Présentent un caractère de secret de la défense nationale au sens de la présente section les renseignements, procédés, objets, documents, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion.

Peuvent faire l'objet de telles mesures les renseignements, procédés, objets, documents, données informatisées ou fichiers dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale".

⁸ cf. ITSEC, § 6.50, page 115

DIFFUSION RESTREINTE

Annexe A : Glossaire

Par conséquent, outre les informations intéressant la défense nationale, leurs supports, quels qu'ils soient, peuvent eux aussi présenter un caractère de secret de la défense nationale et être à ce titre classifiés de défense.

Système ou système informatique : Ensemble formé par un ordinateur et les différents éléments qui lui sont rattachés. Ceci concerne les matériels et les logiciels (IGI N°900/SGDN/SSD/DR, N°900/DISSI/SCSSI/DR, page 23).

DIFFUSION RESTREINTE

**Annexe B : Références
réglementaires**

ANNEXE B : Références réglementaires

DIFFUSION RESTREINTE

**Annexe B : Références
réglementaires**

Cette annexe propose de façon non exhaustive quelques extraits des textes en vigueur qui ont servi de référence à l'établissement de ce guide.

Instruction générale interministérielle sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'état (N°1300/SGDN/SSD).

Article 19 : Les principes de la classification des informations ; Institution des trois niveaux de classification.

- [1] "...L'obligation de secret imposée à celui qui détient ou utilise des informations classifiées a toujours un caractère impératif quel que soit le degré de protection accordé à l'information."

Article 20 : Règles applicables en matière de classification

"La mise en oeuvre de la classification doit tenir compte des règles suivantes :

- [2] - conformément aux dispositions de l'article 3 du décret du 12 mai 1981, toutes les informations qui doivent être protégées nécessitent l'utilisation d'une mention de classification qui doit être portée sur le support de l'information : objet, document, procédé"...
- "...tout extrait d'information classifiée doit seulement recevoir la classification appropriée à son contenu, sous réserve de ne pas citer les sources de l'information : référence du document d'origine et objet. Un extrait d'information classifiée présente généralement un degré de sensibilité moindre, dans la mesure toutefois où il ne peut conduire à reconstituer, directement ou par déduction, l'information initiale. Il peut ne pas impliquer d'obligation de classification."
- "tout dossier reçoit obligatoirement une protection au moins égale à celle du document le plus sensible qui y est inclus. Il peut recevoir une classification si l'ensemble des informations qu'il rassemble l'exige, alors même qu'aucun des documents qui le composent ne nécessite de classification."

Article 22 : Évolution de la sensibilité d'une information

- [3] "La sensibilité d'une information évolue en fonction du temps ou des circonstances. La protection qui lui a été accordée initialement doit donc pouvoir être modifiée soit dans le sens d'un renforcement, soit dans le sens d'une réduction et éventuellement d'une suppression"...

..."La réduction ou la suppression des protections devenues excessives doit être effectuée chaque fois que cela est possible"...

..."La décision qui réduit ou supprime la protection d'une information classifiée appartient dans tous les cas à l'autorité émettrice (cf. article 3 du décret du 12 mai 1981). La mention de modification doit être portée sur les cahiers d'enregistrement et sur le support de l'information (document, fiche, bande magnétique, cassette)".

"L'autorité responsable de la décision de déclassification doit la notifier aux détenteurs des informations correspondantes en précisant le type de marquage qui doit être utilisé compte tenu, suivant le cas, du support de l'information."

DIFFUSION RESTREINTE

Version CD.SD.02
Annexe B : Références
réglementaires

"Dans la mesure du possible, dès la diffusion d'une information classifiée, principalement lorsqu'il s'agit d'informations CONFIDENTIEL DÉFENSE, l'autorité émettrice indiquera par un marquage particulier, porté éventuellement au recto du document, si le niveau de protection est à réduire ou supprimer systématiquement à un terme déterminé ou si la réduction ou suppression n'est à opérer que sur ordre."

"En l'absence de disposition prise par l'autorité d'origine, il appartient aux autorités destinataires de saisir l'autorité émettrice d'une proposition de modification ou de suppression de classification chaque fois qu'elles l'estiment nécessaire."

"La révision du niveau de protection d'une information doit s'effectuer périodiquement. La période des inventaires annuels - 31 décembre - obligatoire pour les documents SECRET DÉFENSE, convient parfaitement à cet examen."

"A titre indicatif, les documents SECRET DÉFENSE devraient en règle générale faire l'objet d'un abaissement ou même d'une suppression de classification au bout de dix ans. Les documents CONFIDENTIEL DÉFENSE doivent pouvoir être déclassifiés, dans un grand nombre de cas, au bout de cinq ans."

Article 23 : Reproduction des documents classifiés

- [4] ..."Il est nécessaire, en outre, de consigner sur un registre le nombre et le détenteur des copies délivrées"...

..."En ce qui concerne les documents CONFIDENTIEL DÉFENSE, leur reproduction par les autorités destinataires peut être autorisée, sauf disposition contraire de l'autorité émettrice, sous réserve de lui faire connaître le nombre et les destinataires des exemplaires reproduits."

Article 26 : Élaboration des documents "SECRET DÉFENSE"

- [5] ..."L'autorité d'origine, émettrice du document et responsable du choix de la classification, doit vérifier le nombre d'exemplaires émis et établir une liste de diffusion sur laquelle doivent être portés le nombre et le numéro des exemplaires attribués à chaque destinataire et celui des exemplaires (deux au moins) conservés par le service émetteur..."

..."Chaque exemplaire d'un document SECRET DÉFENSE doit faire l'objet d'un marquage spécial précisant son degré de classification et son identité et permettant de vérifier son authenticité et son intégralité. En outre, s'il y a lieu, un marquage d'abaissement de classification ou de déclassification à terme est également effectué..."

..."Tout document classifié est identifié dès sa première page, outre les références habituelles à tout document administratif, (service émetteur et date) par :

- un numéro individualisant chaque exemplaire, portant en numérateur le numéro d'ordre dans la série et en dénominateur le nombre total d'exemplaires émis ;
- un numéro d'enregistrement chronologique du bureau SECRET DÉFENSE de l'organisme émetteur."

DIFFUSION RESTREINTE

**Annexe B : Références
réglementaires**

Article 27 : Création et attribution des bureaux "SECRET DÉFENSE"

- [6] ..."Situés en zone de sécurité dite "zone réservée", ces bureaux, composés exclusivement de personnels ayant fait l'objet d'une décision d'admission au SECRET DÉFENSE, sont institués par le chef du service sous l'autorité duquel ils sont placés. Ils peuvent constituer seulement une section spécialisée du bureau d'ordre, ou bureau de courrier général.

Les bureaux SECRET DÉFENSE sont responsables de l'enregistrement et de la circulation des documents classifiés SECRET DÉFENSE..."...

Article 28 : Modalités d'expédition et de réception des documents "SECRET DÉFENSE"

- [7] **a) Modalités d'expédition.**

"Il est procédé aux opérations suivantes par les bureaux d'enregistrement du courrier SECRET DÉFENSE :

- identification, marquage et enregistrement : chaque document doit porter les références définies...
- bordereau d'envoi : ...doit comprendre trois feuillets détachables :
 - les feuillets A et B sont adressés au service destinataire qui conserve le premier à titre d'élément de preuve et renvoie le deuxième, le feuillet B, au service expéditeur, à titre d'accusé de réception ;
 - le feuillet B', de couleur différente, est conservé par le service expéditeur, puis il est détruit au reçu du bordereau accusé de réception (feuillet B)..."

b) Formalités de réception des documents SECRET DÉFENSE.

..."Il y a lieu de procéder aux opérations suivantes :

- vérification de l'intégrité de l'emballage ;
- enregistrement des documents dans l'ordre chronologique sur un registre spécifique SECRET DÉFENSE, coté et paraphé ;
- mention, sur ce registre, des personnes ayant pris en compte ces documents (fonction et signature) ;
- signature et renvoi à l'autorité d'origine du bordereau d'envoi feuillet "B", à titre d'accusé de réception."

Article 30 : Conservation des documents

- [8] ..."Les documents doivent, en dehors des périodes d'utilisation, être enfermés dans des coffres-forts ou des armoires fortes à combinaisons multiples, si possible de fabrication nationale et de fiabilité reconnue..."

DIFFUSION RESTREINTE

Version CD.SD.02
Annexe B : Références
réglementaires

Article 31 : Contrôle administratif : inventaire

[9] ..."Chaque service employeur ou organisme fait procéder, au moins une fois par an (courant décembre), à l'inventaire des documents SECRET DÉFENSE détenus dans l'ensemble de ses services par les bureaux SECRET DÉFENSE ou les personnels relèvent de son autorité, afin de contrôler leur conservation et de s'assurer de leur présence non seulement comptable mais physique. A cette fin est dressé un procès-verbal annuel mentionnant les références et identification de chaque document ou, s'il y a lieu, l'une ou l'autre des pièces administratives suivantes :

- un récépissé du nouveau détenteur ;
- un procès-verbal de destruction ;
- un procès verbal de versement à un dépôt d'archives"...

..."Il convient également de vérifier les dates de péremption et les modifications éventuelles à apporter à la classification."...

..."Les procès-verbaux d'inventaire doivent pouvoir être produits à l'occasion de toute inspection ou contrôle..."

..."Il est souligné sur les cahiers d'enregistrement de courrier départ et arrivée ne peuvent tenir lieu d'inventaire"...

Article 32 : Destruction

[10] ..."Les autorités destinataires de documents qu'elles jugent périmés ou inutiles, au terme d'un certain délai et en l'absence de mention de date de destruction portée sur le document par l'organisme émetteur, procèdent à leur destruction...dans les conditions suivantes : elles font connaître par écrit à l'autorité émettrice leur intention de détruire tel ou tel document, sauf avis contraire. Après destruction elles doivent rendre compte à l'organisme émetteur, ou en cas de suppression de celui-ci, à l'organisme qui lui a succédé en lui adressant copie du procès-verbal de destruction."

Article 33 : Élaboration, marquage, enregistrement des documents

[11] ..."L'enregistrement des documents CONFIDENTIEL DÉFENSE doit se faire sur un registre différent de celui prévu pour le courrier normal."

Article 34 : Expédition des documents - Conservation et reproduction

[12] ..."Les documents doivent être conservés dans les armoires fortes. Lorsqu'il doit être procédé à leur destruction, il convient d'en faire mention sur le cahier d'enregistrement"...

..."La reproduction des documents CONFIDENTIEL DÉFENSE est autorisée dans les conditions définies à l'article 23 ci-dessus, sous réserve d'une stricte limitation du nombre de reproductions, de leur enregistrement par les autorités émettrices ou détentrices"...

Article 37 : Informatique

[13] ..."Il est indispensable de s'opposer aux actions éventuelles de pénétration des systèmes informatiques par des personnes non autorisées en réglementant leur mise en oeuvre."...

DIFFUSION RESTREINTE

**Annexe B : Références
réglementaires**

Article 38 : Bureautique (informatique de bureau)

- [14] ..."Des règles spécifiques de protection doivent être mises en oeuvre en raison notamment des rayonnements émis lors de la frappe..."

Article 39 : Transmissions - Télécommunications

- [15] ..."A des degrés divers, les moyens de transmission sont susceptibles d'intrusions et d'interceptions, soit en raison de leur nature, soit du fait de leur mode d'exploitation. Aussi ne doivent-ils être utilisés pour l'acheminement d'informations classifiées qu'avec des dispositifs de chiffrement ou de camouflage approuvés"...

..."La sécurité des voies de transmission résulte des mesures prises pour assurer leur protection à la fois contre les intrusions (intégrité des informations et authentification des correspondants), et l'exploitation éventuelle des interceptions.

L'ensemble de ces mesures de protection destinées à assurer la sécurité des communications fait l'objet d'instructions interministérielles... dont notamment l'instruction n°500/STC-CH du 23 décembre 1968 sur la sécurité des communications et les instructions complémentaires."

Article 40 : Création de zones réservées pour la protection des documents "SECRET DÉFENSE".

- [16] "La création de zones réservées a pour but :
- d'interdire toute pénétration non contrôlée, que ce soit par les vues ou par les écoutes directes ou indirectes, dans les lieux où les documents classifiés sont élaborés, reçus ou détenus ;
 - d'interdire tout accès aux documents par des personnes n'ayant pas à en connaître et non autorisés."...

"En règle générale, la zone réservée doit répondre aux normes suivantes :

- ouverture en nombre limité et fenêtres protégées ;
- portes équipées de serrures de haute sécurité, munies si possible de compteur d'ouverture ;
- organisation d'un contrôle permanent de la zone, quels que soient les systèmes de protection choisis...

"La création d'une telle zone est recommandée dans tout organisme traitant même occasionnellement d'informations SECRET DÉFENSE. Elle est obligatoire dans les organismes élaborant, recevant ou détenant des informations traitant d'une manière habituelle de telles informations"...

DIFFUSION RESTREINTE

Version CD.SD.02
Annexe B : Références
réglementaires

Article 41 : Contrôle en zone réservée

[17] **1. Contrôle des locaux**

..."Pendant les heures de travail, le contrôle de la zone réservée incombe entièrement aux personnels qui y ont leur emploi. Ils doivent, lors de toute absence, vérifier la mise en sûreté des documents ainsi que la fermeture des coffres et des bureaux".

..."En dehors des heures ouvrables, des inspections doivent être organisées par les autorités compétentes, afin de vérifier que les bureaux, les coffres, les armoires, etc., sont fermés, que les corbeilles à papier ont été vidées et ne contiennent aucun document préparatoires... et qu'aucun document classifié ne demeure hors des coffres... Des rondes de sécurité doivent également être régulièrement effectuées par des gardiens qui doivent être sélectionnés et agréés au niveau de secret le plus élevé des documents détenus. Des consignes écrites doivent leur être adressées pour fixer leur mission."

[18] **2. Contrôle des personnels et visiteurs dans la zone réservée**

a. Personnels en service : les personnels ayant de par leurs fonctions accès aux zones réservées doivent être munis d'un laissez passer et d'une carte d'identité.

b. Visiteurs : ils doivent avoir reçu une autorisation individuelle préalable de l'autorité responsable :

- être munis d'un laissez-passer temporaire ;
- être accompagnés à l'intérieur de la zone réservée pendant toute la durée de la visite sous le couvert d'une autorité habilitée désignée parmi les personnels de la zone.

c. Personnels de nettoyage : le nettoyage doit être effectué par des personnels relevant de l'organisme responsable ou pouvant lui être rattaché surtout lorsque la totalité des documents classifiés ne peut être enfermée dans des coffres...

A défaut, lorsqu'il est fait appel à des entreprises spécialisées dont les personnels n'ont pas fait l'objet d'une procédure d'habilitation et ne sont pas agréés dans le cadre d'un marché classé de défense, il est nécessaire d'assurer la surveillance continue du nettoyage qui doit être effectué en présence d'une personne désignée par l'autorité responsable."

Article 42 : Modalités de protection des matériels en "zone protégée" ou "non protégée".

[19] "Les matériels, équipements et installations à caractère secret (Confidentiel Défense ou Secret Défense) doivent être protégés au même titre que les documents classifiés. Cette protection implique la mise en oeuvre de mesures de sécurité à tous les stades de la réalisation : programmes, études, plans, fabrications ou constructions, essais, etc.

Il doit en être de même après achèvement ou mise en service lors de leur présentation, de leur utilisation (entretien, réparation, gardiennage, transport) ou lors de leur mise hors service et de leur destruction..."

"...Il convient d'éliminer toute possibilité d'accès par vues terrestres ou aériennes et par l'utilisation de procédés techniques de détection ou d'identification..."

DIFFUSION RESTREINTE

**Annexe B : Références
réglementaires**

"...L'un des moyens les plus efficaces pour assurer la protection de matériels sensibles classifiés consiste à les entreposer dans une zone réservée, placée sous garde permanente et dont l'accès est strictement limité aux seules personnes autorisées..."

Article 46 : Versement à l'administration des archives des documents classifiés

- [20] "Dès qu'ils ne font plus l'objet d'une utilisation habituelle, les documents classifiés présentant un intérêt administratif et historique doivent être versés aux dépôts d'archives suivants : soit les services historique des armées pour le département ministériel de la Défense et les services rattachés, soit les archives du ministère des Relations extérieures, pour ce qui les concerne, soit la direction des Archives de France - Archives Nationales - pour toutes les administrations et organismes civils gérant des archives publiques, ces services étant seuls équipés, en effet, pour recevoir des documents classifiés, jusqu'au niveau Secret Défense inclus..."

Article 54 : Contrôles et inspections

- [21] "...Chaque ministre (haut fonctionnaire de Défense pour les départements qui en sont pourvus) prescrit, à l'intérieur de son département, des contrôles et inspections périodiques en vue de vérifier l'application effective des instructions sur la protection des informations classifiées..."

DIFFUSION RESTREINTE

Version CD.SD.02
Annexe B : Références
réglementaires

Directives N°0036/SGDN/SSD/DR du 15 janvier 1985 pour l'application de l'article 22 de l'instruction générale interministérielle N°1300/SGDN/SSD du 12 mars 1982. Déclassification et destruction des documents secret défense et confidentiel défense (page 4, paragraphe IV. Enregistrement).

[22] "Le cahier d'enregistrement (départ et arrivée) ainsi que les inventaires annuels "Secret Défense" feront apparaître au regard des documents :

- l'indication de déclassification (sur ordre, à la date du...),
- une fois la déclassification opérée, la date à laquelle elle a été effectuée.

Ces précautions sont indispensables pour s'opposer à toute utilisation de documents frauduleusement déclassifiés."

DIFFUSION RESTREINTE

Annexe B : Références
réglementaires

**Instruction Générale interministérielle N°900/SGDN/SSD,
N°900/DISSI/SCSSI sur la sécurité des systèmes d'information qui font
l'objet d'une classification de défense pour eux-mêmes ou pour les
informations traitées.**

Article 8 : Protection contre les signaux parasites compromettants

- [23] "Tout matériel ou système qui traite des informations sous forme électrique est le siège de perturbations électromagnétiques. Ces perturbations, provoquées par le changement d'état des circuits qui composent le matériel considéré, sont qualifiées de signaux parasites. Certains de ces signaux sont représentatifs des informations traitées. Leur interception et leur exploitation permettent de reconstituer ces informations. Ces signaux sont, de ce fait, dénommés **signaux parasites compromettants (S.P.C.)**."

"...Les matériels ou systèmes qui traitent des informations classifiées de défense doivent être protégés contre cette menace. L'une des méthodes de protection consiste à utiliser des matériels dits TEMPEST..."

"...D'autres méthodes telles que l'utilisation de cages de Faraday ou le zonage TEMPEST, peuvent être utilisées. Il convient alors de s'assurer du maintien de leur efficacité dans le temps".

Article 9 : Moyens de sécurité informatique

- [24] "La sécurité informatique exige que des équipements et des mécanismes (matériels et logiciels) soient incorporés dans le système informatique pour réaliser la disponibilité, l'intégrité et la confidentialité des informations prévues par les objectifs de sécurité..."

"...Lorsque les mesures générales et particulières de sécurité déjà prises ne permettent pas d'assurer à des informations classifiées de défense, traitées par un système informatique, une protection correspondant à leur niveau de classification, il convient, en outre, de les protéger, soit à l'aide de moyens de sécurité informatiques agréés, soit en ayant recours à des produits informatiques agréés. Cet agrément est prononcé par le SCSSI à l'issue d'une évaluation effectuée sous la responsabilité du ministère de la défense ou du SCSSI et financée par le ministère demandeur."

Article 12 : Méthodologie de sécurisation d'un système d'information

- [25] "...La sécurité doit donc être prise en compte dès l'expression du besoin, puis tout au long de la vie d'un système d'information."

"...Il est donc nécessaire de rédiger une **fiche d'expression rationnelle des objectifs de sécurité** (FEROS), précisant la nature et le niveau de classification des informations que traitera ou utilisera le système d'information, rappelant les obligations légales et réglementaires, analysant les menaces et les risques, et indiquant, le cas échéant, les contraintes a priori, techniques ou non, qui restreignent les choix du concepteur du système et ont une incidence sur la sécurité..."