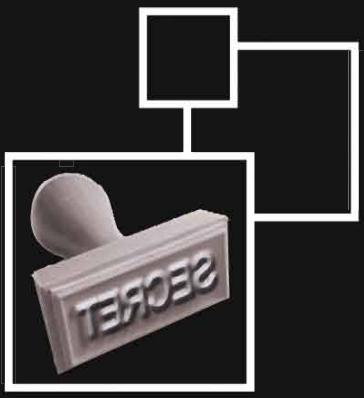
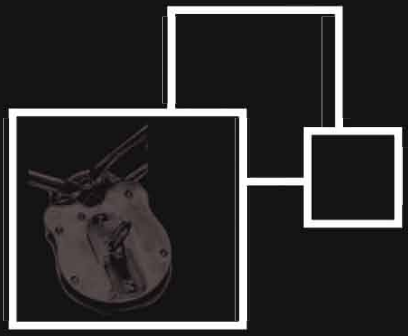
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE
ET DES
ANCIENS COMBATTANTS

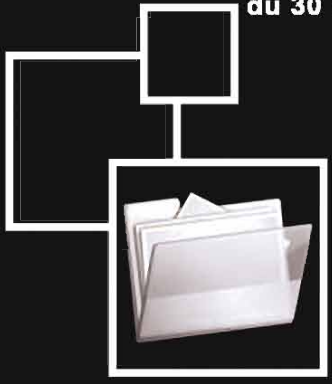
LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE

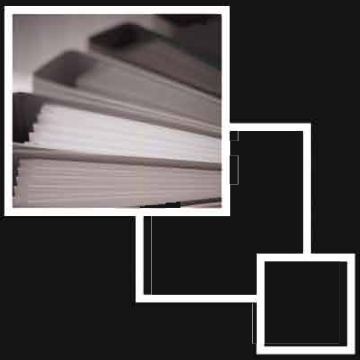
Guide pratique sur le traitement des informations et supports classifiés





Mis à jour après la publication de l'arrêté du 30 novembre 2011





Avant-propos...

Les personnes qui traitent ou détiennent des informations et supports classifiés au titre du secret de la défense nationale ont **l'obligation d'appliquer les mesures de protection prescrites dans l'instruction générale interministérielle 1300/SGDSN/PSE/PSD du 30 novembre 2011** élaborée par le SGDSN et signée par le Premier ministre.

Ce guide reprend certaines dispositions de **l'IGI 1300, seule réglementation officielle**, à laquelle il est nécessaire de se référer.

Il pourra être consulté avec profit par toutes les personnes qui détiennent ou traitent des informations et supports classifiés afin **d'éviter toute violation d'un secret de la défense nationale par inattention ou par ignorance.**

Le présent guide utilise, comme le prévoit **l'article R.2311-1 du code de la défense**, l'expression « informations et supports classifiés » pour désigner les **procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de la défense nationale.**

SOMMAIRE

I. Règles générales

A. Pourquoi classifier ?

Pour protéger le caractère secret de certaines informations relatives à la défense nationale tout en autorisant, sous conditions, leur traitement par des personnes habilitées.

La distinction entre des informations et supports classifiés d'un degré de sensibilité élevé et ceux d'un degré moindre s'effectue au moyen d'un niveau de classification.

Le choix d'un niveau de classification rend **obligatoire l'application des règles de protection prévues** (gestion des informations et supports classifiés, sécurité des locaux où ils sont manipulés, sécurité des systèmes d'information sur lesquels ils sont traités, sélection des personnes pouvant en prendre connaissance).

En dehors du Très Secret Défense, qui n'est pas traité dans ce guide, il existe deux niveaux de classification :

• Le **Secret Défense** est réservé aux informations et supports classifiés dont la divulgation est de nature à nuire gravement à la défense nationale.

• Le **Confidentiel Défense** est réservé aux informations et supports classifiés 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.

La décision de classification appartient à l'autorité hiérarchique : un secrétariat ne peut jamais en prendre l'initiative, mais **il peut attirer l'attention de l'autorité hiérarchique** sur l'absence de classification d'une information ou d'un support habituellement classifié au sein du service.

B. Conséquences de la classification pour les documents, les personnes et les lieux

En classifiant des informations et/ou leurs supports, l'autorité hiérarchique s'engage et engage son service, notamment son secrétariat, à leur appliquer des règles de protection particulières.

Tout manquement à ces règles de protection est une **faute professionnelle** et s'il entraîne la violation d'un secret de la défense nationale, constitue le délit pénal de compromission.

Les peines encourues sont lourdes (article 413-10 du code pénal) : 7 ans d'**emprisonnement** et **100 000 € d'amende**. Même pour des personnes ayant agi **par imprudence ou négligence**, la peine encourue est de 3 ans d'emprisonnement et de **45 000 € d'amende.**

C. La sécurité des personnes

L'accès aux informations et supports classifiés est strictement réservé aux personnes habilitées.

Deux conditions sont nécessaires pour être habilité :

• **avoir fait l'objet d'une décision préalable d'habilitation** : il s'agit d'une procédure de contrôle préalable des personnes qui, pour les besoins de leur travail, doivent avoir accès à des informations et supports classifiés.

Remarque : cette procédure (demande, constitution du dossier etc.) est décrite dans l'IGI 1300, titre II.

• **avoir besoin d'en connaître** : il s'agit d'une règle de contrôle permanent de la destination des informations et supports classifiés : nul ne peut avoir accès à ces informations s'il n'a pas besoin d'en prendre connaissance pour accomplir sa mission, même s'il est habilité.

Remarque : *cette règle ne connaît* ***aucune exception. Un secrétariat saisi d'une demande de communication d'une information et/ou d'un support classifié doit toujours en référer à l'autorité hiérarchique qui appréciera, sous sa responsabilité, du « besoin d'en connaître ».***

Les convoyeurs d'informations et de supports classifiés font l'objet d'une **décision de « sécurité convoyeur »**, mais celle-ci ne leur permet, en aucun cas, de prendre connaissance des informations transportées – **article 36 de l'IGI 1300**. Cette décision est accordée pour une durée déterminée sans excédée trois ans.

Un **certificat de sécurité** est nécessaire pour indiquer le niveau d'habilitation d'une personne lors d'une mission à l'extérieur de son service (lors d'une réunion…) – **article 29 de l'IGI 1300**. Il est détruit dès le retour de mission.

L'accès aux informations et supports classifiés n'est jamais un droit, c'est toujours une obligation liée aux fonctions exercées.

II. Mesures à appliquer pour le traitement des informations et supports classifiés aux niveaux Secret Défense et Confidentiel Défense

A. Élaboration

SECRET DÉFENSE

Les documents sont élaborés dans des bureaux de protection du secret (BPS), situés dans des zones de sécurité appelées « zones réservées », exclusivement par du personnel habilité au niveau Secret Défense.

CONFIDENTIEL DÉFENSE

Les documents sont élaborés dans des locaux sécurisés présentant les garanties de sécurité suffisantes pour éviter toute divulgation, exclusivement par du personnel habilité au niveau Confidentiel Défense.

SECRET DÉFENSE et CONFIDENTIEL DÉFENSE

Les supports préparatoires (brouillons, impressions sur papier, disquettes…), placés sous la responsabilité de celui qui les a élaborés, doivent être détruits le plus rapidement possible, au plus tard lorsque le support classifié est émis.

Cette destruction doit être effectuée par des personnes habilitées au niveau de classification des informations traitées (selon une procédure soumise à autorisation pour le niveau Secret Défense – **article 59 de l'IGI 1300**).

B. Enregistrement

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
• L'enregistrement se fait dans l'ordre chronologique, sur un système informatisé ou sur un registre spécifique classifié au niveau Secret Défense côté et paraphé. • Le nom des destinataires de l'information et/ou du support classifié est porté sur le système d'enregistrement. • L'enregistrement doit établir sans ambiguïté l'attribution du support à un destinataire. Cet enregistrement est en effet la seule référence de l'attribution de la responsabilité à une personne identifiée.	• L'enregistrement se fait sur un système informatisé ou sur un registre spécifique Confidentiel Défense côté et paraphé, pour apporter la preuve de l'attribution du support classifié à un détenteur identifié donc responsable.

C. Marquage

Le marquage a pour but :

1. de caractériser une information ou un support classifié ;
2. d'en assurer le contrôle et le suivi pendant toute son existence selon les règles de sécurité prescrites.

Le marquage comprend : **le timbrage, l'identification et la pagination.**

1. Le timbrage

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
Le timbre « Secret Défense » est apposé avec une encre rouge au milieu du haut et du bas de toutes les pages du document. SECRET DÉFENSE Lettres de 4 mm de hauteur sur 3 mm de largeur ; cadre et lettres de 1,5 mm d'épaisseur.	Le timbre « Confidentiel Défense » est apposé avec une encre rouge au milieu du haut et du bas de toutes les pages du document. CONFIDENTIEL DÉFENSE Lettres de 4 mm de hauteur sur 2 mm de largeur ; cadre et lettres de 1 mm d'épaisseur. Les dimensions du tampon peuvent être adaptées à la taille du support.

L'absence de marquage rend inopérante la protection pénale accordée au secret de la défense nationale : article 42 de l'IGI 1300.

SECRET DÉFENSE

Par ailleurs, il est également prévu d'apposer, par voie électronique le cas échéant, au milieu du bas de la première page des documents reliés disposant d'une couverture et éventuellement d'une page de garde, le timbre spécial suivant, lequel n'est donc pas à placer sur les autres documents tels que bordereau, note, etc. :

Toute personne qui détient ce document sans avoir qualité pour le connaître tombe sous le coup des dispositions du Code pénal réprimant les atteintes au secret de la défense nationale.

CONFIDENTIEL DÉFENSE

Comme pour le Secret Défense, il existe, également un timbre spécial, sur lequel il est indiqué :

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

SECRET DÉFENSE et CONFIDENTIEL DÉFENSE

Le timbre obligatoire est accompagné, dans la mesure du possible, d'une date de déclassification ou de déclassement (voir infra).

2. L'identification

Elle comporte sur la première page du document :

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
a) la référence et la date du document : • un numéro pris dans l'ordre chronologique d'un système d'enregistrement « DÉPART » du bureau de protection du secret compétent ; • la mention du service émetteur et la date de la signature. b) le numéro individuel de chaque exemplaire : • un numéro individualisant chaque exemplaire et faisant apparaître le nombre total d'exemplaires. Exemple : 3/12 : troisième exemplaire d'une série de douze exemplaires. • Lorsqu'il est impossible d'inscrire sur le support l'ensemble des références, l'identification est faite par le numéro d'enregistrement. **Voir Annexe 1**	a) la référence et la date du document : • un numéro pris dans l'ordre chronologique d'un système d'enregistrement « DÉPART » des documents Confidentiel Défense tenu par le service émetteur ; • la mention du service émetteur et la date de la signature. Lorsqu'il est impossible d'inscrire sur le support l'ensemble des références, l'identification est faite par le numéro d'enregistrement. **Voir Annexe 2**

3. La pagination

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
Chaque page du document est numérotée. Au bas de la première page est mentionné le nombre de pages, d'annexes ou de plans qui composent le document. Chaque annexe est également paginée et porte mention de son propre nombre de pages. Les pages blanches et les feuilles intercalaires doivent être numérotées et porter en leur centre la mention « PAS DE TEXTE »	Chaque page est numérotée. Au bas de la première page est mentionné le nombre de pages, d'annexes ou de plans qui composent le document. Chaque annexe est également paginée et porte mention de son propre nombre de pages.

D. Mesures spécifiques à l'usage des systèmes d'information :

• MARQUAGE :

Pour les supports autres que les supports papier, l'identification est assurée par l'inscription des références et éventuellement du volume de chacune des informations enregistrées.

Lorsqu'il est impossible d'inscrire l'ensemble des références, l'identification se fait par le numéro d'enregistrement du document, délivré par le bureau de protection du secret et éventuellement accompagné d'une fiche où sont inscrites les références réglementaires des informations contenues.

Les supports classifiés, autres que papier, doivent également comporter le timbre correspondant au niveau de classification des informations contenues et une identification.

Pour cela, le marquage est adapté au type de support, à ses dimensions. Il comporte l'indication du niveau de protection en toutes lettres, rouges ou contrastant avec la couleur du support. Il est définitif et toujours visible.

Ce type de support conserve toujours le niveau de classification qui lui a été initialement attribué.

• TRAVAIL EN RÉSEAU :

Tout système d'information traitant des informations et supports classifiés doit faire l'objet d'une décision d'homologation : une autorité dite d'homologation déclare que le système d'information concerné est considéré comme étant apte à traiter des informations et supports classifiés du niveau de classification retenu.

Seuls les utilisateurs ayant le niveau d'habilitation requis pour le niveau de classification de l'information et le besoin reconnu d'en connaître ont accès à ces systèmes d'information.

E. Diffusion

Lorsqu'elle diffuse des informations et supports classifiés, l'autorité d'expédition s'assure que les destinataires sont habilités au niveau requis.

L'autorité qui doit diffuser des informations et supports classifiés **au niveau Secret Défense** établit la liste de diffusion sur laquelle sont portés le nombre et le numéro des supports attribués à chaque destinataire ainsi que le numéro des exemplaires conservés par le service émetteur (deux au moins, dont un original destiné, à terme, aux archives).

La liste des destinataires, lorsqu'elle constitue en elle même un secret de la défense nationale, n'est pas jointe à l'envoi de chacun des exemplaires de support.

F. Envoi de documents classifiés

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
La procédure est conduite : • par le **bureau de protection du secret** par qui doivent transiter tous les documents SECRET DÉFENSE (départ, transmission en interne, arrivée).	La procédure est conduite : • soit par le secrétariat du service émetteur ; • soit par le bureau de protection du secret qui peut recevoir des attributions concernant l'ensemble du courrier classifié.

L'envoi de documents classifiés comporte trois étapes :

- la préparation du bordereau d'envoi ;
- le conditionnement ;
- l'enregistrement au départ (voir supra).

1. La préparation du bordereau d'envoi

SECRET DÉFENSE et CONFIDENTIEL DÉFENSE

On emploie un bordereau d'envoi **sans timbre de classification ni indication de l'objet des informations envoyées**, portant le numéro de l'enveloppe de sécurité et se composant de trois feuillets détachables A-B-B' (de préférence de couleurs différentes).

• Dans un premier temps, l'émetteur envoie à chaque destinataire les feuillets A et B du bordereau. Ces feuillets sont obligatoirement insérés dans l'enveloppe intérieure, puis il classe le bordereau B' en attente.

• Dans un deuxième temps, le destinataire retourne le feuillet B à l'émetteur après avoir visé l'accusé de réception.

• Dans un troisième temps, enfin, à réception du feuillet B, l'émetteur détruit l'exemplaire B' et classe le feuillet B.

2. Le conditionnement

SECRET DÉFENSE et CONFIDENTIEL DÉFENSE

Tout document est conditionné sous double enveloppe présentant les conditions de solidité et de sécurité maximales :

• **l'enveloppe extérieure**, plastifiée et numérotée (pour le SD), porte indication du service expéditeur, l'adresse du service destinataire et la mention du suivi. Elle ne doit porter aucune mention susceptible de révéler qu'elle contient un document classifié ;

• **l'enveloppe intérieure** de sécurité de bonne qualité, si possible, modèle « toilé » ou « armé », opaque et de dimension adaptée, contient les feuillets A et B du bordereau d'envoi.

Cette enveloppe intérieure comporte :
• un cachet de timbrage du niveau de classification du document ;
• les références de ce document ;
• le cachet de l'autorité signataire ;
• l'identification du destinataire (organisme et nom + fonction de la personne concernée).

G. Moyens d'acheminement et de transport : article 57 de l'IGI 1300

1. Sans changement d'immeuble

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
En règle générale, la communication d'un document Secret Défense doit être faite sur place par le détenteur avec compte rendu au bureau de protection du secret.	Par une personne habilitée ou, sous enveloppe, par un convoyeur autorisé, ou une personne du service courrier interne autorisée.

2. Avec changement d'immeuble sur le territoire national

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
• Par convoyeur autorisé ou toute personne habilitée au niveau Secret Défense. • Par voie postale militaire : dans les conditions fixées par les instructions du ministre de la Défense. • Par voie postale civile : à défaut de convoyeur ou de personne habilitée disponible dans des délais compatibles avec un degré d'urgence justifiable en recourant obligatoirement à des opérateurs postaux proposant des moyens de transport protégés.	• Par convoyeur autorisé ou toute personne habilitée au niveau Confidentiel Défense. • Par voie postale militaire : dans les conditions fixées par les instructions du ministre de la Défense. • Par voie postale civile : en ayant recours obligatoirement à des opérateurs postaux proposant des moyens de transport protégés.

3. Vers l'étranger

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
Les moyens autorisés sont : • la valise diplomatique ; • le courrier militaire spécialisé ; • la lettre de courrier délivrée par le ministère des Affaires étrangères et européennes ; • le certificat de courrier.	Vers les pays de l'Union européenne et de l'OTAN : • par valise diplomatique ; • par voie postale en « service prioritaire recommandé international » ; • par certificat de courrier. Vers les pays hors Union européenne : • par valise diplomatique, • par courrier militaire spécialisé, • par certificat de courrier.

Le transport est obligatoirement assuré par un convoyeur autorisé ou par une personne habilitée.

H. Réception de documents classifiés

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
Tous les documents Secret Défense, quel que soit le mode d'acheminement utilisé, doivent être réceptionnés par le bureau de protection du secret de l'organisme destinataire.	Tous les documents Confidentiel Défense, quelque soit le mode d'acheminement utilisé doivent être réceptionnés par le bureau d'enregistrement du courrier Confidentiel Défense de l'organisme destinataire.

SECRET DÉFENSE et CONFIDENTIEL DÉFENSE

Les formalités à la réception comprennent :

- la vérification de l'intégrité de l'emballage ;
- l'inscription dans l'ordre chronologique sur le cahier d'enregistrement « ARRIVÉE » prévu à cet effet ;
- la transmission par le bureau de protection du secret au destinataire ;
- la signature et le renvoi du feuillet B du bordereau d'envoi au bureau de protection du secret de l'autorité d'origine.

I. Reproduction des documents classifiés

Seul un chef de bureau, de service ou de division est compétent pour décider du besoin de reproduction d'une information ou d'un support classifié.

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
La reproduction totale ou partielle est interdite sans autorisation préalable de l'autorité émettrice (sauf cas d'urgence exceptionnelle et en rendant compte au plus tôt à l'autorité émettrice). La diffusion séquentielle d'extraits non classifiés par découpage de l'information classifiée est interdite.	La reproduction des documents classifiés Confidentiel Défense peut être effectuée par les autorités destinataires sous leur responsabilité et à condition de conserver sur un système d'enregistrement la trace du nombre et des destinataires des exemplaires reproduits.

J. Conservation

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
Les informations et supports classifiés sont, en dehors des périodes d'utilisation, conservés dans des coffres-forts ou des armoires fortes conformes aux dispositions relatives aux meubles de sécurité énoncées par l'IGI 1300. Les **combinaisons** sont changées au moins tous les six mois, lors des mutations du personnel utilisateur et en cas de risque ou de présomption de compromission. Les **zones réservées** sont créées pour la protection des informations et supports classifiés au niveau Secret Défense. Elles sont **incluses dans des zones protégées.**	Les informations et supports classifiés sont conservés dans des armoires fortes.

AUCUNE INDICATION RELATIVE À LA NATURE DE L'INFORMATION N'EST VISIBLE À L'EXTÈRIEUR DU MEUBLE DE SÉCURITÉ : ARTICLE 47 DE L'IGI 1300.

K. Inventaire

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
L'inventaire des documents Secret Défense est **obligatoire, il a lieu une fois par an** et est adressé au plus tard le 31 mars au SGDSN. Il est effectué par le bureau de protection du secret de l'organisme, et porte sur les documents détenus par l'ensemble de ses services : il consiste à contrôler à l'aide du système d'enregistrement l'existence physique du document. À cette occasion, il peut être procédé aux opérations de déclassification ou de destruction. Les systèmes d'enregistrement sont mis à jour en conséquence. **Lors de toute mutation de personnel**, un inventaire est effectué contradictoirement, chaque détenteur, sortant et arrivant, apposant sa signature sur le procès-verbal d'inventaire (transfert de responsabilité).	L'inventaire **annuel** des documents Confidentiel Défense n'est pas obligatoire mais recommandé pour en faciliter la gestion.

L. Durée de vie de la classification

SECRET DÉFENSE et CONFIDENTIEL DÉFENSE

En pratique, la sensibilité d'une information classifiée peut évoluer en fonction du temps ou des circonstances.

Seule l'autorité émettrice peut déclassifier ou déclasser une information ou un support classifié.

Au moment de la classification, l'autorité émettrice doit indiquer, dans la mesure du possible, sur la première page du document, l'une des deux mentions suivantes :

- **Déclassification sur ordre de l'émetteur**, lorsqu'on ignore le moment où l'information deviendra moins sensible.

À déclassifier sur ordre de l'autorité émettrice

- **Déclassification à terme fixé**, lorsqu'on peut apprécier le moment où la sensibilité de l'information aura faibli ou disparu.

À déclassifier à compter du :

- Pour **déclasser**, l'autorité émettrice procède à l'identique en utilisant les modèles de timbres décrits dans l'IGI 1300.

La révision du besoin et du niveau de classification des informations et supports classifiés doit être effectuée rigoureusement selon une périodicité inférieure ou égale à 10 ans.

À expiration d'un délai de 50 ans (sauf catégories particulières) à compter de la date d'émission du document classifié versé aux archives publiques, se pose la question de la communicabilité du document et de sa déclassification préalable.

M. Destruction

Les autorités détentrices de documents classifiés, qu'elles jugent périmés ou inutiles, peuvent procéder à leur destruction, notamment lors des inventaires.

La destruction doit être effectuée de façon à ce que le document ne puisse pas être reconstitué, même de façon fragmentaire. Les techniques de destruction sont choisies en fonction du type et du nombre de supports à détruire. Les principales sont : le brûlage, l'incinération, le broyage, le déchiquetage et la surtension électrique.

SECRET DÉFENSE

En l'absence de date précisée à l'origine par l'autorité émettrice, le détenteur d'un document Secret Défense doit lui faire connaître son intention de le détruire. Sauf avis contraire de celle-ci dans un délai de 2 mois, la destruction est possible.

Elle est effectuée par le détenteur en présence d'un témoin habilité au niveau Secret défense. Un procès verbal est signé par ces deux personnes : une copie est adressée à l'émetteur et une autre au bureau de protection du secret pour enregistrement.

CONFIDENTIEL DÉFENSE

Le détenteur d'un document Confidentiel Défense fait procéder à la destruction de celui-ci par une personne habilitée.

La mention de la destruction, avec la date, doit être portée sur le cahier d'enregistrement réservé au Confidentiel Défense.

N. Archivage

SECRET DÉFENSE et CONFIDENTIEL DÉFENSE

Dès qu'ils ne sont plus utilisés habituellement, les informations et supports classifiés présentant un intérêt administratif et historique sont versés, selon la périodicité prévue par chaque ministre, aux dépôts d'archives suivants :

- service historique de défense pour le ministère de la défense et des anciens combattants et les services rattachés ;
- archives du ministère des affaires étrangères et européennes pour ce qui le concerne ;
- direction générale des patrimoines de France – archives nationales et services publics d'archives – pour toutes les administrations et organismes civils gérant des archives publiques.

Ces services sont les seuls équipés et habilités pour recevoir des informations et supports classifiés jusqu'au niveau Secret Défense inclus.

III. Protection des lieux de traitement des informations et supports classifiés

SECRET DÉFENSE	CONFIDENTIEL DÉFENSE
Les locaux où sont traités des informations et supports classifiés Secret Défense doivent être aménagés en zones réservées.	Les locaux où sont traités des informations et supports classifiés Confidentiel Défense doivent présenter les garanties de sécurité nécessaires pour éviter toute divulgation.

SECRET DÉFENSE et CONFIDENTIEL DÉFENSE

Les règles qui suivent concernent la protection de tous les locaux dans lesquels sont traités ou détenus des informations et supports classifiés aux niveaux Secret Défense ou Confidentiel Défense.

La vigilance du personnel est déterminante pour assurer la meilleure protection possible.

A. Au début du travail

Au début du travail, des vérifications doivent être effectuées afin de détecter des anomalies pouvant révéler :

- une pénétration dans les locaux ;
- l'ouverture des meubles de sécurité ;
- une manipulation des matériels.

B. Pendant le travail

Pendant le travail, il est nécessaire de contrôler :

- l'accès aux locaux : liste et identification des personnes autorisées, accompagnement constant des visiteurs, **vérification du niveau d'habilitation** ;
- l'emploi des matériels de bureau à l'aide desquels sont traités des documents classifiés : clés USB, photos… ;
- le suivi des informations et supports classifiés qui, pendant la durée de leur exploitation, sont en dehors des meubles de sécurité.

La surveillance doit être renforcée à certains moments :

- heure des repas ;
- absence momentanée des occupants habituels ;
- travaux d'entretien divers.

Durant ces créneaux, les documents doivent, si possible, être enfermés dans des meubles de sécurité.

Les combinaisons des meubles de sécurité doivent être changées (et connues par le seul détenteur) :

- au moins tous les six mois ;
- lors des mutations du personnel ;
- après ouverture en l'absence du détenteur ;
- en cas de compromission supposée.

Chaque numéro de combinaison doit être inscrit et placé dans une enveloppe fermée, placée dans le coffre de l'autorité hiérarchique.

C. À la cessation du travail

Les informations et supports classifiés doivent être rangés dans le meuble de sécurité correspondant à leur niveau de protection :

- coffre-fort ou armoire forte à combinaisons multiples pour le Secret Défense ;
- armoire forte pour le Confidentiel Défense.

Aucune indication sur la nature des documents renfermés dans chaque meuble de sécurité ne doit apparaître. Doivent être rangés dans les meubles de sécurité, non seulement les documents eux-mêmes, mais également :

- les disques durs amovibles des postes de travail ;
- les micro-ordinateurs portables ;
- les clés USB et tout autre support informatique ;
- les brouillons ;
- les exemplaires ne pouvant pas être immédiatement détruits dans des conditions de sécurité suffisante.

Les coffres-forts et armoires fortes doivent être fermés et les compteurs de combinaison placés dans la position zéro.

Une double vérification de ces dispositions est recommandée pour tous les bureaux de protection du secret.

Des rondes de vérification d'exécution de ces mesures doivent être effectuées après la fin du travail.

L'entretien des locaux et des matériels ne peut se faire qu'en présence de personnes habilitées. Les techniciens opérant dans les zones réservées doivent avoir fait l'objet d'un contrôle élémentaire.

D. Pendant les réunions

Il convient de protéger :
les lieux, les personnes et les informations ou supports classifiés.

LES LIEUX

Le local prévu pour la séance doit être à l'abri de toute interception par écoute directe ou indirecte (insonorisation, absence de microphone).

Il est interdit d'accès aux personnes non habilitées et n'ayant pas à en connaître.

Il est inspecté avant, et si nécessaire, pendant et après chaque séance.

LES PERSONNES

Le libellé de l'invitation ou de la convocation doit préciser le niveau d'habilitation requis.

L'identité et le niveau d'habilitation des participants doivent être **contrôlés.**

L'autorité organisatrice s'assure que personne ne détient, lors de la réunion, un téléphone portable, un agenda électronique ou un ordinateur portable.

LES INFORMATIONS ET SUPPORTS

L'autorité organisatrice peut interdire toute prise de note ou enregistrement des interventions par les participants.

Les participants assument la pleine responsabilité de la protection de leurs documents de travail et notes, qui sont à classifier au niveau correspondant à celui des informations recueillies.
Ces divers documents sont détruits dès qu'ils ont cessé d'être utiles.

L'autorité organisatrice fait procéder en fin de séance :

- à la récupération et à la mise en sécurité des informations et supports classifiés éventuellement mis à la disposition des participants ;
- à la destruction des supports provisoires préparatoires.

IV. Conduite à adopter en cas de compromission

QU'EST-CE QU'UNE COMPROMISSION ?

Il y a compromission lorsqu'il y a **prise de connaissance, certaine ou possible**, d'une information et/ou support classifié **par une ou plusieurs personnes non autorisées**. Seule l'autorité hiérarchique peut apprécier les risques d'une compromission, avec l'aide des services spécialisés. De leur côté, les secrétariats et les bureaux courriers qui mettent en œuvre les règles permettant un contrôle continu de ces informations ont un rôle déterminant dans la détection des anomalies révélant une compromission. Ils doivent avertir l'autorité hiérarchique.

QUELQUES SIGNES SIGNIFICATIFS

- Dégradation des enveloppes réceptionnées.
- Disparition définitive ou temporaire d'un document et/ou d'un support informatique classifié.
- Traces de manipulation sur des meubles de sécurité.
- Utilisation de moyens d'acheminement non prescrits.
- Présence non justifiée de personnes dans les zones réservées ou les locaux sécurisés.
- Utilisation ou tentative d'utilisation d'un matériel en dehors des heures de travail…

CONDUITE À TENIR

Lorsqu'une anomalie est constatée, il convient :

- d'en rendre compte, immédiatement, à l'autorité hiérarchique et à l'Officier de Sécurité ;
- de ne procéder à aucune manipulation de l'objet en cause afin de préserver les indices qui seront examinés par les services spécialisés ;
- de modifier les combinaisons des meubles de sécurité.

V. Annexes

- Annexe I : Secret Défense

- Annexe II : Confidentiel Défense

Annexe I

1

PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

SECRET DÉFENSE 2

4 Exemplaire n° 1/3 5 1

3 N°_____/SGDSN/Service/SD
N°_____ /SGDSN/BPS/SD

Service .....

Déclassification à compter du :

7

Paris, le 6

Le secrétaire général de la défense et de la sécurité nationale

à

Monsieur le .....(destinataire)

Objet : .....
Référence : ...

TEXTE

9 Destinataires :
- Monsieur le ... (destinataire) Ex. 1/3

Archives :
- B.PS. Ex. 2/3
- Dossier Service Ex. 3/3

Signature

8

Ce document comporte : X pages 10

SECRET DÉFENSE

SECRET DÉFENSE

1. Références du service émetteur. Ensemble des renseignements qui permettent au destinataire du document d'en identifier immédiatement l'expéditeur.

2. Timbre « Secret Défense » apposé à l'encre rouge au milieu du haut et au milieu du bas de chaque page.

3. Identification sous forme d'une double numérotation :
- numéro du service émetteur
- numéro du bureau de protection du secret de l'organisme émetteur.

4. Complété après tirage, ce numéro individualise chaque exemplaire sous forme de fraction portant en numérateur (1er chiffre) le numéro d'ordre dans la série et en dénominateur (2e chiffre) le nombre total d'exemplaires.

5. Chaque page écrite du document doit être numérotée.

6. Lieu d'émission et date du document.

7. Ce cadre est rempli, chaque fois que possible, lorsque l'auteur du document a fixé une date de déclassification. Il peut être remplacé par le cadre :

Déclassification sur ordre de l'émetteur

8. Le signataire approuve le choix du niveau de classification retenu.

9. Liste de diffusion portant le nombre et le numéro des exemplaires attribués à chaque destinataire ainsi que ceux des exemplaires (2 au moins, dont un original) conservés par le service émetteur.

10. Nombre de pages, annexes, plans, etc. qui composent le document. Chaque annexe est également paginée et porte son propre nombre de pages.

Pour de plus amples informations, se référer aux articles 42 à 44 et 54 de l'IGI 1300.

1

PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Service .....

CONFIDENTIEL DÉFENSE

2

4 1

3 N°_____/SGDSN/Service/CD

Déclassification sur ordre de l'émetteur

Paris, le .....

5

6

Objet : .....
Référence : ...
Pièce jointe : une annexe.

TEXTE

Destinataires : 8

- M ; le ...
- M ; le ...
- M ; le ...
- Archives
- Chrono

Signature

7

CONFIDENTIEL DÉFENSE

CONFIDENTIEL DÉFENSE

1. Références du service émetteur. Ensemble des renseignements qui permettent au destinataire du document d'en identifier immédiatement l'expéditeur.

2. Timbre « Confidentiel Défense » apposé à l'encre rouge au milieu du haut et au milieu du bas de chaque page.

3. Numéro d'enregistrement chronologique du service émetteur.

4. Pagination.

5. Lieu d'émission et date du document.

6. Ce cadre doit, chaque fois que possible, être remplacé par le cadre de déclassification à terme fixé (voir exemple en annexe I).

7. Le signataire approuve le choix du niveau de classification retenu.

8. Liste de diffusion dans laquelle figurent tous les destinataires. Deux exemplaires du document au moins sont conservés par le service émetteur, dont un original.

Pour de plus amples informations, se référer aux articles 42 à 44 et 54 de l'IGI 1300.