PREMIER
MINISTRE

Liberté
Égalité
Fraternité

PROTECTION DU SECRET DE LA DÉFENSE NATIONALE

Fiches pratiques à destination des personnes habilitées

Version du 9 août 2021

Secrétariat général de la défense
et de la sécurité nationale

SOMMAIRE

Attention, ces fiches présentent les principales mesures définies dans l'instruction générale interministérielle n° 1300 (IGI 1300) qui peuvent être complétées par l'instruction ministérielle, les directives techniques particulières et/ou les dispositions contractuelles applicables au sein de votre organisme.

FICHE N° 1

Interlocuteurs en matière de protection du secret de la défense nationale

La mise en œuvre de la politique de protection du secret de la défense nationale repose sur plusieurs acteurs. Parmi eux, l'officier de sécurité est votre interlocuteur principal pour toutes questions relatives à la protection du secret (habilitation, élaboration ou envoi d'un document classifié, incident de sécurité, etc.).

1 L'officier de sécurité (OS) : votre interlocuteur privilégié en matière de protection du secret

- L'OS est votre interlocuteur privilégié pour toutes les questions et démarches liées à la protection du secret.
- Il gère les dossiers d'habilitation du personnel.

Bon à savoir C'est auprès de l'OS que :

- → vous engagez, à la demande de votre employeur, une procédure d'habilitation ou de renouvellement d'habilitation, en lui transmettant le formulaire de demande d'habilitation dûment rempli et signé ;
- → vous mettez à jour les informations personnelles consignées dans ce formulaire pendant toute la durée de votre habilitation ;
- → vous sollicitez un certificat de sécurité attestant de votre niveau d'habilitation (par exemple pour assister à une réunion « classifiée ») ;
- → vous êtes sensibilisé et formé aux enjeux de la protection du secret et aux règles de manipulation des informations et supports classifiés ;
- → vous signalez tout déplacement à l'étranger pour être informé des précautions à prendre avant, pendant et après votre voyage.

- Il est votre référent en matière de protection des informations et supports classifiés.

Bon à savoir C'est auprès de l'OS que :

- → vous vous assurez des règles de manipulation des informations et supports classifiés (élaboration, diffusion, destruction d'un document classifié, organisation d'une réunion « classifiée », etc.) ;
- → vous présentez, en cas de contrôle, votre inventaire des informations et supports classifiés au niveau *Secret* (y compris ceux portant l'ancien timbre de classification *Confidentiel-Défense*).

- Il est chargé de la gestion des incidents de sécurité.

Bon à savoir C'est auprès de l'OS que :

- → vous rendez compte de tout événement suspect (exemples : vous avez été interrogé de façon insistante sur votre travail ; vous avez vu une personne prendre des photographies d'un lieu abritant des informations et supports classifiés, etc.) ;
- → vous rendez compte de tout incident de sécurité (exemples : perte d'une clé USB contenant des informations classifiées, attaque informatique sur son poste de travail hébergeant des informations classifiées, vol d'un sac contenant un document classifié, suspicion de tentative d'approche, etc.).

Attention Informez simultanément votre officier de sécurité des systèmes d'information (cf. point 2) en cas d'incident de sécurité en lien avec le matériel informatique.

2 Autres interlocuteurs

- L'officier de sécurité des systèmes d'information (OSSI) pour les questions spécifiques à la sécurité des systèmes d'information.

Bon à savoir Prenez l'attache de l'OSSI si :

→ vous souhaitez avoir des renseignements pour élaborer, transmettre ou recevoir des informations classifiées de manière dématérialisée ;

→ vous êtes sensibilisé et formé aux enjeux de la protection du secret et aux règles de manipulation des systèmes d'information classifiés ;

→ vous avez besoin de connecter une clé USB à un système d'information classifié ;

→ vous souhaitez utiliser un ordinateur portable ou un rétroprojecteur lors d'une réunion « classifiée », etc.

- Le bureau de protection du secret (BPS) pour les questions spécifiques à la gestion des informations et supports classifiés *Très Secret* (et ceux portant l'ancien timbre de classification *Secret-Défense*).

Bon à savoir Prenez l'attache de votre BPS si :

→ vous souhaitez élaborer, transmettre ou recevoir des informations et supports classifiés à ce niveau ;

→ vous souhaitez obtenir une copie d'un document classifié à ce niveau ;

→ vous quittez vos fonctions afin de vérifier votre inventaire des informations et supports classifiés à ce niveau.

Attention Dans certaines structures, le BPS est également chargé de la gestion des informations et supports classifiés au niveau *Secret* (et ceux portant l'ancien timbre de classification *Confidentiel-Défense*).

- Les bureaux d'ordre « OTAN » et « UE » pour les questions spécifiques à la gestion des informations et supports classifiés de l'OTAN et de l'UE.

Bon à savoir Prenez l'attache du bureau d'ordre correspondant si :

→ vous souhaitez élaborer, transmettre ou recevoir un support classifié de l'OTAN ou de l'UE ;

→ vous souhaitez avoir une copie d'un document classifié de l'OTAN ou de l'UE.

Textes de référence

IGI 1300 Partie 2 « structures et instruments de pilotage et de mise en œuvre ».

FICHE N° 2

Habilitation au secret de la défense nationale

Pour pouvoir accéder à des informations et supports classifiés, vous devez être préalablement habilité au secret de la défense nationale. Cette habilitation intervient à l'issue d'une enquête administrative destinée à évaluer d'éventuelles vulnérabilités.

1 Prérequis : votre poste ou votre mission nécessite d'accéder à des informations et supports classifiés

- Votre procédure d'habilitation ne peut être initiée que si vous devez occuper un poste ou accomplir une mission nécessitant d'accéder à des informations et supports classifiés.

Bon à savoir Les postes nécessitant une habilitation figurent dans un document dénommé « catalogue des emplois » qui est tenu à jour par votre officier de sécurité. Le niveau d'habilitation requis y est précisé.

Attention Si votre poste ou mission figure dans le catalogue des emplois, cette procédure d'habilitation est obligatoire. Si vous accédez à des informations et supports classifiés sans être préalablement habilité, vous encourrez des sanctions pénales.

2 Procédure d'habilitation

- Si votre besoin d'accéder à des informations et supports classifiés est avéré, votre procédure d'habilitation est engagée.
- Renseignez le formulaire de demande d'habilitation (notice individuelle de sécurité) puis transmettez-le à votre officier de sécurité.

Bon à savoir Contactez votre officier de sécurité en cas de doute sur les informations à renseigner.

Rappel Ce formulaire vise à recueillir des informations personnelles vous concernant et concernant vos proches (conjoints, enfants, parents, etc.).

- L'officier de sécurité vérifie la complétude du dossier et le transmet à l'autorité d'habilitation compétente.

Bon à savoir L'officier de sécurité pourra prendre votre attache afin de vérifier certaines informations contenues dans votre formulaire.

Rappel Le Premier ministre est autorité d'habilitation pour les demandes au niveau *Très Secret* faisant l'objet d'une classification spéciale. Chaque ministre, pour son champ de compétence, est l'autorité d'habilitation pour les demandes aux niveaux *Secret* et *Très Secret* (hors classification spéciale), ainsi que pour les niveaux *Confidentiel OTAN*, *Secret OTAN* et *Confidentiel UE*, *Secret UE*.

- L'autorité d'habilitation saisit le service enquêteur compétent pour mener l'enquête administrative.

Bon à savoir L'enquête administrative peut durer plusieurs mois.

Rappel Cette enquête a pour objet de vérifier de façon objective qu'aucun élément dans votre situation ou comportement ou dans ceux des personnes qui vous sont proches n'est susceptible de constituer un risque pour le secret de la défense nationale, soit directement, soit compte tenu des risques de pression ou de chantage qui en découlent.

- À l'issue de l'enquête, l'autorité d'habilitation prend sa décision et en informe votre officier de sécurité.

3 Notification

- Votre officier de sécurité vous informe de la décision.
- Vous devez signer un engagement de responsabilité auprès de votre officier de sécurité en cas d'acceptation de votre habilitation (cf. fiche n° 3).

Attention Ce document fixe les obligations auxquelles vous devez vous conformer, sous peine d'engager votre responsabilité pénale.

Rappel La décision d'habilitation n'est remise qu'en cas de refus. Les voies et délais de recours y sont alors précisés.

4 Durée de votre habilitation

- Votre habilitation prend fin :
  - → à la date d'échéance fixée par l'autorité d'habilitation ;
  - → lorsque le besoin d'en connaître n'est plus justifié, notamment lorsque vous quittez votre poste ou que vous achevez votre mission.

Bon à savoir L'enquête administrative a une durée de validité limitée. Si cette dernière expire alors même que vous êtes toujours en poste, une procédure de renouvellement de votre habilitation devra être engagée.

Textes de référence

Code de la défense Articles R. 2311-7, R. 2311-8, R. 2311-8-1 et R. 2311-8-2.

IGI 1300 Partie 3 « mesures de sécurité applicables aux personnes physiques ».

FICHE N° 3

Obligations liées à l'habilitation

L'autorisation d'accéder, pour l'exercice de vos fonctions, à des informations et supports classifiés, vous confère des droits mais aussi des obligations. Certaines de ces obligations perdurent au-delà du terme de votre habilitation.

1 Au moment de votre habilitation, vous devez :

- Signer auprès de votre officier de sécurité le premier volet de l'engagement de responsabilité.
- Être sensibilisé à la protection du secret par votre officier de sécurité et le cas échéant par votre officier de sécurité des systèmes d'information.
- Vérifier l'inventaire des documents classifiés mis en votre possession (cf. fiche n° 7).

Rappel L'inventaire d'arrivée est vérifié de façon contradictoire avec votre prédécesseur ou, à défaut, avec votre officier de sécurité.

- Prendre l'attache de l'officier de sécurité des systèmes d'information pour obtenir le matériel informatique nécessaire au traitement d'informations classifiées (clé USB, etc.).

2 Durant toute la durée de votre habilitation, vous :

- Pouvez accéder aux informations et supports classifiés en fonction de votre niveau d'habilitation et de votre besoin d'en connaître.

Bon à savoir Le besoin d'en connaître est entendu strictement : il s'agit de la nécessité impérieuse de prendre connaissance d'une information dans l'exercice de vos fonctions ou l'accomplissement de votre mission.

- Devez être sensibilisé et formé à intervalle régulier par votre officier de sécurité et votre officier de sécurité des systèmes d'information à la protection du secret.
- Ne devez divulguer aucune information classifiée à des tiers, à l'exception des personnes habilitées au niveau approprié et dont le besoin d'en connaître est avéré.

Bon à savoir Vérifiez le besoin d'en connaître et le niveau d'habilitation de vos correspondants en leur demandant un certificat de sécurité.

Attention Votre responsabilité pénale peut être engagée si vous communiquez des informations classifiées à des personnes qui ne remplissent pas ces critères.

- Êtes tenu d'informer votre officier de sécurité de tout changement affectant votre vie personnelle ou professionnelle.

Rappel Mettez à jour votre notice individuelle de sécurité en liaison avec votre officier de sécurité dans les cas suivants : changements dans votre vie sentimentale (relation suivie, concubinage, pacte civil de solidarité, mariage, séparation), familiale (naissance, adoption, etc.) ou amicale (relation suivie hors du cadre professionnel avec un ressortissant étranger, etc.), déménagement, déplacements professionnels ou personnels à l'étranger, etc.

- Restez discret sur votre habilitation et vos missions.

Rappel Cette consigne s'applique dans tous vos échanges privés et professionnels (pas de mention dans vos cv. ou réseaux sociaux, y compris réseaux sociaux professionnels type LinkedIn).

- Mettez à jour l'inventaire des documents classifiés en votre possession depuis votre prise de poste (cf. fiche n° 7).
- Signalez à votre officier de sécurité tout incident de sécurité (perte d'une clé USB contenant des informations classifiées, attaque informatique sur votre poste de travail hébergeant des informations classifiées, vol d'un sac contenant un document classifié, suspicion de tentative d'approche, etc.).

Rappel Tout incident de sécurité affectant les systèmes d'information classifiés (vol d'un ordinateur portable, perte d'une clé USB, crainte d'une tentative de piratage, etc.) doit être simultanément signalé à votre officier de sécurité des systèmes d'information.

3 À l'issue de votre habilitation, vous devez :

- Vérifier que l'inventaire des documents classifiés en votre possession est à jour lorsque vous quittez la fonction ou achevez la mission qui justifiait habilitation (cf. fiche n° 7).

Rappel L'inventaire de départ est vérifié de façon contradictoire avec votre successeur ou, à défaut, votre officier de sécurité.

- Restituer à votre officier de sécurité des systèmes d'information les ordinateurs portables et supports amovibles (clés USB, etc.) mis à disposition pour traiter d'informations classifiées.
- Signer auprès de votre officier de sécurité le second volet de votre engagement de responsabilité.
- Ne jamais divulguer d'informations classifiées dont vous avez eu connaissance.

Rappel La discrétion à l'égard de votre habilitation perdure de la même manière.

Textes de référence

Code de la défense	Articles R. 2311-7, R. 2311-8, R. 2311-8-1 et R. 2311-8-2.
Code pénal	Articles 413-9 à 413-12.
IGI 1300	Partie 3 « mesures de sécurité applicables aux personnes physiques », annexe 7 « modèle de dossier de demande d'habilitation d'une personne physique », annexe 11 « modèle d'engagement de responsabilité » et annexe 14 « modèle de certificat de sécurité ».

FICHE N° 4

Classifier une information ou un support

Classifier une information au titre du secret de la défense nationale est un acte juridique fort entraînant d'importantes conséquences : il induit la mise en œuvre de mesures de protection rigoureuses susceptibles d'entraîner, en cas de non-respect, des sanctions pénales.

1 Évaluation de la sensibilité et du niveau de classification

▶ Lors de la création d'un document ou d'un support, il convient d'évaluer sa sensibilité et d'apposer le marquage correspondant (cf. annexe 1).

Rappel Lorsque vous déterminez le niveau de protection, respectez la consigne « ni trop, ni trop peu ».
Afin de définir le niveau de protection adéquat, utilisez le guide de classification définit dans la ou les instruction(s) ministérielle(s) applicables à votre organisme, ainsi, que le cas échéant, dans les directives techniques particulières et les plans contractuels de sécurité pertinents.

Attention Appliquez le « timbre de classification » dès les premiers brouillons ou premiers supports ; manipulez et conservez ces documents en conséquence.
L'agrégat d'un ensemble d'informations d'un niveau de protection ou de classification donné peut en accroître la sensibilité. Ainsi, un agrégat d'informations protégées par la mention *Diffusion Restreinte* peut nécessiter une classification au niveau *Secret*. De même, un agrégat d'informations de niveau *Secret* peut nécessiter une classification au niveau *Très Secret*.

▶ Si la sensibilité de l'information nécessite d'en restreindre l'accès aux seules personnes disposant du besoin d'en connaître, mais n'est pas telle qu'elle justifie une protection au titre du secret de la défense nationale, utilisez la mention *Diffusion Restreinte* (cf. fiche n° 5).

2 Création du document

▶ Utilisez un système d'information homologué au niveau approprié.

Bon à savoir Le niveau d'homologation du système d'information est généralement précisé sur l'étiquette apposée sur le matériel.

Rappel En cas de doute, adressez-vous à votre officier de sécurité des systèmes d'information.

Attention Vous ne devez pas commencer à élaborer votre document informatique sur un matériel non classifié ou sous-classifié.

▶ Conformez-vous aux exigences de présentation et de formalisme prévues par le niveau de classification utilisé.

Rappel Pour le niveau *Secret*, reportez-vous à l'annexe 2. Pour le niveau *Très Secret*, prenez préalablement contact avec votre bureau de protection du secret. Pour les classifications « OTAN » ou « UE », prenez l'attache du bureau d'ordre correspondant.

Bonne pratique Pour vos fichiers informatiques, nommez-les en signalant la classification par une abréviation et faites immédiatement figurer le marquage dans le document.

▶ Fixez la date obligatoire d'échéance de classification en fonction de la durée de sensibilité de vos informations.

Bon à savoir L'échéance de la classification n'entraîne pas automatiquement la libre communicabilité du document, dont la communication peut, en fonction de l'objet et de la date du document, continuer à faire l'objet de restrictions au titre du code des relations entre le public et l'administration, et du code du patrimoine.

Rappel La durée de classification doit être inférieure à 50 ans, et même, largement inférieure à 50 ans dans la très grande majorité des cas.

Attention En cas d'impossibilité, déterminez une date de réévaluation de la classification inférieure à 20 ans.

▶ Indiquez, le cas échéant, dans votre document classifié les paragraphes qui ne sont pas soumis à protection.

Rappel Faites figurer dans la marge des paragraphes concernés la mention [NP] pour non protégé, [DR] pour diffusion restreinte. Cela vous permettra par la suite de réutiliser ces éléments dans des documents non protégés au titre du secret de la défense nationale et de respecter l'exigence de classification au strict besoin.

▶ Utilisez la mention « Spécial France » pour restreindre l'accès de l'information aux seuls ressortissants français.

3 Traçabilité

▶ Faites enregistrer votre document.

Bon à savoir Aucune démarche d'enregistrement n'est à effectuer pour les documents dématérialisés. La traçabilité du document est assurée par le système d'information.

Rappel Pour le niveau *Secret*, adressez-vous au service chargé de l'enregistrement (secrétariat, bureau de protection du secret, etc.) ; pour le niveau *Très Secret* à votre bureau de protection du secret de votre organisme ; pour l'OTAN ou l'UE à votre bureau d'ordre correspondant.

▶ Mettez à jour votre inventaire.

Rappel Pour les documents classifiés au niveau *Très Secret*, cet inventaire est établi avec l'appui du bureau de protection du secret (cf. fiche n° 7). Pour les documents classifiés « OTAN » et « UE », il est établi avec l'appui du bureau d'ordre correspondant.

Attention Tout détenteur de documents classifiés au niveau *Secret* (y compris ceux portant l'ancien timbre de classification *Confidentiel-Défense*) doit obligatoirement disposer d'un inventaire.

Textes de référence

Code du patrimoine Article L. 213-2.

IGI 1300 Parties 6 « sécurité des systèmes d'informations classifiés » et 7 « gestion des informations et supports classifiés tout au long de leur cycle de vie ».

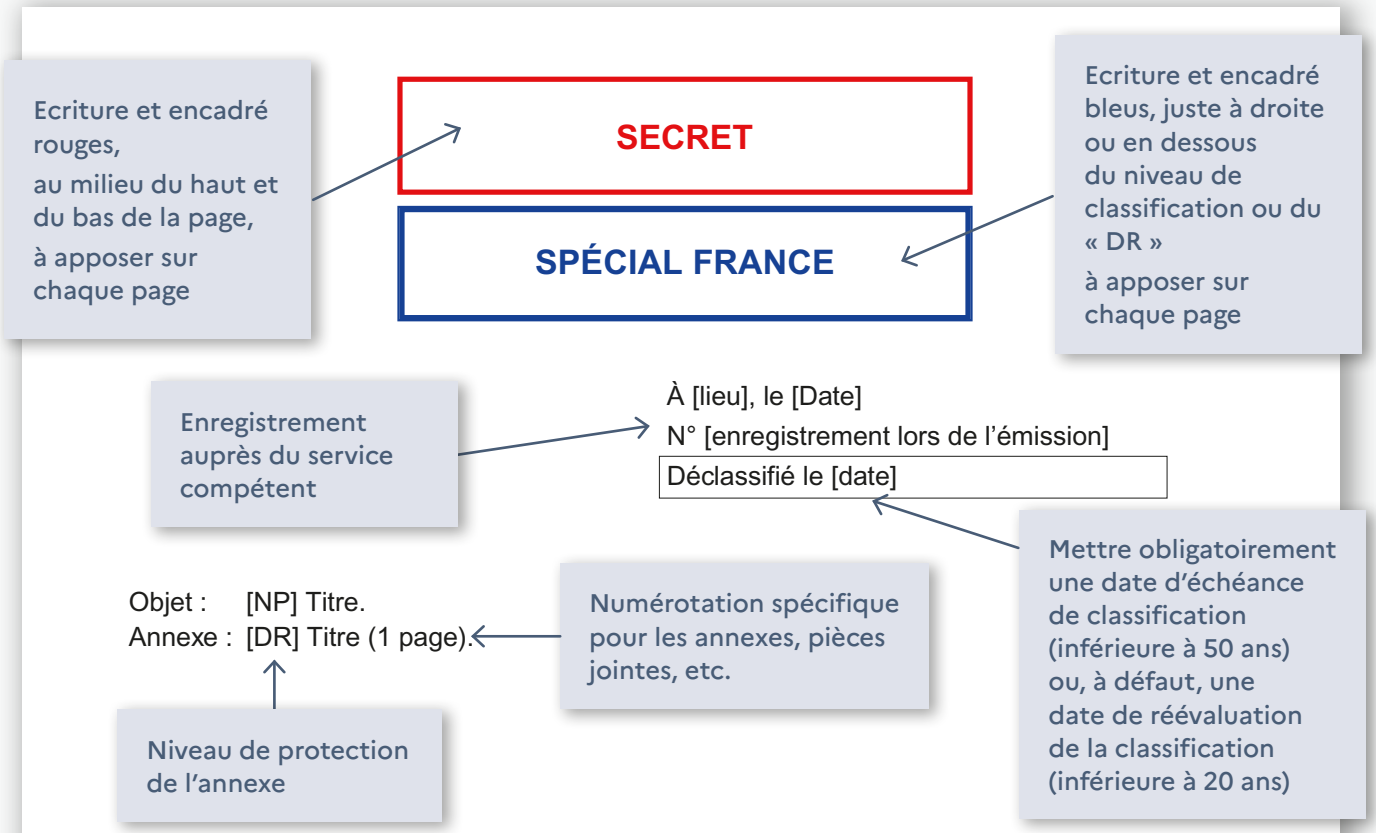
Annexe 1 Présentation des niveaux de classification français, de l'UE et de l'OTAN

Niveau de classification	Conséquences de l'atteinte en cas de divulgation non autorisée	Timbre de classification à apposer
Très Secret	Divulgation qui aurait des conséquences exceptionnellement graves pour la défense et la sécurité nationale. Des classifications spéciales sont créées, pour le niveau *Très Secret*, pour protéger les informations relatives aux priorités gouvernementales en matière de défense et de sécurité nationale	TRÈS SECRET
Secret	Divulgation de nature à porter atteinte à la défense et à la sécurité nationale	SECRET

Si votre organisme est autorisé à produire des informations et supports classifiés de l'UE ou de l'OTAN, vous pourriez être amenés à utiliser les timbres suivants :

Niveau de classification	Conséquences de l'atteinte en cas de divulgation non autorisée	Timbre de classification à apposer
Très Secret UE	Divulgation causant un préjudice exceptionnellement grave aux intérêts de l'UE ou d'un ou de plusieurs de ses États membres	TRÈS SECRET UE / EU TOP SECRET
Secret UE	Divulgation de nature à nuire gravement aux intérêts essentiels de l'UE ou d'un ou de plusieurs de ses États membres	SECRET UE / EU SECRET
Confidentiel UE	Divulgation de nature à nuire aux intérêts essentiels de l'UE ou d'un ou de plusieurs de ses États membres	CONFIDENTIEL UE / EU CONFIDENTIAL
Très Secret COSMIC	Divulgation qui aurait des conséquences exceptionnellement graves pour l'OTAN	TRÈS SECRET COSMIC
Secret OTAN	Divulgation qui aurait des conséquences graves pour l'OTAN	SECRET OTAN
Confidentiel OTAN	Divulgation qui serait préjudiciable aux intérêts de l'OTAN	CONFIDENTIEL OTAN
Diffusion Restreinte OTAN	Divulgation qui serait préjudiciable aux intérêts de l'OTAN mais nécessitant une protection inférieure à celle qui est assurée aux informations *Confidentiel OTAN*	DIFFUSION RESTREINTE OTAN

Annexe 2 Modèle de document classifié au niveau *Secret*



1. Chapitre contenant des informations classifiées jusqu'au niveau *Secret* et protégées par la mention *Spécial France*

[NP] Paragraphe contenant des éléments non classifiés et non *Diffusion Restreinte*.

Paragraphe contenant des éléments classifiés au niveau *Secret* et protégés par la mention *Spécial France*

Préciser lorsque les informations ne sont pas protégées ou sont d'un niveau de protection différent

2. Chapitre contenant des informations classifiées jusqu'au niveau *Secret* et protégées par la mention *Spécial France*

[DR] Paragraphe contenant des éléments non classifiés mais *Diffusion Restreinte*.

Paragraphe contenant des éléments classifiés au niveau *Secret* et protégés par la mention *Spécial France*

SECRET

Nombre total de pages dans le document

Page 1 sur 2

Ecriture et encadré rouges,
au milieu du haut et du bas de la page,
à apposer sur chaque page

DIFFUSION RESTREINTE

Annexe : titre

[NP] Paragraphe 1

Paragraphe 2

Indique que l'information n'est pas protégée

Numérotation indépendante de celle du document

Page 1 sur 2

FICHE N° 5

Utiliser la mention de protection *Diffusion Restreinte*

La protection accordée aux documents et supports portant la mention *Diffusion Restreinte* ne relève pas du secret de la défense nationale. Cette mention de protection permet toutefois de signaler qu'un document ou support contient des informations sensibles. Elle implique des utilisateurs qu'ils se conforment à une certaine discrétion et à des règles de protection spécifiques.

1 Évaluation de la sensibilité des informations

- Évaluez la sensibilité des informations contenues dans le document ou support lors de sa création.
- Apposez la mention de protection *Diffusion Restreinte* si vous jugez que l'information ne relève pas de la protection du secret de la défense nationale mais possède une certaine sensibilité.

Bon à savoir La mention *Diffusion Restreinte* peut par exemple être utilisée lorsqu'une information est susceptible de porter atteinte à la conduite de la politique extérieure de la France, à la sûreté de l'État, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations.

Rappel Il n'est pas nécessaire d'être habilité pour utiliser la mention *Diffusion Restreinte*. Toutefois, seules les personnes disposant du besoin d'en connaître peuvent y avoir accès.

Attention Plusieurs informations *Diffusion Restreinte* rassemblées peuvent devenir plus sensibles et nécessiter une classification au niveau *Secret*.

2 Création du document

- Utilisez un système d'information homologué au niveau *Diffusion Restreinte* ou classifié.

Attention Sauf urgence, vous ne devez pas commencer à élaborer votre document informatique sur un matériel non protégé.

- Conformez-vous aux exigences de présentation et de formalisme prévues pour la mention *Diffusion Restreinte* et, le cas échéant, à celles prévues dans votre organisme.

Bon à savoir La mention complémentaire de protection *Spécial France* peut être accolée à la mention *Diffusion Restreinte* si l'information ne doit être diffusée qu'aux ressortissants français (abréviation « DR-SF »).

Rappel Si la mention *Diffusion Restreinte* ne peut être apposée en toutes lettres sur le document en raison de son format, utilisez l'abréviation « DR ».

Attention La mention *Diffusion Restreinte* ne se met qu'en haut des documents, contrairement aux timbres de classification qui sont apposés en haut et en bas.

- Indiquez dans votre document protégé les paragraphes qui ne nécessitent pas de protection.

Rappel Faites figurer dans la marge du paragraphe la mention [NP] pour non protégé.

3 Traçabilité

- Faites enregistrer vos documents *Diffusion Restreinte* auprès du service compétent au départ et à l'arrivée (votre secrétariat par exemple).

4 Gestion du document tout au long de son cycle de vie

- Rapprochez-vous de votre officier de sécurité afin de connaître les modalités de gestion des documents *Diffusion Restreinte*.

Bon à savoir Conservez ces documents portant la mention *Diffusion Restreinte* dans un meuble fermant à clef ou sur un système d'information homologué *Diffusion Restreinte* ou classifié.
Limitez au strict nécessaire les copies dématérialisées et papier de ces documents.
Transmettez de et vers un système d'information homologué *Diffusion Restreinte* ou classifié ou par courrier sous double enveloppe.

Attention Certaines messageries sont homologuées *Diffusion Restreinte* uniquement pour les envois internes à votre structure et non pas pour les envois vers l'extérieur. Dans ce cas, pensez à utiliser un moyen de chiffrement (Acid, Zed!). En cas de doute, contactez votre officier de sécurité des systèmes d'information.

Textes de référence

IGI 1300 Partie 1 « principes généraux » et annexe 1 « règles de protection des informations et supports portant la mention *Diffusion Restreinte* ».

II 901 Relative à la protection des systèmes d'information sensibles.

FICHE N° 6

Protection des informations et supports classifiés

Aussi bien pendant leur utilisation qu'en dehors de cette période, vos informations et supports classifiés doivent être protégés de façon à ne pas être accessibles à des personnes non autorisées.

1 Pendant leur utilisation

- Veillez à ce qu'aucune information ne soit visible d'une personne non autorisée lorsque vous produisez ou consultez des informations classifiées.
- Lorsque vous vous absentez du bureau même momentanément, adoptez la politique du « bureau propre » et de l'« écran vide ».

Bon à savoir Dès que vous vous absentez, verrouillez votre ordinateur et rangez les documents papier et clés USB classifiés dans votre coffre-fort.

2 En dehors des périodes d'utilisation

- Rangez vos supports classifiés (document papier, CD-Rom, ordinateur portable, clé USB, etc.) dans un coffre-fort approprié à leur niveau de classification.

Bon à savoir Si vous avez oublié la combinaison de votre coffre-fort, contactez votre officier de sécurité.

Attention La conservation d'informations et supports classifiés nationaux, UE et OTAN dans un même coffre-fort est autorisée sous réserve de mettre en place les mesures nécessaires pour préserver le besoin d'en connaître (séparation physique des documents et précision de l'origine des documents).

- Conservez vos informations classifiées dématérialisées (messages, fichiers informatiques, etc.) sur un système d'information homologué au niveau approprié.

Rappel Le niveau d'homologation du système d'information est généralement précisé sur l'étiquette apposée sur le matériel.

Textes de référence

IGI 1300 Partie 7 « gestion des informations et supports classifiés tout au long de leur cycle de vie ».

FICHE N° 7

Faire l'inventaire des supports classifiés

L'inventaire est un élément essentiel de la traçabilité des supports couverts par le secret de la défense nationale. Il vise à connaître précisément les supports classifiés que vous détenez et à vérifier qu'aucune perte n'est à déplorer. Il permet par ailleurs de s'interroger sur la pertinence de la classification des supports détenus.

1 Obligation d'inventorier tous vos supports classifiés « physiques »

▶ L'inventaire ne porte que sur les supports « physiques » classifiés (document, clé USB, CD-Rom, disque dur, etc.) dont vous êtes détenteur.

Bon à savoir Les informations classifiées dématérialisées (exemples : courriels, fichiers informatiques, etc.) n'ont pas à être inventoriées. Leur traçabilité est assurée par le système d'information.

Rappel Prenez l'attache de votre bureau de protection du secret pour connaître les modalités d'inventaire des supports *Très Secret* (et de ceux portant l'ancien timbre de classification *Secret-Défense*) et du bureau d'ordre correspondant pour celui des supports « UE » et « OTAN ».

Attention Les informations classifiées dématérialisées que vous imprimez doivent être enregistrées et intégrées à votre inventaire.

▶ Tenez à jour l'inventaire de vos supports classifiés pendant toute la durée de votre poste ou de votre mission.

Bon à savoir L'inventaire est réalisé :

→ lors de votre prise de poste, idéalement avec l'ancien détenteur, sous réserve que vous soyez habilité ; à défaut, dès que votre habilitation est prononcée ;

→ chaque année, avant le 31 décembre ;

→ lorsque vous quittez votre poste, idéalement avec votre successeur, sous réserve qu'il soit habilité.

Rappel Pensez à mettre à jour votre inventaire dès que vous : élaborez un nouveau support classifié et que vous le conservez ; recevez un nouveau support classifié et que vous le conservez ; réalisez une copie d'un support classifié et que vous la conservez ; transmettez définitivement un support classifié que vous déteniez.

Attention Lors de l'inventaire contradictoire avec votre prédécesseur, vérifiez que les supports qui y sont indiqués sont bien présents. N'oubliez pas de dater et signer le procès-verbal contradictoire.

2 Déroulé de l'inventaire

- Vérifiez la présence physique des supports classifiés listés dans votre inventaire.
- Vérifiez que la classification des informations et supports classifiés (niveau et durée de classification) dont vous êtes l'auteur est toujours justifiée (cf. fiche n° 8).

Bon à savoir Vous ne pouvez proposer à l'autorité émettrice de faire évoluer la classification que des documents dont vous êtes l'auteur.

- En cas de doute, vérifiez que la classification des informations et supports classifiés dont vous n'êtes pas l'auteur est restée inchangée (cf. fiche n° 8).

Bon à savoir Contactez l'auteur afin de vous assurer que le document n'a pas été déclassifié.

- Conservez dans votre coffre-fort uniquement les supports utiles à votre travail quotidien. Archivez ou détruisez les autres supports (cf. fiche n° 13).

Rappel Si les supports versés aux archives ou détruits sont répertoriés dans votre inventaire, précisez dans ce dernier la date de versement aux archives ou de leur destruction.

Textes de référence

IGI 1300 Partie 7 « gestion des informations et supports classifiés tout au long de leur cycle de vie » et annexe 46 « modèle d'inventaire des supports classifiés ».

FICHE N° 8

Évaluation de la pertinence de la classification

La pertinence de la classification des informations dont vous êtes le détenteur évolue dans le temps. Il convient à ce titre, au moment de l'inventaire annuel et avant le versement aux archives, de réévaluer la pertinence de la classification des informations (niveau et durée de classification) dont vous êtes l'auteur.

1 Au moment de l'élaboration de l'information

- Vous devez évaluer au mieux la nécessité et, le cas échéant, le niveau de classification approprié, conformément au guide de classification ou au plan contractuel de sécurité applicables.

Rappel Il vous appartient de trouver le bon équilibre selon la règle : « ni trop, ni trop peu » :

- → une classification abusive entraîne des conséquences : mesures de protection contraignantes et coûteuses, lourdeur des procédures administratives, risques judiciaires, dépréciation du principe de la classification, etc.
- → à l'inverse, ne pas recourir à la classification ou au bon niveau de classification affaiblit la protection du secret de la défense nationale et facilite l'action malveillante des services de renseignement étrangers, des groupements hostiles ou des individus cherchant à déstabiliser l'État ou la société.

- Vous devez faire figurer une date d'échéance de classification au-delà de laquelle votre information ne sera plus protégée au titre du secret de la défense nationale, conformément, le cas échéant, au guide de classification ou au plan contractuel de sécurité applicables (cf. fiche n° 4).

2 Chaque année, lors de l'inventaire

- Chaque année, au moment de l'inventaire, demandez-vous si la classification des informations et supports classifiés dont vous êtes l'auteur est toujours justifiée. Proposez, le cas échéant, à l'autorité émettrice de faire évoluer le niveau et/ou la durée de classification.

Bon à savoir Vous pouvez proposer à l'autorité émettrice de :

- → déclassifier ou d'abaisser le niveau de classification (déclassement) des informations ayant, selon vous, perdu en sensibilité ;
- → relever le niveau de classification (reclassement) des informations ayant, selon vous, gagné en sensibilité ;
- → réduire ou allonger la durée de classification des informations en fonction de l'évolution de la menace ;
- → le cas échéant, réexaminez la date de réévaluation de la classification (cf fiche n° 4)

Rappel Sauf exceptions prévues dans le cadre de la gestion des archives publiques, une décision administrative doit obligatoirement être prise par l'autorité émettrice avant toute modification du niveau ou de la date d'échéance de classification sur le document.

▶ En cas d'accord de l'autorité émettrice et sauf exceptions prévues dans le cadre de la gestion des archives publiques, apposez le marquage approprié sur le support :

DÉCLASSIFIÉ
le
par décision n°
du

Le déclassement du niveau *Très Secret* au niveau *Secret*
intervient le
par décision n°
du

Le reclassement du niveau *Secret* au niveau *Très Secret*
intervient le
par décision n°
du

Classification à réévaluer le *[date]*

Attention Pensez à informer les destinataires des documents de tout changement dans la classification.

▶ Pour les documents classifiés dont vous n'êtes pas l'auteur et qui ne comportent pas de date d'échéance de classification, vous pouvez contacter le service auteur afin de vous assurer que la classification du document est restée inchangée.

Bon à savoir S'il s'agit d'un document *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*), le bureau de protection du secret prendra l'attache du service auteur. S'il s'agit d'un document classifié de l'OTAN et de l'UE, rapprochez-vous de votre bureau d'ordre correspondant.

Rappel Les documents classifiés après le 1er juillet 2021 comportent une échéance de classification. À compter de cette date, ces documents sont automatiquement déclassifiés.

À titre exceptionnel, certains documents classifiés après le 1er juillet 2021 peuvent ne pas comporter de date d'échéance de classification. Dans ce cas, ces documents comportent une date de réexamen de la pertinence de la classification. Si celle-ci est dépassée, rapprochez-vous de l'autorité émettrice afin de connaître la décision prise à cet égard.

▶ La réévaluation de la pertinence de la classification d'une information ou d'un support doit également être réalisée avant tout versement aux archives et lorsque vous quittez votre poste ou achevez votre mission.

Textes de référence

IGI 1300 Partie 7 « gestion des informations et supports classifiés tout au long de leur cycle de vie ».

FICHE N° 9

Reproduire une information ou un support classifié

La reproduction d'une information ou d'un support classifié est assortie de règles visant à en garantir la confidentialité et la traçabilité.

1 Copie dématérialisée (copie d'un fichier informatique classifié sur un ordinateur ou sur une clé USB)

▸ Copiez le fichier classifié sur un système d'information homologué au niveau approprié.

Bon à savoir Le niveau d'homologation du système d'information est généralement précisé sur l'étiquette apposée sur le matériel.

Rappel Les formalités pour copier un document *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*) sont assurées par votre bureau de protection du secret. Pour les documents classifiés de l'UE et de l'OTAN, rapprochez-vous du bureau d'ordre correspondant.

Attention Pour obtenir la copie d'un fichier *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*), vous devez obtenir au préalable l'autorisation de l'auteur du document.

Cas particulier Par principe, il est interdit de photographier des informations et supports classifiés. Lorsque cela est absolument nécessaire, vous devez obtenir l'accord de votre officier de sécurité et utiliser un matériel spécifiquement homologué à cet effet.

▸ Aucune actualisation de votre inventaire n'est à effectuer. La traçabilité de la copie est effectuée par le système d'information.

2 Copie physique (impression d'un fichier informatique ou photocopie d'un document papier)

▸ Reproduisez la totalité ou une partie du document en utilisant un matériel autorisé (photocopieuse, télécopieur, système d'information).

Bon à savoir Le niveau de classification maximal des documents autorisés à être reproduits est généralement précisé sur l'étiquette apposée sur le matériel.

Rappel Les formalités pour copier un document *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*) sont assurées par votre bureau de protection du secret. Pour les documents classifiés de l'UE et de l'OTAN, rapprochez-vous du bureau d'ordre correspondant.

Attention Pour obtenir la copie d'un fichier *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*), vous devez obtenir au préalable l'autorisation de l'auteur du document.

▶ Faites enregistrer le document copié auprès du service compétent.

Rappel Le service compétent varie en fonction du niveau de classification du document :

- → pour un document *Secret* (ou portant l'ancien timbre de classification *Confidentiel-Défense*) : le service compétent ou le bureau de protection du secret de votre organisme ;
- → pour un document *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*) : le bureau de protection du secret ;
- → pour un document UE ou OTAN : le bureau d'ordre correspondant.

Attention Dans certaines structures, le bureau d'ordre est également chargé de la gestion des informations et supports classifiés au niveau *Secret* (ou portant l'ancien timbre de classification *Confidentiel-Défense*).

▶ Mettez à jour votre inventaire si vous conservez le document copié (cf. fiche n° 7).

Rappel Pour les documents classifiés au niveau *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*), cet inventaire est établi en lien avec votre bureau de protection du secret. Pour les documents de l'UE et de l'OTAN, il est établi en lien avec le bureau d'ordre correspondant.

▶ Protégez la copie selon les mêmes modalités que sa version originale (cf. fiche n° 6).

Textes de référence

IGI 1300 Partie 7 « gestion des informations et supports classifiés » et annexes 39 « modèle de demande de reproduction d'un support classifié *Très Secret* » et 40 « modèle d'autorisation de reproduction d'un support classifié *Très Secret* ».

FICHE N° 10

Se déplacer avec des informations et supports classifiés

Dans certaines circonstances (réunion, déplacement professionnel, etc.), il peut être nécessaire de déplacer un support classifié en dehors de son lieu de détention habituel. Respectez les mesures suivantes afin d'en garantir la traçabilité et la confidentialité.

1 Sur le territoire national

- Lorsque vous transportez un document classifié au sein de votre site d'emploi, veillez à ce qu'il ne soit pas visible de personnes non autorisées.
- En dehors de votre site d'emploi, vous pouvez transporter personnellement le document en le plaçant dans une double enveloppe.

Bon à savoir Vous pouvez également le faire transporter par :

→ une personne habilitée au niveau approprié, qui peut être une personne du service de courrier interne à votre organisme ;

→ un convoyeur autorisé par votre organisme pour transporter des documents classifiés.

Attention Rapprochez-vous de votre bureau de protection du secret pour vous assurer des modalités de transport d'un document *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*). S'il s'agit d'un document « UE » ou « OTAN », rapprochez-vous du bureau d'ordre correspondant.

- Si vous souhaitez transporter un document classifié en vue de le transmettre à une personne habilitée et ayant le besoin d'en connaître : choisissez le mode de transport, faites établir le bordereau d'envoi ABB' par le service compétent (cf. fiche n° 11) et mettez à jour votre inventaire s'il s'agit d'un document que vous déteniez préalablement (cf. fiche n° 7).

Attention Pensez à respecter les règles habituelles de protection : enregistrement des copies de documents, vérification des habilitations et du besoin d'en connaître, etc. Ceci s'applique y compris pour la transmission d'un document classifié à l'intérieur du site d'emploi.

2 Vers ou depuis l'étranger

- Rapprochez-vous de votre officier de sécurité afin d'obtenir un certificat de courrier avant le déplacement à l'étranger.

Rappel Pour les informations échangées dans le cadre d'un accord ou d'un programme international référez-vous aux stipulations de l'accord ou de l'annexe de sécurité internationale applicable.

- Si vous souhaitez transporter un document classifié en vue de le transmettre à une personne habilitée et ayant le besoin d'en connaître : choisissez le mode de transport, faites établir les formalités d'envoi par le service compétent (cf. fiche n° 11) et mettez à jour votre inventaire s'il s'agit d'un document que vous déteniez préalablement (cf. fiche n° 7).

Textes de référence

IGI 1300 Partie 7 « gestion des informations des informations et supports classifiés tout au long de leur cycle de vie ».

FICHE N° 11

Transmettre une information ou un support classifié

La transmission d'informations ou supports classifiés est régie par des règles spécifiques visant à en garantir la confidentialité et la traçabilité.

1 Transmission orale (par audio/visioconférence)

- Assurez-vous que vos interlocuteurs sont habilités au niveau approprié et qu'ils ont le besoin d'en connaître.

Bon à savoir En cas de doute sur le niveau d'habilitation d'un interlocuteur, demandez-lui un certificat de sécurité.

- Utilisez un moyen de communication sécurisé (homologué ou agréé au niveau approprié, tel que le téléphone OSIRIS, etc.).

Rappel Si vous ne disposez pas d'un moyen de communication adapté, prenez l'attache de votre officier de sécurité des systèmes d'information.

2 Transmission dématérialisée (par messagerie sécurisée)

- Établissez la liste des destinataires en vous assurant qu'ils sont habilités au niveau approprié et qu'ils ont le besoin d'en connaître.

Bon à savoir En cas de doute sur le niveau d'habilitation d'un destinataire, demandez-lui un certificat de sécurité.

- Envoyez le document classifié depuis et vers un système d'information homologué au niveau approprié.

Bon à savoir Le niveau d'homologation du système d'information est généralement précisé sur une étiquette apposée sur le matériel.

Rappel L'envoi dématérialisé d'un document *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*) est assuré par votre bureau de protection du secret. Pour les documents classifiés de l'UE et de l'OTAN, rapprochez-vous de votre bureau d'ordre correspondant.

- Aucune actualisation de votre inventaire n'est à effectuer. La traçabilité de l'information est assurée par le système d'information.

3 Transmission physique (par vous-même, par courrier, par porteur ou par valise diplomatique)

- Établissez la liste des destinataires et assurez-vous qu'ils sont habilités au niveau approprié et qu'ils ont le besoin d'en connaître.

Bon à savoir En cas de doute sur le niveau d'habilitation d'un destinataire, demandez-lui un certificat de sécurité.

- Faites enregistrer le support envoyé auprès du bureau compétent.

Bon à savoir Le bureau compétent varie en fonction du niveau de classification du support :

→ pour un support *Secret* (ou portant l'ancien timbre de classification *Confidentiel-Défense*) : le service compétent ou le bureau de protection du secret de votre organisme ;

→ pour un support *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*) : le bureau de protection du secret (BPS) ;

→ pour un support UE ou OTAN : le bureau d'ordre correspondant.

Attention Dans certaines structures, le BPS est également chargé de la gestion des informations et supports classifiés au niveau *Secret* (portant l'ancien timbre de classification *Confidentiel-Défense*).

- Remettez le support à envoyer et la liste des destinataires au bureau compétent chargé d'effectuer les formalités d'envoi (renseignement du bordereau d'envoi et mise sous enveloppe).

Bon à savoir Le transport par voie postale est autorisé uniquement pour les supports classifiés au niveau *Secret* (ou portant l'ancien timbre de classification *Confidentiel-Défense*) envoyés sur le territoire national ou vers les pays de l'UE ou de l'OTAN. Ces documents doivent être placés sous double enveloppe.

En cas d'urgence, si les formalités d'envoi ne peuvent être réalisées par le bureau compétent, contactez l'officier de sécurité afin d'obtenir des renseignements sur les modalités d'envoi de votre support classifié.

Rappel Pour les informations échangées dans le cadre d'un accord ou d'un programme international référez-vous aux stipulations de l'accord ou de l'annexe de sécurité internationale applicable.

Attention Un document classifié peut être transporté à l'étranger par valise diplomatique, par porteur habilité ou convoyeur spécifiquement autorisé par votre organisme à transporter des documents classifiés.

- Informez le(s) destinataire(s) de l'envoi.
- Mettez à jour votre inventaire lorsque vous étiez préalablement détenteur du document ou du support transmis (cf. fiche n° 7).

Rappel Pour les documents classifiés au niveau *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*), cet inventaire est établi en lien avec votre bureau de la protection du secret.

Textes de référence

IGI 1300 Partie 7 « gestion des informations et supports classifiés tout au long de leur cycle de vie » et annexe 41 « modèle de bordereau de transmission de supports classifiés ».

FICHE N° 12

Recevoir une information ou un support classifié

La réception d'une information ou d'un support classifié est régie par des règles spécifiques visant à en garantir la confidentialité et la traçabilité.

1 Réception dématérialisée (par messagerie sécurisée)

- Réceptionnez l'information classifiée sur un système d'information homologué au niveau approprié.

Bon à savoir Le niveau d'homologation du système d'information est généralement précisé sur une étiquette apposée sur le matériel.

Attention La réception dématérialisée d'un document *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*) est assurée par votre bureau de protection du secret. Pour les documents classifiés de l'UE et de l'OTAN, rapprochez-vous du bureau d'ordre correspondant.

- Aucune actualisation de votre inventaire n'est à effectuer. La traçabilité de l'information est assurée par le système d'information.

Attention Si vous imprimez le document classifié, faites procéder à son enregistrement et mettez à jour votre inventaire.

2 Réception physique (par courrier, par un collègue ou par porteur)

- Lors de la réception, l'intégrité de l'emballage doit être vérifiée.

Rappel Les personnes chargées de la réception des documents varient en fonction du niveau de classification :

- → pour les documents *Secret* (ou portant l'ancien timbre de classification *Confidentiel-Défense*) : vous-même, le service compétent ou le bureau de protection du secret (BPS) de votre organisme ;
- → pour les documents *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*) : le bureau de protection du secret ;
- → pour les documents classifiés de l'UE et de l'OTAN : le bureau d'ordre compétent.

Attention Dans certaines structures, le BPS est également chargé de la gestion des informations et supports classifiés au niveau *Secret* (et de ceux portant l'ancien timbre de classification *Confidentiel-Défense*).

- Informez l'expéditeur de la réception du document en datant et signant le bordereau d'envoi.

Bon à savoir Pour les documents *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*), ces formalités sont réalisées par votre bureau de protection du secret et pour les documents classifiés de l'UE et de l'OTAN, par le bureau d'ordre compétent.

Rappel Il convient de renvoyer à l'expéditeur sans délai à titre d'accusé de réception le feuillet B du bordereau d'envoi et de conserver le feuillet A.

Attention Si le document a été envoyé depuis l'étranger, vous devrez signer le certificat de courrier.

- Faites enregistrer le document réceptionné auprès du service compétent (cf. point ci-dessus).
- Mettez à jour votre inventaire si vous conservez le document dans votre coffre-fort (cf. fiche n° 7).

Rappel Pour les documents classifiés au niveau *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*), cet inventaire est établi en lien avec votre bureau de la protection du secret.

Attention Comme pour le niveau *Très Secret*, les documents classifiés au niveau *Secret* (ou portant l'ancien timbre de classification *Confidentiel-Défense*) doivent faire l'objet d'un inventaire.

Textes de référence

IGI 1300 Partie 7 « gestion des informations et supports classifiés tout au long de leur cycle de vie ».

FICHE N° 13

Conserver, archiver ou détruire un support classifié

Dès que des informations et supports classifiés conservés dans un coffre-fort ou sur un système d'information classifié ne vous sont plus utiles pour votre travail quotidien, il convient, soit de les archiver, soit de les détruire.

1 Documents à conserver

▶ Conservez les informations et supports classifiés utiles à votre travail quotidien : les supports physiques (document, clé USB, CD-Rom, disque dur, etc.) dans un coffre-fort adapté ; les informations dématérialisées (courriel, fichier informatique, etc.) sur un système d'information homologué au niveau approprié.

Bon à savoir Le niveau d'homologation du système d'information est généralement précisé sur l'étiquette apposée sur le matériel.

Rappel Avant de quitter vos fonctions ou votre mission, effectuez systématiquement le tri des supports classifiés.

Attention La conservation des documents *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*) est effectuée dans une zone réservée.

2 Documents à archiver

▶ Pendant toute la durée de votre poste ou de votre mission, faites archiver les documents qui ne sont plus utiles pour votre travail quotidien mais qui conservent une utilité administrative ou un intérêt scientifique ou historique.

Bon à savoir Contactez la personne responsable des archives au sein de votre organisme pour procéder au versement.

Rappel Assurez-vous à cette occasion que la classification de l'information (niveau et durée de classification) reste toujours pertinente (cf. fiche n° 8).

Attention Prenez l'attache du bureau de protection du secret pour l'archivage des documents *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*) et du bureau d'ordre correspondant pour les documents UE et OTAN.

▶ Mettez à jour votre inventaire (cf. fiche n° 7).

Rappel Pour les documents classifiés au niveau *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*), cet inventaire est établi en lien avec votre bureau de la protection du secret. Pour les documents de l'UE et de l'OTAN, il est établi en lien avec le bureau d'ordre correspondant.

3 Documents à détruire

- Détruisez ou faites détruire les autres documents de façon à rendre impossible toute reconstitution, même partielle, des informations contenues sur les supports (brûlage, incinération, broyage, effacement sécurisé à l'aide d'une solution agréée pour les informations dématérialisées, etc.).

Bon à savoir Pour les documents et supports classifiés au niveau *Secret* (ou portant l'ancien timbre de classification *Confidentiel-Défense*) : détruisez le document ou le support ou faites-le détruire sous votre surveillance, avec un moyen adapté.
Au niveau *Très Secret* (ou portant l'ancien timbre de classification *Secret-Défense*), les moyens de destruction sont mis en œuvre par votre bureau de protection du secret.
Pour les supports émis par l'UE ou l'OTAN, rapprochez-vous du bureau d'ordre correspondant.

Rappel Pensez à détruire les copies inutiles.

- Établissez ou faites établir par le service compétent le procès-verbal de destruction (à conserver).
- Mettez à jour votre inventaire (cf. fiche n° 7).

Textes de référence

Code du patrimoine Articles L. 211-1, L. 212-2, L. 212-3, L. 213-1, L. 213-2, L. 213-3, L. 213-3-1, L. 213-4, L. 213-5, L. 213-6 et L. 213-7.

IGI 1300 Partie 7 « gestion des informations et supports classifiés tout au long de leur cycle de vie » et annexe 45 « modèle de procès-verbal de destruction de supports classifiés *Secret* ou *Très Secret* ».

FICHE N° 14 Utiliser un système d'information classifié

Un système d'information classifié permet d'élaborer, de conserver et d'envoyer des informations de façon protégée. Son utilisation est encadrée afin de garantir la disponibilité, l'intégrité, la confidentialité et la traçabilité des informations classifiées contenues.

1 Règles de sécurité pour l'utilisation

- Protégez les identifiants, mots de passe, cartes et matériels vous permettant d'accéder à votre poste de travail classifié et aux outils qui y sont associés.

Rappel Vous êtes responsable de la protection des informations d'authentification (exemple : identifiant, mot de passe, etc.). Ne les conservez pas de façon manuscrite sans en assurer la protection. Conservez vos cartes à puce dans un meuble fermé à clé.

- Élaborez, recevez, transmettez, copiez des informations classifiées sur du matériel informatique (poste de travail, clé USB, etc.) homologué au niveau approprié.

Bon à savoir Le niveau d'homologation du système d'information est généralement précisé sur l'étiquette apposée sur le matériel.

- Pensez à verrouiller votre poste informatique lorsque vous quittez votre bureau, même pour une courte pause.
- Ne connectez à votre poste de travail que les équipements autorisés (clé USB, imprimante, scanner).

Bon à savoir En cas de doute, interrogez votre officier de sécurité des systèmes d'information.
Attention La connexion d'équipements personnels à votre poste de travail est strictement interdite.

- Utilisez impérativement une station blanche pour vérifier l'innocuité d'un support (l'absence de virus) s'il a été, à titre dérogatoire, connecté à un équipement non autorisé.

Bon à savoir En cas de doute, prenez l'attache de votre officier de sécurité des systèmes d'information.

2 Règles de sécurité en cas de déplacement professionnel

- Le déplacement d'un matériel informatique classifié (clé USB, ordinateurs, etc.) en dehors de votre lieu de travail est autorisé uniquement dans le cadre professionnel. La décision d'homologation doit le prévoir et les mesures de sécurité préconisées doivent être respectées.

Bon à savoir Rapprochez-vous de votre officier de sécurité des systèmes d'information pour vous en assurer et connaître les modalités de protection du matériel tout au long du transport.

Rappel L'usage de matériel informatique personnel est strictement interdit pour transporter des informations classifiées.

- En déplacement ou lors d'une réunion, surveillez votre matériel informatique de façon permanente.
- Lors de l'utilisation de votre matériel classifié, assurez-vous qu'aucune personne non-qualifiée ne peut y accéder et prendre connaissance des informations qui y sont stockées.

Rappel Veillez à la confidentialité de votre travail lors de vos déplacements ou en réunion. N'oubliez pas vos impressions classifiées sur une imprimante ou un copieur. N'oubliez-pas vos clés USB sur vos postes. Etc.

- Ne traitez aucune information classifiée en télétravail.

Textes de référence

Code de la défense Articles R. 2311-6-1 à R. 2311-7-1.

IGI 1300 Partie 6 « sécurité des systèmes d'informations classifiés ».

FICHE N° 15

Organiser une réunion classifiée

Organiser une réunion au cours de laquelle des informations classifiées sont abordées suppose de mettre en œuvre des mesures de sécurité spécifiques.

1 Préparation de la réunion

- Établissez la liste des participants et transmettez-la à votre officier de sécurité.

Bon à savoir Vous devez préciser dans l'invitation le niveau d'habilitation requis pour participer à la réunion.

Rappel Demandez aux participants de vous transmettre un certificat de sécurité attestant de leur habilitation.

- Assurez-vous auprès de votre officier de sécurité et de votre officier de sécurité des systèmes d'information que la salle et les équipements qui seront utilisés (ordinateur, projecteur, etc.) présentent les garanties de sécurité suffisantes.

Rappel Si vous projetez de présenter des informations classifiées dématérialisées, utilisez des équipements informatiques (poste de travail, vidéoprojecteur, etc.) homologués au niveau approprié.

- Si un participant souhaite projeter des informations classifiées durant la réunion, demandez-lui de vous transmettre par voie électronique sécurisée le support de présentation en amont de la réunion.

Attention Les connexions entre vos équipements et ceux de vos partenaires (ordinateur portable et vidéoprojecteur, clé USB, etc.) sont, par principe, interdites.

- Si vous devez remettre des documents classifiés aux participants à l'occasion de la réunion, faites les copies (cf. fiche n° 9) et préparez les bordereaux d'envoi (cf. fiche n° 11).
- Assurez-vous de la prise en charge des participants dès leur arrivée dans vos locaux.

Bon à savoir Vérifiez que les personnes présentes figurent bien sur la liste des participants et qu'elles ont bien justifiées de leur habilitation.

Attention Les appareils de communication des participants (exemples : téléphone mobile, ordinateur portable, montre connectée, etc.) doivent, sauf autorisation, être laissés à l'extérieur de la salle.

2 Tenue de la réunion

- Au début de la réunion, rappelez le niveau maximal de classification des informations qui peut être abordé.
- Tout au long de la réunion, assurez-vous que le niveau de classification des informations évoquées ne dépasse pas le niveau fixé.

- Veillez à la sécurité des supports classifiés (poste informatique, clé USB, carnets de note par exemple) tout au long de la réunion.

Rappel Pendant les pauses, assurez-vous de la sécurité des supports classifiés laissés dans la salle. Veillez à ce que les participants ne discutent pas d'informations classifiées à l'extérieur de la salle.

- Si vous remettez des supports classifiés aux participants, faites signer le bordereau d'envoi aux participants.
- S'il s'agit d'une réunion classifiée à distance, utilisez le matériel homologué au niveau approprié (station HORUS, terminal OSIRIS, etc.).

Rappel L'organisateur de la réunion doit veiller au respect des conditions générales d'utilisation de l'équipement. En cas de doute, contactez votre officier de sécurité des systèmes d'information.

3 Suites de la réunion

- Conservez dans votre coffre-fort les supports élaborés ou échangés durant la réunion uniquement s'ils sont utiles à votre travail quotidien. Archivez ou détruisez les autres supports (cf. fiche n° 13).

Rappel Pensez à mettre à jour votre inventaire si vous conservez de nouveaux supports dans votre coffre-fort.

Important Toute information classifiée communiquée lors de la réunion et faisant l'objet d'une prise de notes entraîne la classification du support au même niveau de classification.

- Rédigez une note succincte, éventuellement classifiée, dans laquelle il est fait mention de la liste des participants, des domaines d'informations classifiées exposés ainsi que des mesures prises pour en assurer la protection.

4 Consignes en cas de participation à une réunion « classifiée »

- Si vous souhaitez projeter des informations classifiées durant la réunion, transmettez-les à l'organisateur par voie électronique sécurisée (par exemple ISIS) en amont de la réunion.

Bon à savoir L'organisateur se chargera des modalités de diffusion lors de la réunion.

- Ne communiquez que des informations qui sont classifiées au niveau prévu pour la réunion (et qui relèvent de l'ordre du jour de la réunion).
- Ne laissez à aucun moment votre poste informatique, vos notes sans surveillance.

Textes de référence

IGI 1300 Annexe 35 « guide des mesures de sécurité applicables au cours d'une réunion impliquant des informations et supports classifiés ».

FICHE N° 16

Protéger le secret de la défense nationale en toute circonstance

En toute circonstance, vous êtes responsable des supports classifiés que vous détenez et des informations classifiées dont vous avez eu à connaître.

1 Obligation de protéger le secret de la défense nationale, y compris après votre habilitation (cf. fiche n° 3)

- Durant toute la durée de votre habilitation, vous ne devez communiquer des informations ou des supports classifiés qu'à des personnes habilitées au niveau approprié et dont le besoin d'en connaître est avéré.
- Vos obligations perdurent après la fin de votre habilitation. Même lorsque vous n'êtes plus habilité, vous devez continuer à protéger les informations classifiées dont vous avez eu connaissance et ne devez, en aucun cas, les divulguer, y compris à des personnes habilitées et ayant le besoin d'en connaître ; vous n'êtes plus autorisé à en parler.
- Limitez les risques de compromission en agissant avec discernement, en respectant les règles et bonnes pratiques, en les rappelant si nécessaire dans votre entourage professionnel.

Bon à savoir Assurez-vous auprès de votre officier de sécurité et de votre officier de sécurité des systèmes d'information que vous disposez du matériel approprié à la gestion des informations et supports classifiés dont vous avez à connaître (coffre-fort, système d'information homologué, etc.).

Rappel Vous devez participer aux formations et actions de sensibilisation. Renseignez-vous auprès de votre hiérarchie ou de votre officier de sécurité.

2 Gestion des incidents de sécurité et éventuelles compromissions

- Signalez immédiatement toute suspicion ou tout acte de compromission à votre officier de sécurité et le cas échéant à votre officier de sécurité des systèmes d'information si la compromission concerne des informations classifiées dématérialisées ou un système d'information classifié, y compris lorsque cette compromission est de votre fait.

Rappel La compromission ou sa simple tentative est une infraction pénale punie jusqu'à 7 ans d'emprisonnement et 100 000 euros d'amende.

Elle consiste en la destruction, le détournement, la soustraction, la reproduction, l'accès ou la divulgation non autorisée d'une information ou d'un support classifié au regard des règles de la protection du secret de la défense nationale. Pour les personnes qualifiées (habilitées et ayant le besoin d'en connaître), le délit est caractérisé, que la compromission soit volontaire ou qu'elle résulte d'une imprudence ; pour les personnes non qualifiées, l'intention est nécessaire pour caractériser le délit.

Attention Signalez à votre officier de sécurité toute compromission qu'elle soit volontaire ou involontaire (imprudence, négligence, laissez faire). Si vous avez commis une compromission par négligence ou imprudence, informez sans attendre votre officier de sécurité, il saura comment traiter la situation pour en limiter au maximum les effets.

- Signalez également à votre officier de sécurité tout incident de sécurité.

Bon à savoir Un incident de sécurité est tout événement pouvant conduire directement ou indirectement à une compromission (exemples : perte d'une clé USB contenant des informations classifiées, attaque informatique sur son poste de travail hébergeant des informations classifiées, vol d'un sac contenant un document classifié, suspicion de tentative d'approche, etc.).

Rappel Informez simultanément votre officier de sécurité des systèmes d'information (cf. point 2) en cas d'incident de sécurité en lien avec le matériel informatique.

- Demandez conseil en cas de doute à votre officier de sécurité ou votre officier de sécurité des systèmes d'information.

3 Cas spécifiques

- Les personnels d'intervention (exemples : incendie, assistance à personne, intrusion) sont dispensés de formalités d'accès pour intervenir dans un lieu abritant des informations et supports classifiés.

Rappel Informez votre officier de sécurité et, dans la mesure du possible, restez présent lors de l'intervention.

- Conformez-vous aux instructions données par votre officier de sécurité en cas d'évacuation d'urgence de vos locaux (destruction ou conservation des informations classifiées, etc.)
- En cas de contrôle inopiné de l'inspection du travail, prévenez également votre officier de sécurité et alertez les inspecteurs de la présence d'informations classifiées.

Bon à savoir Les inspecteurs ne peuvent prendre connaissance d'informations et supports classifiés que s'ils sont habilités au niveau approprié et ont le besoin d'en connaître.

- En cas de perquisition, prévenez immédiatement votre officier de sécurité et alertez les enquêteurs de la présence d'informations classifiées.

Bon à savoir La perquisition dans un lieu abritant est régie par des règles spécifiques et ne peut intervenir qu'en présence du président de la commission du secret de la défense nationale ou de son représentant. Il est donc essentiel de préciser aux enquêteurs qu'ils se trouvent dans un tel lieu pour s'assurer du respect de ces règles.

- Si vous êtes interrogé par un magistrat ou un enquêteur, vous ne pouvez en aucun cas divulguer d'informations classifiées.

Important Dans la mesure du possible, informez votre autorité hiérarchique et prenez également l'attache de votre officier de sécurité pour connaître la conduite à tenir.

Textes de référence

Code pénal Articles 413-10 à 413-12.

IGI 1300 Parties 5 « sécurité des lieux », 6 « sécurité des systèmes d'information classifiés » et 7 « gestion des informations et supports classifiés tout au long de leur cycle de vie ».

FICHE N° 17

Les mots clés de la protection du secret de la défense nationale

La protection du secret de la défense nationale possède un vocabulaire propre défini par la réglementation. Il convient donc de se l'approprier.

Auteur / autorité émettrice

L'auteur d'une information ou d'un support classifié est l'autorité qui, conformément aux modalités de classification arrêtées par l'autorité émettrice, prend la décision d'apposer le timbre de classification sur une information ou un support au niveau requis par son contenu.

L'autorité émettrice est, quand-à-elle, l'autorité étatique nationale, étrangère ou supranationale sous la responsabilité de laquelle un timbre de classification est apposé sur une information ou un support. C'est elle qui prend la décision de classification.

Autorité d'habilitation

Autorité compétente pour diligenter une enquête administrative dans le cadre de l'habilitation au secret de la défense nationale et prendre la décision d'habilitation ou de refus d'habilitation.

Besoin d'en connaître

Nécessité impérieuse de prendre connaissance d'une information dans le cadre de l'exercice d'une fonction ou de l'accomplissement d'une mission.

Catalogue des emplois

Établi pour chaque niveau de classification, le catalogue des emplois permet d'identifier via l'octroi d'un numéro de poste, chaque fonction ou mission impliquant nécessairement l'accès à des informations et supports classifiés au niveau de classification considéré, ainsi que les nom et prénom des personnes physiques les occupant.

Certificat de sécurité

Document attestant de l'habilitation d'une personne à accéder à des informations et supports classifiés à un niveau donné.

Compromission

Destruction, détournement, soustraction, reproduction non autorisée ou divulgation d'une information ou d'un support classifié à une ou plusieurs personnes non qualifiées.

Habilitation au secret de la défense nationale

Procédure visant à s'assurer qu'une personne peut, sans risque pour la défense et la sécurité nationale ou pour sa propre sécurité, connaître des informations et supports classifiés dans l'exercice de ses fonctions. Au terme de cette procédure, l'autorité d'habilitation prend soit une décision d'habilitation pour un niveau de classification donné, soit une décision de refus d'habilitation.

Homologation d'un système d'information

Démarche visant à s'assurer, sur la base d'une analyse de risques globale, prenant en compte tous les éléments, y compris environnementaux, indispensables au fonctionnement et à la sécurité du système d'information considéré, que l'ensemble des risques a été identifié et fait l'objet d'un traitement approprié et que les risques résiduels sont acceptés. Cette démarche est sanctionnée par une décision d'homologation par laquelle l'autorité d'homologation atteste de la capacité du système d'information à traiter des informations classifiées pour un niveau de classification donné.

Déclassification / déclassement / reclassement

La déclassification est la suppression de la classification d'une information ou d'un support classifié.

Le déclassement est la modification, par abaissement, du niveau de classification d'une information ou d'un support classifié.

Le reclassement est la modification, par relèvement, du niveau de classification d'une information ou d'un support classifié.

Engagement de responsabilité

Document en deux volets signés par le titulaire de la décision d'habilitation par lequel il reconnaît avoir été informé que les manquements aux obligations liées à son habilitation sont susceptibles d'engager sa responsabilité pénale. Le premier volet est signé lors de la notification de la décision d'habilitation, le second lors de sa cessation de fonction ou, le cas échéant, en cas d'abrogation explicite de la décision d'habilitation, lors de la notification de la décision d'abrogation.

Enquête administrative

Procédure destinée à vérifier que le comportement des personnes physiques ou morales intéressées n'est pas incompatible avec l'exercice de la fonction ou l'accomplissement de la mission envisagée (Art. L. 114-1 du code de la sécurité intérieure).

Information ou support classifiés (ISC)

Information, document, support, matériel, procédé, réseau informatique, donnée informatisée ou fichier, quels qu'en soient la forme, la nature ou le mode de transmission, qu'ils soient élaborés ou en cours d'élaboration, auxquels un niveau de classification a été attribué et qui, dans l'intérêt de la défense nationale et conformément aux procédures, lois et règlements en vigueur, nécessitent une protection contre toute violation, toute destruction, tout détournement, toute divulgation, toute perte ou tout accès par toute personne non autorisée ou tout autre type de compromission. Pour avoir accès à ce type d'information, il faut être habilité au niveau requis et avoir le besoin d'en connaître.

Officier de sécurité (OS)

Personne chargée de mettre en œuvre, au sein d'un organisme ayant accès à des informations ou des supports classifiés, les mesures de protection du secret et de veiller à leur application.

Officier de sécurité des systèmes d'information (OSSI)

Personne chargée, au sein d'un organisme détenant au moins un système d'information traitant d'informations classifiées, de mettre en œuvre et de contrôler l'application de la réglementation en matière de protection du secret.

Personne qualifiée

Est qualifiée, au sens de l'article 413-10 du code pénal, la personne qui, par son état, sa profession, sa fonction ou sa mission, temporaire ou permanente, est habilitée à avoir accès à une information classifiée ou à détenir un support classifié et a le besoin d'en connaître.

Service enquêteur

Services du ministère de la défense ou du ministère de l'intérieur chargés des enquêtes administratives dans le cadre de l'habilitation ou d'évaluer l'aptitude physique des lieux abritant. Ces services rendent leurs conclusions sous forme d'avis.

Système d'information classifié

Système d'information homologué pour traiter, stocker ou transmettre des informations classifiées.

À PROPOS
DU SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE :

Service du Premier ministre travaillant en liaison étroite avec le Président de la République, le secrétariat général de la défense et de la sécurité nationale (SGDSN) assiste le chef du Gouvernement dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. À ce titre, il prépare notamment la réglementation interministérielle relative à la protection du secret de la défense nationale, en assure la diffusion et en suit l'application.

http://www.sgdsn.gouv.fr/missions/proteger-le-secret-de-la-defense-et-de-la-securite-nationale/

Version du 9 août 2021

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
sgdsn.gouv.fr

Maquette : Pôle Graphisme, Déplacement, Fabrication, Images – DSAF/DPSG – Octobre 2021.