



**MINISTÈRE
DE LA JUSTICE**

*Liberté
Égalité
Fraternité*

**Le garde des Sceaux
ministre de la Justice**

Paris, le **05 MARS 2026**

Le garde des Sceaux, ministre de la Justice

à

Monsieur le vice-président du Conseil d'Etat

Madame la secrétaire générale, haute fonctionnaire de défense et de sécurité

Monsieur l'inspecteur général, chef de l'inspection générale de la Justice

Monsieur le directeur général de l'administration pénitentiaire

Mesdames les directrices et Messieurs les directeurs d'administration centrale

Mesdames les cheffes et Messieurs les chefs de service du secrétariat général

N° NOR : JUST2605601C

Objet : circulaire relative à l'organisation ministérielle de la protection du secret de la défense nationale (PSDN)

Annexe : instruction ministérielle de la PSDN

Mots-clés : chaîne de protection du secret, officier central de sécurité, habilitation personne physique, habilitation personne morale, sécurité des lieux, sécurité et gestion des systèmes d'informations classifiés.

Publication : bulletin officiel du ministère de la Justice et intranet Justice

Dans un contexte de tensions et de menaces, où les informations deviennent un enjeu de sécurité pour la stabilité et la résilience de notre pays, la publication de l'instruction ministérielle relative à la protection du secret de la défense nationale (PSDN) est essentielle pour organiser et, in fine, garantir la sécurité des informations classifiées présentes au ministère de la Justice et donc sous ma responsabilité.

Pour la mise en œuvre de la politique relative à la PSDN au sein du ministère de la justice, il est désormais nécessaire d'unifier les méthodes et les pratiques autour d'une organisation partagée, afin d'assurer une meilleure protection des informations classifiées. L'instruction ministérielle de la protection du secret de la défense nationale vise à harmoniser et à consolider les pratiques de protection du secret.

En conséquence, vous devrez, dans votre champ de compétence, inscrire votre action en matière de protection du secret dans la politique et l'organisation portées par cette instruction ministérielle. Sous mon autorité, l'instruction ministérielle organise la protection du secret, répartit les rôles et les attributions au sein du ministère en administration centrale et dans les territoires. Elle décline les règles et les principes généraux selon les modalités et la réalité ministérielles.

Avec l'appui de vos officiers de sécurité, vous déploierez cette instruction jusqu'au sein des établissements de votre périmètre de responsabilité. Vous établirez un plan de déploiement de la

protection du secret, en précisant les responsabilités et les échéances à respecter. Vous présenterez ce plan au département de la haute fonctionnaire de défense et de sécurité, et lui transmettez régulièrement des points d'étape.

Cette démarche doit être menée avec rigueur et dans un esprit de coopération.

J'attache une importance toute particulière à ce que ces documents soient établis et adressés au département de la haute fonctionnaire de sécurité et de défense avant le 30 juin 2026.

Vous voudrez bien, en conséquence, veiller à l'application de cette instruction et rendre compte de toute difficulté dans sa mise en œuvre au département de la haute fonctionnaire de sécurité et de défense (hfds-habilitations@justice.gouv.fr) en charge de la coordination ministérielle de ce dossier.

Smant



Gérald DARMANIN



**MINISTÈRE
DE LA JUSTICE**

*Liberté
Égalité
Fraternité*

INSTRUCTION MINISTÉRIELLE

PROTECTION DU SECRET DE LA DEFENSE NATIONALE

Annexe de la circulaire NOR : JUST2605601C

HISTORIQUE DES MODIFICATIONS

Version	Date	Auteur(s) - Entité	Description
V1	19/12/2025	BPS/DHFDS/MINJUS	

VALIDATION DU DOCUMENT

Prénom NOM	Entité	Fonction	Date
Gérald DARMANIN	Ministère de la Justice	Garde des Sceaux, ministre de la Justice	

TABLE DES MATIERES

REFERENCES.....	5
LISTE DES ACRONYMES	7
PREAMBULE	8
CHAPITRE 1 - DISPOSITIONS GENERALES.....	9
1.1. PRINCIPES GENERAUX	9
1.1.1 <i>Le fondement du secret de la défense nationale</i>	9
1.1.2 <i>Les éléments constitutifs de la politique de sécurité de protection du secret</i>	10
1.1.2.1. Le marquage.....	10
1.1.2.2. L'accès des personnes physiques au secret : l'habilitation.....	10
1.1.2.3. La communication et la conservation des ISC	11
1.1.2.4. La compromission.....	11
1.2. LA GOUVERNANCE ET SES INSTRUMENTS	12
1.2.1. <i>Champs d'application</i>	12
1.2.2. <i>La chaîne de la protection du secret</i>	14
1.2.2.1 Les autorités interministérielles en charge de la protection du secret	14
1.2.2.2. Le ministre (cf. paragraphe 2.1.2.1 de l'IGI 1300).....	14
1.2.2.3. Le haut fonctionnaire de défense et de sécurité (HDFS).....	14
1.2.2.4. Le haut fonctionnaire de défense et de sécurité adjoint (HFDS-A)	15
1.2.2.5. Le fonctionnaire de sécurité de défense (FSD)	15
1.2.3. <i>La chaîne fonctionnelle de la protection du secret</i>	16
1.2.3.1. Organisation de la chaîne ministérielle de protection du secret	16
1.2.3.2. Les officiers de sécurité	16
1.2.3.3. Le détenteur d'ISC.....	19
1.2.3.4. L'officier de sécurité des systèmes d'information (OSSI)	19
1.2.4. <i>Les outils de suivi de l'activité de protection du secret</i>	19
1.2.4.1. Un cadre réglementaire	19
1.2.4.2. Des outils de traitement et de suivi des activités.....	20
1.2.4.3. Des outils de contrôle : inspections et contrôles	21
1.2.4.4. Le rapport annuel sur la politique de sécurité de protection du secret.....	21
1.2.4.5. La formation et la sensibilisation	21
CHAPITRE 2 – HABILITATION PERSONNE PHYSIQUE.....	22
2.1. PRINCIPES GENERAUX	22
2.2. LES PROCEDURES DE DROIT COMMUN ET D'URGENCE	22
2.2.1. <i>La procédure de droit commun</i>	22
2.2.2. <i>La procédure d'urgence</i>	23
2.3. LES PROCEDURES SPECIFIQUES	23
2.3.1. <i>La portabilité de l'avis de sécurité</i>	23
2.3.2. <i>Habilitation temporaire</i>	24
2.3.3. <i>Habilitation des ressortissants étrangers et des agents en postes à l'étranger</i>	24
2.4. LE CYCLE DE VIE D'UNE DECISION D'HABILITATION	24
2.4.1. <i>Le renouvellement d'une décision d'habilitation</i>	24
2.4.2. <i>L'abrogation d'une décision d'habilitation</i>	24
2.4.3. <i>Conservation et communication des dossiers d'habilitation</i>	24
CHAPITRE 3 – HABILITATION PERSONNE MORALE	25
3.1. LES DIFFERENTS TYPES DE MARCHES	25
3.2. L'HABILITATION DES PERSONNES MORALES	25
3.2.1. <i>La portabilité de l'avis de sécurité de l'habilitation personne morale</i>	25
3.2.2. <i>Le cas spécifique de l'habilitation d'une personne morale de droit étranger</i>	25
3.2.3. <i>Le plan contractuel de sécurité (PCS)</i>	25
CHAPITRE 4 – SECURITE DES LIEUX	26
4.1. PRINCIPES GENERAUX DE SECURITE.....	26
4.2. LES LIEUX ABRITANT	26

4.3. LA ZONE PROTEGEE (ZP).....	27
4.4. LA ZONE RESERVEE (ZR).....	27
CHAPITRE 5 – SECURITE DES SYSTEMES D’INFORMATION CLASSIFIES (SIC).....	28
5.1. GENERALITES.....	28
5.2. PROCESSUS D’INSTALLATION D’UN SYSTEME D’INFORMARTION CLASSIFIE (ISIS/OSIRIS/HORUS).....	28
5.3. UTILISATION DU POSTE	28
5.3.1. <i>Demande d’accès</i>	28
5.3.2. <i>Accès à l’intranet sécurisé ISIS</i>	28
5.4. REGLES DE SECURITE D’UTILISATION ET DE CONSERVATION	29
5.5. SUPPORTS EXTERNES	29
5.6. CONTROLE/INSPECTION	29
CHAPITRE 6 – GESTION DES INFORMATIONS ET SUPPORTS CLASSIFIES	30
6.1. DEBUT DE VIE DES INFORMATIONS ET SUPPORTS CLASSIFIES	30
6.1.1. <i>Autorité émettrice</i>	30
6.1.2. <i>Elaboration des informations et supports classifiés</i>	30
6.2. TRAITEMENT DES INFORMATIONS ET SUPPORTS CLASSIFIES	31
6.2.1. <i>Cas particulier de la gestion des ISC de niveau Très Secret</i>	31
6.2.2 <i>Conservation, traçabilité et reproduction</i>	31
6.2.3 <i>Transmission des informations et supports classifiés</i>	31
6.3. DESTRUCTION DES INFORMATIONS ET SUPPORTS CLASSIFIES	32
6.4. VERSEMENT DES INFORMATIONS ET SUPPORTS CLASSIFIES AUX ARCHIVES	32
6.4.1. <i>Communicabilité des informations et supports classifiés ayant fait l’objet d’une mesure de classification versés aux archives</i>	32
6.4.2 <i>Demande de consultation d’une information ou support classifié par une personne habilitée</i>	32
6.4.3 <i>Demande de consultation d’une information ou support classifié par une personne non habilitée</i>	33
6.5. DECLASSIFICATION DES INFORMATIONS ET SUPPORTS CLASSIFIES	33
6.5.1 <i>Déclassification automatique</i>	33
6.5.2 <i>Déclassification nécessitant une décision formelle matérialisée par un timbre de déclassification</i>	33
6.5.3 <i>Démarche de demande de déclassification auprès du service émetteur</i>	33
ANNEXE.....	34
Guide de classification.....	35

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD), notamment ses articles 2, 23, 24, 30 et 33 ;
- Code civil, notamment son article 22 ;
- Code de la commande publique, notamment ses articles L. 2141-1 et suivants, R. 2300-1, R. 2332-8, R. 2343-4, R. 2343-5, R. 2343-13, R. 2351-14, R. 2396-6 et R. 3123-3 ;
- Code du commerce, notamment son article L. 210-3 ;
- Code de la défense, notamment ses articles L. 1111-1, L. 1131-1 L. 1332-1 et suivants, L. 2311-1, L. 2312-1 à L. 2312-8, L. 2362-1, L. 4121-2, R. 1132-1 à R. 1132-3 ; R. 1143-1, R. 1143-2, R. 1143-5, R. 1143-6, R. 1143-8, R. 2311-1 à R. 2311-9-1, R. 2311-10 à R. 2311-11, D. 2311-12, R. 2312-1 et R. 2312-2 ;
- Code du patrimoine, notamment ses articles L. 211-1, L. 212-2, L. 212-3 et L. 213-1 à L. 213-7 ;
- Code pénal, notamment ses articles 411-6 à 411-8, 413-7, 413-9 à 413-12, 414-5 à 414-9, 434-4, R. 413-1 à R. 413-5 et 444-1 à 444-9 et 56-4 ;
- Code des postes et des communications électroniques, notamment ses articles L. 36-5, R. 12-1 et R. 1-2-6 ;
- Code des relations entre le public et l'administration, notamment ses articles L. 211-2 et L. 311-1 à 8 ;
- Code de la sécurité intérieure, notamment ses articles L. 114-1, L. 114-2 et L. 234-1 ;
- Code du travail, notamment ses articles L. 8112-1, L. 8113-10 à 11, L. 8114-1, L. 8114-2, L. 8123-1, L. 8123-4 et L. 812-35 ;
- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 6, 31, 115 et suivants ;
- Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles ;
- Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 85, 140 et suivants ;
- Arrêté du 9 août 2021 portant approbation de l'instruction générale n° 1300 sur la protection du secret de la défense nationale ;

- Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics ;
- Arrêté du 20 août 2024 relatif aux normes techniques de destruction des informations et supports classifiés ou protégés
- Instruction interministérielle n° 2100/SGDN/SSD du 1er décembre 1975 pour l'application en France du système de sécurité de l'organisation du traité de l'atlantique nord (II 2100) ;
- Instruction générale interministérielle n° 2102/SGDSN/PSE/PSD du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union européenne ;
- Instruction interministérielle n° 910/SGDSN/ANSSI du 22 octobre 2013 relative aux articles contrôlés de la sécurité des systèmes d'information ;
- Instruction générale interministérielle n° 6600 du 7 janvier 2014 relative à la sécurité des activités d'importance vitale (SAIV) ;
- Instruction interministérielle n°300/SGDSN/ANSSI du 23 juin 2014 sur la protection contre les signaux compromettants
- Instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015 sur la protection des systèmes d'information sensibles.

ACSSI	Articles contrôlés de la sécurité des systèmes d'information
AGS	Accords généraux de sécurité
ATAP	Avis technique d'aptitude physique
BPS	Bureau de protection du secret
CSDN	Commission du secret de la défense nationale
DHFDS	Département du haut fonctionnaire de défense et de sécurité
DPR	Délégation parlementaire au renseignement
DR	Diffusion restreinte
EAS	Enquête administrative de sécurité
FSD	Fonctionnaire de sécurité de défense
FSSI	Fonctionnaire de sécurité des systèmes d'information
HFDS	Haut fonctionnaire de défense et de sécurité
HFDS-A	Haut fonctionnaire de défense et de sécurité adjoint
HPM	Habilitation personne morale
HPP	Habilitation personne physique
IGI	Instruction générale interministérielle
II	Instruction interministérielle
IM	Instruction ministérielle
ISC	Information et support classifiés
ISR	Inspection des services de renseignement
NIS	Notice individuelle de sécurité
OCS	Officier central de sécurité
OLS	Officier local de sécurité
OSIIC	Opérateur des systèmes d'information interministériel classifié
OSSI	Officier de sécurité des systèmes d'information
PCS	Plan contractuel de sécurité
PPS	Politique de protection du secret
PSDN	Politique de sécurité de protection du secret
RGPD	Règlement général sur la protection des données
S	Secret
SGDSN	Secrétariat général de la défense et de la sécurité nationale
SIC	Systèmes d'information classifiés
TS	Très Secret
ZP	Zone protégée
ZR	Zone réservée

La présente instruction organise la politique du secret de la défense nationale (PSDN) au ministère de la Justice. Au nom du garde des Sceaux, ministre de la Justice, l'instruction décline les règles de la politique de sécurité de protection du secret, portée par l'instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 9 août 2021, ci-après dénommée « IGI 1300 », à la réalité et aux contraintes du ministère de la Justice.

Complémentaire à l'IGI 1300, à laquelle elle se réfère, elle en reconnaît les grands principes (cf. chapitre 1 de l'IGI 1300), sans qu'il soit nécessaire de les reprendre *in extenso*. Elle en reconnaît aussi l'objectif général de limitation du nombre d'habilitations, ainsi que des informations et supports classifiés (ISC), au strict nécessaire, afin de garantir la plus grande efficacité du dispositif.

La présente instruction adapte la politique de sécurité de protection du secret aux réalités ministérielles, reprend l'organisation en chapitres de l'IGI 1300, sans la copier. Elle offre un cadre dans lequel les différents acteurs impliqués dans la politique de protection du secret au sein du ministère pourront établir leur procédure, avec un objectif ministériel commun d'harmonisation des pratiques. Elle fixe les règles générales propres à la protection du secret, en précisant la chaîne des acteurs et leurs responsabilités.

L'instruction ne traite ni des procédures internes liées à la gestion des ISC ni de la gestion des informations protégées, dites diffusion restreinte (DR). Ces problématiques sont renvoyées à des documents spécifiques.

1.1. PRINCIPES GENERAUX

La présente instruction reconnaît et applique les principes édictés par l'instruction générale interministérielle (IGI) n° 1300/SGDSN/PSE/PSD du 9 août 2021.

1.1.1 Le fondement du secret de la défense nationale

L'article 413-9 du code pénal définit le secret de la défense nationale comme suit : « *Présentent un caractère de secret de la défense nationale au sens de la présente section les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès.*

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

Le secret de la défense nationale ne constitue pas uniquement un enjeu de défense militaire, il concerne également toutes les administrations responsables de ressources essentielles à la vie du pays. La défense nationale s'inscrit dans le cadre de la stratégie de sécurité nationale. Ce cadre transversal a pour objet « *d'identifier l'ensemble des menaces et des risques susceptibles d'affecter la vie de la Nation, notamment en ce qui concerne la protection de la population, l'intégrité du territoire et la permanence des institutions de la République, et de déterminer les réponses que les pouvoirs publics doivent y apporter*¹ ».

A l'exception des dossiers juridictionnels, soumis à une réglementation spécifique – le secret de l'instruction –, les informations relevant de la sécurité pénitentiaire, de la protection judiciaire de la jeunesse, des activités judiciaires et des services administratifs du ministère de la Justice peuvent être protégées par le secret de la défense nationale.

La décision de classer une information est une prérogative du pouvoir exécutif (articles 5, 20 et 21 de la Constitution).

Le secret de la défense nationale se caractérise par l'apposition d'un timbre de classification (Secret ou Très Secret). Dès lors, cette information ou ce support devient classifié et est soumis à des règles spécifiques encadrant sa création, sa gestion, sa conservation, son transport, sa destruction et son traitement. Cette protection implique la mise en place de mesures de sécurité pour les personnes susceptibles de détenir et de traiter cette information ou ce support, ainsi que des mesures de protection physique pour son stockage.

¹ Article L. 1111-1 du code de la défense.

1.1.2. Les éléments constitutifs de la politique de sécurité de protection du secret

1.1.2.1. Le marquage

Conformément à l'article 413-9 du code pénal, seuls les informations et supports ayant fait l'objet d'une mesure de classification en application des articles R. 2311-2 et R. 2311-3 du code de la défense présentent un caractère de secret de la défense nationale. L'apposition de ce timbre de classification définit le secret et lui confère la protection pénale.

Au sein du ministère de la Justice, il existe deux niveaux de classification : *Secret* (S) et *Très Secret* (TS). Néanmoins, certains cas spécifiques existent : sont soumis à une habilitation « classification spéciale », des membres de l'Inspection générale de la Justice, dans le cadre de l'inspection des services de renseignement (ISR), ainsi que des membres du cabinet du garde des Sceaux, dont le directeur de cabinet pour consulter les dossiers des conseils de défense restreints.

Le ministère de la Justice ne dispose pas des capacités pour créer ou conserver des informations et supports classifiés (ISC) de niveau supérieur (*Très Secret* « classifications spéciales »).

Les mentions particulières, diffusion restreinte, confidentiel personnel et autres marques de confidentialité ne constituent pas des niveaux de classification et ne bénéficient pas de la protection pénale prévue par la politique de sécurité de protection du secret.

La mention « Spécial France » n'est pas un timbre de classification. Lorsqu'elle est associée à une marque de classification, elle signale que l'information ou le support ne saurait être communiqué, en tout ou partie, à un État étranger ou à l'un de ses ressortissants, à une organisation internationale, une institution, un organisme ou un organe de l'Union européenne, ni à une personne morale de droit étranger. Seules des personnes physiques ou morales françaises considérées comme qualifiées au regard du code pénal peuvent y accéder.

1.1.2.2. L'accès des personnes physiques au secret : l'habilitation

L'accès par une personne physique aux ISC est limité. Conformément aux articles R. 2311-7 à R. 2311-7-1 du code de la défense, deux critères cumulatifs doivent être remplis :

- être habilité au niveau requis, c'est-à-dire au minimum au niveau de classification de l'information ou du support classifié. L'obtention de cette habilitation nécessite un processus spécifique. Toutefois, des personnes sont habilitées es-qualité par la loi ou par leur statut constitutionnel (cf. IGI 1300, paragraphe 3.1.4) ;
- le besoin d'en connaître : il est défini par la fonction occupée. Le poste ou la mission doit être préalablement inscrit dans un catalogue des emplois qui justifie le recours à une habilitation. Ce catalogue, validé par l'autorité d'emploi, est établi et actualisé par la chaîne de sécurité en charge de la protection du secret de la défense nationale.

Ces conditions d'accès s'appliquent également aux personnes morales (cf. IGI 1300, paragraphe 1.2.1.2).

Les cas particuliers

Cette instruction reconnaît les cas spécifiques énoncés par l'IGI 1300 (paragraphe 1.2.2.2), régissant l'accès au secret de la défense nationale.

Les parlementaires n'ont pas accès au secret dans le cadre de leur mission en tant que membres du Parlement (cf. IGI 1300, paragraphe 1.2.2.3), sauf les membres de la délégation parlementaire au renseignement (DPR). Le ministère de la Justice abrite un service de renseignement, le service national du renseignement pénitentiaire (SNRP), soumis à l'évaluation et au contrôle de la DPR. De même, l'inspection générale de la Justice (IGJ) est membre de l'inspection des services de renseignement (décret n° 2018-798 du 19 septembre 2018 ajoutant l'IGJ aux corps et services d'inspection et de contrôle concourant au fonctionnement de l'inspection des services de renseignement).

A l'exception des membres de la formation spécialisée du Conseil d'État chargée du contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et de l'exercice du droit d'accès aux fichiers intéressant la sûreté de l'État (cf. IGI 1300, paragraphe 2.1.3.3), les magistrats n'ont pas accès au secret de la défense nationale dans l'exercice de leurs prérogatives juridictionnelles (cf. IGI 1300, paragraphe 1.2.2.2), même s'ils disposent d'une habilitation. Ils doivent suivre une procédure spécifique de demande de déclassification des informations et supports classifiés.

1.1.2.3. La communication et la conservation des ISC

Conservation

Les ISC doivent être conservés dans un coffre ou une armoire forte qui répond à un cadre défini par l'IGI 1300 (cf. annexe 30). Les locaux où sont conservés des ISC sont nommés « lieux abritant ». Afin de renforcer la protection physique et périmétrique des lieux abritant, des zones protégées doivent être créées ainsi que des zones réservées pour le stockage des ISC de niveau *Très Secret*. L'accès à ces zones spécifiques est soumis à autorisation préalable.

Communication

Les ISC sont soumis à des règles de protection, dont les modalités de diffusion et de transport sont présentées au chapitre 6 de cette instruction.

L'accès au secret de la défense nationale est interdit aux personnes non-habilitées n'ayant pas besoin d'en connaître.

1.1.2.4. La compromission

Le non-respect des règles de la protection du secret de la défense nationale crée une situation de compromission, volontaire ou non.

Le délit de compromission est prévu aux articles 413-10 et suivants du code pénal. Il s'agit de la destruction, du détournement, de la soustraction ou de la reproduction non autorisée d'un ISC au regard des règles de l'IGI 1300 et de la présente instruction ministérielle (IM). Il est aussi caractérisé par la divulgation volontaire ou non d'informations couvertes par le secret. Ce délit concerne également l'accès et la connaissance d'ISC à un tiers non habilité.

Ainsi, tout détenteur d'ISC est responsable de leur protection. Cette responsabilité exige une vigilance particulière, dont le défaut peut être sanctionné. Le détenteur peut être poursuivi même en cas d'imprudence ou de négligence.

La compromission ou sa simple tentative est punie jusqu'à sept ans d'emprisonnement et 100 000 euros d'amende pour un agent habilité. La nature particulière du secret de la défense nationale et son rôle essentiel dans la protection des intérêts fondamentaux de la Nation expliquent la sévérité des sanctions.

1.2. LA GOUVERNANCE ET SES INSTRUMENTS

1.2.1. Champs d'application

La présente instruction s'adresse à toute personne détenant ou manipulant des informations et supports classifiés (ISC) au sein du périmètre de responsabilité du garde des Sceaux, ministre de la Justice, y compris les organismes qui lui sont liés par contrat ou convention.

Sont concernés, les structures, directions et services réputés abriter ou manipuler des ISC, à savoir :

- le cabinet du garde des Sceaux. Les mesures de protection visant les ISC sont assurées par l'officier central de sécurité (OCS) du périmètre et son équipe au sein du bureau du cabinet (BDC) ;
- l'administration centrale, comprenant le secrétariat général et plusieurs de ses composantes – la direction du numérique (DNum), l'agence nationale des techniques d'enquêtes numériques et judiciaires (ANTENJ), le service du pilotage et du soutien de proximité (SPSP), le département du haut fonctionnaire de défense et sécurité (DHFDS) – ainsi que les cinq directions du ministère – la direction générale de l'administration pénitentiaire (DGAP), direction des services judiciaires (DSJ), la direction des affaires civiles et du sceau (DACS), la direction des affaires criminelles et des grâces (DACG), la direction de la protection judiciaire de la jeunesse (DPJJ).

L'instruction s'adresse également au service national du renseignement pénitentiaire (SNRP) et à l'inspection générale de la Justice (IGJ), membre de l'inspection des services de renseignement.

Elle est aussi applicable :

- au réseau judiciaire et des ressorts des tribunaux, comprenant les cours d'appel, y compris celles des zones de défense, et les tribunaux judiciaires², les parquets spécialisés et la Cour de cassation. Ce réseau est coordonné et organisé par l'officier central de sécurité de la direction des services judiciaires ;
- au réseau pénitentiaire avec ses directions interrégionales des services pénitentiaires (DISP), ses établissements pénitentiaires et ses services pénitentiaires d'insertion et de

² Les cours d'appel sont au nombre de trente-six, y compris les onze cours d'appel de zones de défense, et les tribunaux judiciaires au nombre de cent soixante-quatre.

probation (SPIP)³. Ce réseau est organisé par l'officier central de sécurité de la direction générale de l'administration pénitentiaire ;

- au réseau des directions interrégionales de la protection judiciaire de la jeunesse (DRPJJ)⁴. Ce réseau est organisé par l'officier central de sécurité de la direction de la protection judiciaire de la jeunesse ;
- au réseau des cellules interrégionales du renseignement pénitentiaire (CIRP)⁵, dépendant du service national du renseignement pénitentiaire (SNRP). Ce réseau est organisé par l'officier central de sécurité du service national du renseignement pénitentiaire ;
- au réseau du secrétariat général du ministère de la Justice avec ses délégations interrégionales (DIR-SG⁶). Ce réseau est organisé par l'officier central de sécurité du périmètre du secrétariat général.

L'instruction s'applique également aux établissements de formation :

- l'École nationale des greffes (ENG) relevant de la direction des services judiciaires ;
- l'École nationale de l'administration pénitentiaire (ENAP) relevant de la direction générale de l'administration pénitentiaire ;
- l'École nationale de protection judiciaire de la jeunesse (ENPJJ) relevant de la direction de la protection judiciaire de la jeunesse.

L'École nationale de la magistrature (ENM), autonome dans son action et par son statut, applique la présente instruction. Elle s'appuie, pour ses besoins et pour la mise en œuvre des dispositions relatives à la politique de protection du secret de la défense nationale, sur l'officier central de sécurité de la direction des services judiciaires.

Plusieurs établissements publics à caractère administratif s'inscrivent dans ce périmètre ministériel et sont concernés par la présente instruction : l'agence de gestion et de recouvrement des avoirs saisis et confisqués (AGRASC) et l'agence publique pour l'immobilier de la justice (APIJ).

La délégation interministérielle de l'aide aux victimes (DIAV) hébergée dans le périmètre ministériel suit également les règles de cette présente instruction.

La présente instruction s'applique également aux personnes morales de droit public ou privé ayant conclues une convention, un contrat impliquant l'accès à des ISC. Les besoins et les relations sont assurés par la chaîne de protection du secret de la direction ou du service avec lequel les organismes ont contracté.

Cas spécifique : le Conseil d'État est autonome dans l'élaboration de sa politique de protection du secret de la défense nationale. Sont incluses dans son périmètre, les juridictions de l'ordre administratif : les tribunaux administratifs, les cours administratives d'appel, la Cour nationale du droit d'asile et le tribunal du stationnement payant.

Le ministère de la Justice lui apporte un soutien dans ses missions de protection du secret de la défense nationale conformément à l'IGI 1300. A ce titre, le ministère de la Justice, au travers

3 Il existe dix directions interrégionales des services pénitentiaires, cent quatre-vingt-sept établissements pénitentiaires et cent trois services pénitentiaires d'insertion et de probation.

4 Il existe neuf directions interrégionales de la protection judiciaire de la jeunesse.

5 Les cellules interrégionales du renseignement pénitentiaire sont au nombre de dix.

6 Les délégations interrégionales sont au nombre de neuf.

du haut fonctionnaire de défense et de sécurité ou de ses représentants, délivre aux agents qui assistent les membres de la formation spécialisée du Conseil d'Etat, les habilitations nécessaires à l'accomplissement de leurs missions. Sur demande du Conseil d'Etat, le ministère peut également assurer des missions supplémentaires.

1.2.2. La chaîne de la protection du secret

1.2.2.1 Les autorités interministérielles en charge de la protection du secret

Conformément à l'IGI 1300 (cf. paragraphe 2.1.1), la protection du secret de la défense nationale est de la responsabilité du Premier ministre. Sous son autorité, le secrétaire général de la défense et de la sécurité nationale (SGDSN) est chargé de définir et de coordonner la politique en matière de protection du secret de la défense nationale.

Le SGDSN veille à la mise en œuvre des mesures relatives aux classifications spéciales.

En tant qu'autorité nationale de sécurité pour le secret de la défense nationale⁷, le SGDSN est l'interlocuteur des autorités nationales de sécurité étrangères, notamment pour l'habilitation des personnes morales et physiques, qu'elles soient étrangères en France ou françaises à l'étranger. Ses autres attributions, sur le plan international, sont précisées dans l'IGI 1300 (cf. paragraphe 2.1.1.2).

1.2.2.2. Le ministre (cf. paragraphe 2.1.2.1 de l'IGI 1300)

En vertu de l'article R. 2311-6 du code de la défense, le garde des Sceaux, ministre de la Justice, est responsable de la protection du secret de la défense nationale dans son champ d'attribution, y compris pour les informations et supports classifiés (ISC) étrangers qui lui sont confiés en vertu d'un accord général de sécurité (AGS) ou d'un accord spécifique de sécurité.

A ce titre, dans son champ d'attribution ministériel, il est l'autorité émettrice⁸ du secret de la défense nationale⁹, et l'autorité d'habilitation¹⁰ pour les niveaux *Secret* et *Très Secret* (hors classifications spéciales).

Pour l'exercice de cette responsabilité, le garde des Sceaux est assisté d'un haut fonctionnaire de défense et de sécurité (HFDS). Il lui délègue sa signature pour tous les actes et décisions administratifs relatifs à la politique de sécurité de protection du secret.

1.2.2.3. Le haut fonctionnaire de défense et de sécurité (HFDS)

Le HFDS supervise, anime et coordonne la politique de défense et de sécurité au nom du ministre. Par délégation du ministre, le HFDS prend les décisions d'habilitation pour les niveaux *Secret* et *Très Secret*, hors classifications spéciales. Il tient à jour le registre des personnes

⁷ Cf. article R. 2311-10-1 du code de la défense.

⁸ Autorité étatique 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.

⁹ Cf. IGI 1300, paragraphe 1.4.1.

¹⁰ Autorité compétente pour diligenter une enquête administrative dans le cadre de l'habilitation au secret de la défense nationale et pour prendre la décision d'habilitation ou de refus d'habilitation.

physiques ou morales habilitées ou en cours d'habilitation et définit toutes mesures de protection physique ou numérique nécessaires à la protection du secret.

Il dispose, pour l'exercice des missions relatives à la politique de sécurité de protection du secret, d'un service spécialisé, le département du haut fonctionnaire de défense et de sécurité (DHFDS), dirigé par le haut fonctionnaire de défense et de sécurité adjoint (HFDS-A), département au sein duquel se trouvent un fonctionnaire de sécurité de défense (FSD) et un fonctionnaire de sécurité des systèmes d'information (FSSI).

1.2.2.4. Le haut fonctionnaire de défense et de sécurité adjoint (HFDS-A)

Le haut fonctionnaire de défense et de sécurité adjoint (HFDS-A), en tant que responsable du département du haut fonctionnaire de défense (DHFDS), supervise la politique ministérielle du secret de la défense nationale. Par délégation du HFDS, il peut signer toute décision relevant du champ de cette politique, au titre d'autorité d'habilitation et d'autorité émettrice d'informations et supports classifiés (ISC).

Pour l'accompagner ou le remplacer dans l'élaboration et le déploiement de la politique de protection du secret, il s'appuie sur un fonctionnaire de sécurité de défense (FSD).

1.2.2.5. Le fonctionnaire de sécurité de défense (FSD)

Désigné par arrêté du HFDS, le FSD assure des fonctions de conseil, d'élaboration et de pilotage de la politique ministérielle de protection du secret de la défense nationale.

Dans ses fonctions de conseil, il propose des pistes d'amélioration et de renforcement des mesures de protection, conseille les autorités ministérielles et la chaîne fonctionnelle de la protection du secret sur les différentes activités liées à la politique de sécurité de protection du secret. Il élabore et structure la politique ministérielle de protection du secret.

Au niveau de l'administration centrale, il s'appuie sur un réseau d'officiers centraux de sécurité (OCS).

Par délégation et pour le compte du HFDS, il est autorisé d'habilitation, signe les arrêtés de création de zones protégées, et supervise la liste des lieux abritant des ISC. Il prend, au profit du HFDS, toute mesure et décision relative à la politique de sécurité de protection du secret de la défense nationale. Il diligente des contrôles et supervise, pour le compte du HFDS, la gestion des cas de compromissions.

Il représente le ministre de la Justice auprès des autorités au niveau interministériel, des services enquêteurs et des autres ministères pour les questions relatives à cette politique.

Il rend compte de son action auprès du HFDS, garant de la politique ministérielle de la protection du secret, et du HFDS-A dont il dépend.

Il peut être assisté d'un adjoint auquel il délègue une partie de ses attributions.

En collaboration avec le FSSI, et sous l'autorité du HFDS-A, il supervise les missions confiées à l'officier de sécurité des systèmes d'information (OSSI) du ministère sur les moyens de

communication classifiés et plus largement sécurisés de l'État. Ces missions concernent notamment leur déploiement, leur gestion et leur contrôle.

1.2.3. La chaîne fonctionnelle de la protection du secret

La chaîne de protection du secret ministérielle est constituée d'un réseau en administration centrale, rassemblé autour du FSD. Elle est constituée d'un réseau d'officiers de sécurité représentant le périmètre des directions et des services centraux. Ces officiers de sécurité sont nommés officiers centraux de sécurité (OCS).

A ce réseau central sont articulés des réseaux au sein du territoire. L'organisation de ces réseaux est une prérogative de l'OCS des directions, services et entités, disposant d'implantations dans les territoires. Les officiers de sécurité qui composent ces réseaux au sein des territoires, sont nommés officiers locaux de sécurité (OLS).

1.2.3.1. Organisation de la chaîne ministérielle de protection du secret

La chaîne fonctionnelle de protection du secret¹¹ est structurée de façon à :

- identifier et tracer les ISC ;
- veiller à la mise en œuvre des mesures de prévention et de protection y compris pour les systèmes d'information classifiés ;
- assurer la gestion des ISC tout au long de leur cycle de vie et conformément à la réglementation ;
- être en capacité de détecter et de répondre dans les meilleurs délais à toute compromission.

La chaîne de protection du secret en administration centrale : pilotée par le FSD, elle comprend les OCS des différentes directions, services et entités présents en administration centrale. Ce réseau impulse la politique de protection du secret et en harmonise les pratiques.

La chaîne de protection du secret au sein des entités, services et directions : pour la diffusion et le respect des règles de protection du secret, chaque OCS pilote un réseau sur son périmètre. Il le structure selon ses besoins, les modes d'organisation propres à l'entité, à la direction ou au service qui l'emploie, et dans le respect des règles de la présente instruction.

Ainsi, plusieurs réseaux sont articulés autour de la chaîne d'administration centrale : ils permettent de déployer la politique du secret de la défense nationale dans les territoires.

1.2.3.2. Les officiers de sécurité

La chaîne ministérielle de protection du secret est composée d'officiers centraux de sécurité (OCS), d'officiers locaux de sécurité (OLS) et de correspondants de sécurité. Pour composer leur réseau, les OCS s'appuient sur des OLS et des correspondants. Sur proposition de l'OCS, ils sont officiellement désignés par leur hiérarchie d'emploi. Ces appellations recouvrent des missions et des responsabilités différentes.

¹¹ Cf. IGI 1300 paragraphe 2.2.2.

L'officier central de sécurité (OCS)

Par souci de simplification et de lisibilité de la présente instruction, le terme OCS désigne l'officier de sécurité en administration centrale, qu'il pilote ou non un réseau d'OLS ou de correspondants sur son périmètre de responsabilité. Il est chargé d'appliquer les règles de protection du secret. Il est membre du réseau des officiers de sécurité piloté et animé par le FSD.

L'officier central de sécurité peut également disposer d'un adjoint.

L'OCS, qui relève directement du chef de service ou du directeur, est désigné par ce dernier. Il doit :

- appartenir de façon stable à l'organisme ;
- être habilité à un niveau requis ;
- être formé à la protection du secret ;
- détenir des moyens nécessaires pour accomplir ses missions.

Sa désignation est formalisée par une décision adressée au HFDS ou ses représentants. Il déploie, sur son périmètre de responsabilité, la présente instruction qu'il décline.

Au sein de son périmètre, l'OCS¹² est investi de diverses missions :

- la déclinaison et l'application de la politique de protection du secret et son contrôle¹³ ;
- la préparation et la vérification des dossiers de demandes d'habilitation des agents de son périmètre en référence au catalogue des emplois de l'organisme. Il notifie les décisions aux candidats. Il est informé des difficultés liées à l'habilitation des candidats et assure les entretiens avec les intéressés, seul ou avec le HFDS ou ses représentants selon les cas ;
- l'élaboration d'une doctrine de sécurité relative aux zones protégées ;
- la sensibilisation aux règles de la politique de protection du secret ;
- la définition, en lien avec l'officier de sécurité des systèmes d'information (OSSI), des besoins en matière de systèmes d'information et de communication classifiés ;
- la déclinaison des règles en matière d'élaboration, de traitement, de marquage, de conservation et de destruction de ces ISC ;
- l'élaboration et l'actualisation :
 - o du ou des catalogues des emplois. Présentés annuellement par l'officiel central de sécurité, ils sont visés par le HFDS ou ses représentants ;
 - o de l'inventaire annuel des informations et supports classifiés. Une copie est annuellement remise au HFDS ou ses représentants ;
 - o de la liste des lieux abritant des ISC qu'il transmet au HFDS ou ses représentants, à sa demande.

Il constitue, en relation avec l'organisme contractant, le dossier d'habilitation personne morale (HPM), en lien avec le HFDS ou ses représentants.

Il effectue des contrôles et inspections sur son périmètre de responsabilité. Il rend compte au HFDS ou ses représentants, des difficultés rencontrées dans :

¹² Les missions de l'officier de sécurité : IGI 1300, paragraphe 2.2.2.1.

¹³ Les prescriptions d'élaboration de la politique de protection du secret d'un organisme : IGI 1300, paragraphe 2.3.1.3.

- la gestion des informations et supports classifiés ;
- la sécurité des systèmes d'information classifiés ;
- l'aptitude physique des lieux abritant des éléments couverts par le secret de la défense nationale.

Il rend compte au HFDS ou ses représentants, des compromissions au secret de la défense nationale.

Lorsqu'il constate des défauts dans la protection des ISC, il propose des mesures correctives au HFDS ou ses représentants.

Il rédige un guide de classification qu'il diffuse dans son périmètre de responsabilité et l'ajuste selon les besoins. Il le transmet au HFDS ou ses représentants. Ce document est agrégé à l'ensemble des guides de classification des OCS du ministère pour constituer le guide de classification ministériel.

Pour l'accomplissement de ses missions, l'officier central de sécurité peut s'appuyer sur un réseau, dont l'ampleur dépend de l'organisme qui l'emploie. Ce réseau relève de sa responsabilité pour sa construction et son pilotage. Il rend compte de cette organisation au HFDS ou ses représentants.

Officier local de sécurité (OLS)

L'officier central de sécurité (OCS) décline la chaîne de protection du secret et, selon ses besoins, peut s'entourer d'officiers locaux de sécurité (OLS) ou de correspondants. Ils sont désignés par le responsable du service, de la direction ou de l'établissement et sont placés sous la supervision de l'OCS. L'officier local de sécurité doit être habilité au niveau requis.

L'OLS assure des missions que l'officier central de sécurité ne peut exercer en raison de l'éloignement ou de la charge de travail. Cela inclut l'élaboration et l'actualisation du catalogue des emplois, le contrôle des informations et supports classifiés, les mises en éveil, le suivi des demandes d'habilitation, les inventaires, les contrôles et les inspections sur son périmètre de responsabilité. Il appartient à la chaîne de protection du secret pilotée par l'OCS. Cette chaîne s'articule au réseau des OCS piloté par le fonctionnaire de sécurité de défense.

Correspondant de sécurité

Le correspondant de sécurité n'aborde que certaines activités de la politique de sécurité de protection du secret. Il traite les demandes d'habilitation des agents de la structure qui l'héberge. Le cas échéant, il peut être chargé, par l'officier central ou local de sécurité de compléter et d'actualiser la liste des lieux abritant des informations et supports classifiés. Il ne peut effectuer de mises en éveil, de contrôles ou d'inspections.

Le correspondant de sécurité n'est pas nécessairement habilité, une enquête administrative de sécurité (EAS) est suffisante.

1.2.3.3. Le détenteur d'ISC

Le détenteur, personne habilitée et clairement identifiée par son officier de sécurité, assume la responsabilité des ISC qu'il détient. A son niveau, il assure un inventaire des ISC reçus ou créés et en informe l'officier de sécurité de son organisme.

1.2.3.4. L'officier de sécurité des systèmes d'information (OSSI)

L'IGI 1300 (cf. paragraphe 2.2.3) mentionne la mise en place d'une chaîne fonctionnelle de la sécurité des systèmes d'information. Au ministère de la Justice, la surveillance et la sécurité des systèmes d'information classifiés sont, au moins en partie, découplées de la chaîne fonctionnelle de la sécurité des systèmes d'information. Le ministère dispose d'une chaîne spécifique pour assurer la surveillance et la sécurité des systèmes d'information classifiés, dont l'animation repose sur un officier de sécurité des systèmes d'information (OSSI).

Responsable de la sécurité des systèmes d'information classifiés, l'officier de sécurité des systèmes d'information :

- veille à la sécurité et au suivi des articles contrôlés de la sécurité des systèmes d'information (ACSSI) ;
- contribue au déploiement des moyens concourant à la sécurité des réseaux classifiés.

Placé auprès du fonctionnaire de sécurité de défense (FSD), il est rattaché au bureau de la protection du secret du département du haut fonctionnaire de défense et de sécurité. Le cas échéant, et à la demande du fonctionnaire de sécurité des systèmes d'information (FSSI), il peut participer à la comitologie de la sécurité des systèmes d'information du ministère. L'OSSI rend compte au fonctionnaire de sécurité de défense du suivi des articles contrôlés de la sécurité des systèmes d'information et participe aux homologations des systèmes d'information classifiés que le ministère développe. Pour assurer sa mission, il s'appuie sur un réseau dédié, composé des responsables techniques en charge du déploiement et du suivi des systèmes d'information classifiés, généralement les responsables de la sécurité des systèmes d'information, et à défaut les officiers centraux de sécurité du ministère. A ce titre, il est membres du réseau des officiers centraux de sécurité d'administration centrale.

1.2.4. Les outils de suivi de l'activité de protection du secret

Pour assurer le pilotage et le suivi de la politique de protection du secret au ministère, le HFDS ou ses représentants mettent à disposition des outils (cf. paragraphe 2.3.2 de l'IGI 1300).

1.2.4.1. Un cadre réglementaire

Le cadre réglementaire comprend un cahier de procédures et de dispositions particulières (directive sur les enquêtes administratives ; doctrine sur les informations sensibles - diffusion restreinte) ainsi que la présente instruction, qui décline l'IGI 1300 au ministère de la Justice et qui sera révisée en tant que de besoin en fonction des évolutions.

L'instruction ministérielle est déclinée par chaque officier central de sécurité, en tenant compte des contraintes et des spécificités de son périmètre de responsabilité. Cette déclinaison, dénommée politique de protection du secret (PPS), précise :

- la chaîne de protection du secret qu'il a mis en œuvre et qu'il pilote ;
- les mesures de protection et de gestion des ISC ;
- les mesures de sécurité relatives aux zones protégées ;
- les informations à classifier quel qu'en soit le support. Elles sont intégrées au guide de classification ministériel ;
- les mesures en matière de contrôle, d'actualisation des inventaires des ISC, des lieux abritant ;
- les circuits de remontée d'information en cas de compromission.

1.2.4.2. Des outils de traitement et de suivi des activités

Il s'agit :

- **du registre des habilitations** : au sein du DHFDS, la structure en charge du traitement des habilitations pour l'ensemble du périmètre ministériel, le bureau de la protection du secret, dispose d'un outil de suivi. Cependant, chaque officier central de sécurité doit également avoir son propre registre pour les demandes relevant de son périmètre¹⁴ ;
- **de la base de données des lieux abritant** : le département du haut fonctionnaire de défense et de sécurité dispose de l'accès et de certains droits à la base de données des lieux abritant gérée par le secrétariat général de la défense et de la sécurité nationale. Le département l'actualise annuellement ou selon les directives du secrétaire général de la défense et de la sécurité nationale. Dans ce cadre, les officiers centraux de sécurité sont chargés de transmettre au fonctionnaire de sécurité de défense ou à ses représentants la liste actualisée des lieux abritant relevant de leur périmètre de responsabilité. Il leur est conseillé d'en conserver une copie.

Cette base de données constitue une cartographie des lieux où sont entreposés les informations et supports classifiés relevant de la responsabilité des officiers centraux. Elle est consultée par les magistrats de la direction des affaires criminelles et des grâces (DACG) en cas de perquisition.
- **du catalogue des emplois** : le HFDS ou ses représentants conserve l'ensemble des catalogues des emplois du périmètre ministériel. Chaque officier central de sécurité doit leur fournir annuellement un catalogue actualisé, constitué notamment des différents catalogues de son réseau territorial. Ce catalogue actualisé est soumis à la validation du HFDS ou ses représentants. Est vérifiée la cohérence des ajouts et du niveau d'habilitation demandé. L'objectif est de rationaliser les catalogues des emplois et de définir le besoin réel d'habilitation qui permet de justifier les demandes d'habilitation ;
- **des inventaires des informations et supports classifiés** : chaque OCS transmet au HFDS ou ses représentants la liste actualisée des ISC selon un calendrier annuel, et au minimum lors du changement de détenteur.

¹⁴ La gestion de cette base de données doit être conforme aux règles du RGPD en vigueur au ministère de la Justice.

1.2.4.3. Des outils de contrôle : inspections et contrôles

Le HFDS ou ses représentants organisent des contrôles et inspections sur le périmètre ministériel en informant et en associant l'OCS concerné. Le cas échéant, le HFDS ou ses représentants peuvent mobiliser l'Inspection générale de la justice.

Les OCS doivent également organiser des contrôles sur leur périmètre. Ces contrôles visent à vérifier les différentes activités et obligations imposées par la présente instruction. A l'issue de ces contrôles, un rapport est adressé au responsable de l'organisme contrôlé, avec une copie au HFDS ou ses représentants. Ces contrôles ont également une vocation pédagogique.

Le secrétariat général de la défense et de la sécurité nationale peut réaliser un contrôle ou une inspection en liaison avec le HFDS ou ses représentants.

1.2.4.4. Le rapport annuel sur la politique de sécurité de protection du secret

Rédigé par le haut fonctionnaire de défense et de sécurité ou ses représentants, classifié au niveau Secret-Spécial France et transmis au secrétaire général de la défense et de la sécurité nationale, le rapport annuel présente l'organisation de la politique de sécurité de protection du secret sur le périmètre du ministère. Il s'agit d'une évaluation et des mesures correctives envisagées pour améliorer les fragilités constatées. Les conclusions de ce rapport servent à orienter les priorités en vue de parfaire la politique de sécurité de protection du secret au ministère.

La chaîne de protection du secret est associée à l'élaboration de ce document. Sollicités par le haut fonctionnaire de défense et de sécurité ou ses représentants, les officiers centraux de sécurité transmettent les parties les concernant, charge à eux d'interroger leur réseau pour obtenir les précisions attendues.

1.2.4.5. La formation et la sensibilisation

Une politique ministérielle de formation et de sensibilisation est impulsée et organisée par le haut fonctionnaire de défense et de sécurité ou ses représentants. Des actions de sensibilisation et des formations spécifiques sont proposées à l'ensemble du réseau ministériel.

Lors de leur nomination, les OCS et les membres de la chaîne de la protection du secret sont formés aux spécificités de leur mission.

Les OCS et les membres de la chaîne de protection du secret proposent des formations et des actions de sensibilisation sur leur périmètre. Ils en informent le HFDS ou ses représentants afin d'assurer une harmonisation de la politique de sensibilisation ministérielle.

CHAPITRE 2 – HABILITATION PERSONNE PHYSIQUE

2.1. PRINCIPES GENERAUX

A titre de rappel, l'accès aux informations et supports classifiés (ISC) doit répondre à deux exigences cumulatives : l'habilitation et le besoin d'en connaître.

Le haut fonctionnaire de défense et de sécurité ou ses représentants sont autorité d'habilitation par délégation des pouvoirs du garde des Sceaux. L'établissement d'un catalogue des emplois est nécessaire pour chaque niveau de classification.

La fiche de poste et le contrat de travail doivent mentionner que le poste est soumis à l'habilitation au secret de la défense nationale.

La procédure d'habilitation vise à vérifier que l'agent a le droit d'accéder à des ISC dans l'exercice de ses missions et fonctions. L'IGI 1300 définit trois procédures d'habilitation :

- la procédure de droit commun ;
- la procédure d'urgence ;
- la procédure simplifiée : le ministère de la Justice n'y a pas recours sauf de manière exceptionnelle.

Les notices individuelles de sécurité (NIS) des candidats du ministère de la Justice à l'habilitation sont adressées par le HFDS ou ses représentants au service enquêteur en charge de rendre un avis de sécurité.

2.2. LES PROCEDURES DE DROIT COMMUN ET D'URGENCE

2.2.1. La procédure de droit commun

Cette procédure concerne tous les agents appelés à occuper un poste pour lequel le besoin d'habilitation au niveau *Secret* ou *Très Secret* est avéré, y compris pour le niveau *Très Secret* faisant l'objet d'une classification spéciale.

Délai de traitement : conformément à l'IGI 1300, la durée de l'enquête par le service enquêteur est en principe de six mois pour le niveau *Très Secret* et de trois mois pour le niveau *Secret*.

Typologie des avis de sécurité : le service enquêteur délivre un avis de sécurité qu'il transmet à l'autorité d'habilitation. Il y a trois types d'avis :

- sans objection : lorsque l'enquête n'a révélé aucune vulnérabilité de nature à constituer un risque pour la sécurité des ISC ;
- restrictif : lorsque le candidat présente des vulnérabilités susceptibles de constituer un risque pour la sécurité des ISC qu'il pourrait manipuler ;

- défavorable : lorsque les vulnérabilités sont telles qu'aucune mesure de sécurité ne serait à même de les maîtriser.

La durée d'une décision d'habilitation est de sept ans pour le niveau *Secret* et de cinq ans pour le niveau *Très Secret*, à partir de la date de l'avis de sécurité émis par le service enquêteur.

Pour sa décision, l'autorité d'habilitation n'est pas liée à l'avis du service enquêteur, mais l'informe de toute décision qui déroge à son avis. Elle y ajoute les éventuelles mesures complémentaires qu'elle aura décidées.

Le candidat concerné par le refus d'habilitation doit en être informé. Il ne peut occuper le poste soumis à habilitation inscrit au catalogue des emplois. Ce refus n'a pas l'obligation d'être argumenté par l'autorité d'habilitation. Le candidat a la possibilité d'effectuer un recours.

Procédure d'habilitation au *Très Secret* faisant l'objet d'une classification spéciale

Le haut fonctionnaire de défense et de sécurité n'est pas autorité d'habilitation pour les habilitations de niveau *Très Secret* faisant l'objet d'une classification spéciale. Pour ce type d'habilitation, l'officier central de sécurité du périmètre concerné se rapproche du haut fonctionnaire de défense et de sécurité ou de ses représentants.

2.2.2. La procédure d'urgence

Conformément à l'IGI 1300, cette procédure n'est pas applicable aux agents du service national du renseignement pénitentiaire (SNRP).

La procédure d'urgence revêt un caractère exceptionnel. Elle doit être justifiée et soumise à l'arbitrage de l'autorité d'habilitation.

Dans les quinze jours ouvrables suivant sa saisine, le service enquêteur émet un avis de sécurité provisoire au niveau *Secret* ou *Très Secret*, uniquement en cas d'avis sans objection, sur lequel s'appuie l'autorité d'habilitation pour délivrer une décision d'habilitation provisoire valable six mois.

2.3. LES PROCEDURES SPECIFIQUES

2.3.1. La portabilité de l'avis de sécurité

La décision d'habilitation est délivrée sur la base de l'avis de sécurité, rendu sur le poste antérieurement occupé. Cette décision n'excède pas la durée de validité de la précédente décision.

La décision d'habilitation dans le cadre de la portabilité n'est pas systématique. L'autorité d'habilitation peut la refuser et engager une procédure d'habilitation classique notamment en cas de changements significatifs dans la situation du candidat.

2.3.2. Habilitation temporaire

À la demande de l'officier central de sécurité, l'autorité d'habilitation peut décider d'accorder une décision d'habilitation temporaire, à un agent du ministère lorsque celui-ci est habilité au niveau *Secret* et a besoin de prendre connaissance ponctuellement d'informations ou supports classifiés au niveau *Très Secret*, hors classification spéciale. Cette décision est valable pour une durée de trois mois.

La décision d'habilitation temporaire n'est pas valable pour les personnes physiques travaillant pour le compte d'une personne morale habilitée dans le cadre d'un contrat prévoyant l'exécution de travaux classifiés.

2.3.3. Habilitation des ressortissants étrangers et des agents en postes à l'étranger

Le processus d'habilitation au sein du périmètre du ministère de la Justice pour les personnes physiques en poste au sein d'organisations internationales et des agents étrangers en poste au sein du périmètre du ministère de la Justice relève des dispositions de l'IGI 1300.

2.4. LE CYCLE DE VIE D'UNE DECISION D'HABILITATION

2.4.1. Le renouvellement d'une décision d'habilitation

Sur demande de l'officier central de sécurité, l'autorité d'habilitation prolonge d'un an une décision d'habilitation arrivée à échéance pour couvrir le délai de renouvellement de celle-ci, sous réserve de l'obtention par l'autorité d'habilitation de la notice individuelle de sécurité et du maintien du candidat sur le même poste.

2.4.2. L'abrogation d'une décision d'habilitation

Une décision d'habilitation est abrogée dans les cas suivants :

- au terme de sa durée de validité ;
- lorsque l'agent quitte les fonctions qui ont conduit à son habilitation ;
- en cas de comportements ou de vulnérabilités incompatibles avec le maintien de l'habilitation.

2.4.3. Conservation et communication des dossiers d'habilitation

Les dossiers d'habilitation et l'ensemble des documents liés à l'habilitation sont conservés par l'autorité d'habilitation pendant leur durée de validité et deux ans au-delà (soit neuf ans pour les dossiers *Secret* et sept ans pour les dossiers *Très Secret*).

L'autorité d'habilitation ne communique qu'à l'officier central de sécurité les informations relatives aux dossiers des personnes habilitées de son périmètre.

CHAPITRE 3 – HABILITATION PERSONNE MORALE

3.1. LES DIFFERENTS TYPES DE MARCHES

Afin de protéger le secret de la défense nationale dans les contrats, la réglementation (cf. IGI 1300 chapitre 4) prévoit trois types de marchés :

- marché classifié avec détention d'informations et supports classifiés (ISC) : le titulaire du contrat détient les ISC nécessaires à leur exécution et est responsable de leur gestion et de leur protection ;
- marché classifié sans détention d'ISC : le titulaire du contrat ne détient pas d'ISC dans ses locaux. Il y aura accès pour l'exécution du contrat au sein des locaux de l'autorité contractante ;
- marché sensible : toute prestation qui ne nécessite pas de détenir ou de consulter d'informations classifiées pour son exécution, au profit d'un service qui détient des ISC.

3.2. L'HABILITATION DES PERSONNES MORALES

L'autorité d'habilitation doit être informée par l'autorité contractante de tout appel d'offre public lorsque la prestation implique l'accès à des ISC. Le dossier d'habilitation de chaque candidat ayant répondu à l'appel d'offre doit être transmis au haut fonctionnaire de défense et de sécurité (HFDS) ou ses représentants pour un traitement auprès du service enquêteur. A l'issue, le service enquêteur rend un avis (sans objection, restrictif ou défavorable).

En cas d'urgence justifiée et après saisine du service enquêteur, une décision d'habilitation provisoire peut être délivrée.

3.2.1. La portabilité de l'avis de sécurité de l'habilitation personne morale

L'autorité d'habilitation ministérielle reconnaît les décisions prises par les autres autorités d'habilitation et s'appuie sur elles pour délivrer une décision d'habilitation dont la durée n'excédera pas celle de la décision prise antérieurement.

3.2.2. Le cas spécifique de l'habilitation d'une personne morale de droit étranger

Le ministère de la Justice reconnaît les principes exposés au sein de l'IGI 1300 pour une personne morale de droit étranger (cf. chapitre 4). Le HFDS ou ses représentants contactent à cet effet le secrétariat général de la défense et de la sécurité nationale (SGDSN) en sa qualité d'autorité nationale de sécurité.

3.2.3. Le plan contractuel de sécurité (PCS)

Faisant partie intégrante du contrat, ce plan détaille les mesures de sécurité requises pour garantir la protection des ISC tout au long de l'exécution du contrat. La signature du plan contractuel de sécurité par le HFDS ou ses représentants est indispensable pour obtenir la décision d'habilitation.

CHAPITRE 4 – SECURITE DES LIEUX

4.1. PRINCIPES GENERAUX DE SECURITE

Conformément à l'IGI 1300 (cf. chapitre 5), les informations et supports classifiés (ISC) doivent être détenus selon des règles de protection physique.

Les ISC sont conservés dans des lieux dits abritant. Ces locaux font l'objet de mesures de protection particulières selon l'analyse de risques et le niveau de classification des informations et supports détenus. Ces lieux doivent disposer des mesures de protection physique requises par la réglementation.

Les lieux d'échanges d'ISC, telles que des salles de réunion, doivent disposer de mesures de sécurité appropriées : au minimum, lors d'une réunion classifiée, la salle doit être fermée, les moyens connectés (portables, écouteurs connectés, montres connectées, ordinateurs ...) laissés à l'extérieur de la salle et les participants doivent être habilités.

Outre les lieux abritant, ce présent chapitre traite aussi des zones protégées et des zones réservées. Ces dernières, incluses dans une zone protégée, sont obligatoires pour les ISC au niveau *Très Secret*.

Ces mesures de protection recouvrent des moyens organisationnels, humains, techniques et logiques, qui peuvent être dissociés ou combinés selon le niveau de classification et les menaces identifiées.

Dans tous les cas, le système de protection s'inscrit dans une logique de défense en profondeur et repose sur des principes mentionnés dans l'IGI 1300 (cf. paragraphe 5.1 et annexes 29 et 30 de l'IGI 1300).

4.2. LES LIEUX ABRITANT

Les lieux abritant des ISC sont reconnaissables par la présence d'un meuble de sécurité (coffre ou armoire forte) conservant des éléments couverts par le secret de la défense nationale, élément minimal de protection pour conserver des ISC.

Les lieux dans lesquels sont conservés les éléments actifs des réseaux informatiques classifiés et les informations classifiées dématérialisées (disque dur, clé USB, CDROM...) sont considérés comme des lieux abritant.

Les lieux abritant doivent être clos et leurs accès fermés en l'absence du détenteur des ISC. Sous sa responsabilité, le lieu abritant peut accueillir des personnes non habilitées sous réserve de la fermeture du meuble de sécurité.

Pour la sécurité des ISC qui y sont conservés, les lieux abritant font l'objet d'un avis technique d'aptitude physique (ATAP). Cet avis reste facultatif sauf pour :

- les lieux abritant des ISC au niveau *Très Secret* ;

- les organismes extérieurs de droit privé qui détiennent des ISC sous la responsabilité du ministre de la Justice (cf. paragraphe 5.3.3 de l'IGI 1300).

4.3. LA ZONE PROTEGEE (ZP)

Une zone protégée (ZP) délimite des locaux et terrains clos dans lesquels la libre circulation est interdite et auquel l'accès est soumis à autorisation afin de protéger les installations, matériels et ISC qui s'y trouvent. La création d'une zone protégée est recommandée pour les lieux abritant des informations et supports classifiés au niveau *Secret*.

La ZP est créée par arrêté ministériel signé par le HFDS ou ses représentants. Cet arrêté n'est pas publié au *Journal officiel* de la République française. La ZP est matérialisée par des panneaux visibles mentionnant l'interdiction de pénétrer sans autorisation sous peine de poursuites, conformément aux articles 413-7 et 413-8 du code pénal.

Gestion des accès en zone protégée

Sous l'autorité du responsable de l'entité qui abrite la ZP, l'OCS ou ses représentants proposent et mettent en œuvre la politique d'accès dans le respect des modalités détaillées au point 5.3.1.1 de l'IGI 1300. Cette politique est présentée au HFDS ou à ses représentants qui se réservent le droit d'émettre d'éventuelles recommandations.

4.4. LA ZONE RESERVEE (ZR)

Incluse au sein d'une ZP, la zone réservée (ZR) est obligatoire pour les lieux abritant des ISC au niveau *Très Secret*. Elle vise à renforcer les mesures de sécurité comprenant le meuble de sécurité (coffre-fort ou armoire forte), le contrôle des accès et la surveillance des lieux (cf. paragraphe 5.3.1.2 et annexe 32 de l'IGI 1300).

Pour la création d'une ZR, un avis technique d'aptitude physique, délivré par le service enquêteur est obligatoire préalablement à la détention d'ISC. Pour que la ZR soit reconnue et enregistrée, la décision de création, signée par le chef de l'entité concernée, doit être transmise au HFDS ou à ses représentants.

CHAPITRE 5 – SECURITE DES SYSTEMES D'INFORMATION CLASSIFIES (SIC)

5.1. GENERALITES

Le présent chapitre porte sur les réseaux interministériels classifiés développés et mis à disposition par l'opérateur des systèmes d'information interministériels classifiés (OSIIC) : ISIS intranet sécurisé, OSIRIS (téléphone sécurisé) et HORUS (visioconférence sécurisée).

Au sein du ministère de la Justice, il existe d'autres systèmes d'information classifiés (SIC) qui répondent à des procédures particulières d'installation et d'accès. Tout système d'information classifié utilisé par un service du ministère de la Justice doit être porté à la connaissance du haut fonctionnaire de défense et de sécurité (HFDS) ou de ses représentants, notamment l'officier de sécurité des systèmes d'information (OSSI) et ce afin de définir les priorités et les travaux d'installation.

En cas d'élaboration d'un système d'information classifié, le ministère de la Justice applique la réglementation en vigueur.

5.2. PROCESSUS D'INSTALLATION D'UN SYSTEME D'INFORMATION CLASSIFIE (ISIS/OSIRIS/HORUS)

L'installation d'un système d'information classifié est soumise :

- à l'accord de principe du HFDS ou de ses représentants ;
- à la faisabilité technique (local technique, câblage) ;
- au respect des obligations de sécurité spécifiques à ce type d'équipement, notamment en matière de lutte contre les signaux parasites compromettants (cf. II 300)

5.3. UTILISATION DU POSTE

5.3.1. Demande d'accès

Chaque utilisateur doit être habilité. Avant toute demande, l'officier de sécurité (OS) vérifie cette habilitation, au risque d'engager sa responsabilité en cas d'utilisation non conforme du SIC. Les accès sont valables le temps de l'habilitation et sont immédiatement retirés lorsque l'utilisateur perd son habilitation.

5.3.2. Accès à l'intranet sécurisé ISIS

La carte et le code secret sont des articles contrôlés de la sécurité des systèmes d'information (ACSSI) et doivent être traités comme des informations et supports classifiés (ISC) au niveau Secret. Ils doivent être conservés dans un meuble de sécurité (coffre-fort ou armoire forte). La carte sans son code secret n'est pas soumise aux mesures de conservation et de

manipulation propres aux ISC (cf. II 910 relative aux ACSSI).

5.4. REGLES DE SECURITE D'UTILISATION ET DE CONSERVATION

L'utilisateur est responsable du bon usage de l'ensemble des équipements et du respect des conditions générales d'utilisation établies par l'OSIIC. Ce matériel ne doit pas être débranché sans autorisation préalable du HFDS ou de ses représentants. Chaque officier central de sécurité (OCS) ou ses représentants, conseillés par l'OSSI, s'assurent du respect de ces mesures par les utilisateurs de leur périmètre.

5.5. SUPPORTS EXTERNES

La connexion ou l'installation d'équipements non autorisés à un SIC est interdite. L'intégrité de l'unité collective (souris, écran, clavier, lecteur carte, unité centrale, imprimante éventuelle), doit être préservée.

Toutefois, des supports numériques professionnels (notamment clés USB, disques durs) dédiés exclusivement à l'usage du SIC peuvent être autorisés par l'OCS ou ses représentants. Ces supports externes deviennent des supports classifiés. A ce titre, ils sont enregistrés sur l'inventaire du détenteur et contrôlés par l'OCS ou ses représentants. Ils sont conservés dans un meuble de sécurité (coffre-fort ou armoire forte).

5.6. CONTROLE/INSPECTION

Un contrôle, à la fois qualitatif (respect des règles d'utilisation) et quantitatif (recensement du matériel et localisation), est effectué sur tous les matériels utilisés, annuellement par l'OCS ou ses représentants. Le HFDS ou ses représentants sont informés des infractions aux règles de sécurité. Un rappel des règles est effectué à l'utilisateur par l'OCS ou ses représentants.

En cas de non-respect des règles d'utilisation, le HFDS ou ses représentants peuvent diligenter une inspection auprès des services compétents. L'utilisateur s'expose alors aux sanctions relatives à la compromission.

CHAPITRE 6 – GESTION DES INFORMATIONS ET SUPPORTS CLASSIFIES

6.1. DEBUT DE VIE DES INFORMATIONS ET SUPPORTS CLASSIFIES

La classification d'une information ou d'un support au titre du secret de la défense nationale vise à en limiter l'accès aux seules personnes dûment habilitées, conformément aux articles 413-10 et suivants du code pénal. Cette classification est matérialisée par l'apposition d'un timbre. Non seulement il caractérise l'infraction pénale en cas de compromission mais il impose également des mesures de protection pour la gestion de ces informations et supports classifiés (ISC) tout au long de leur cycle de vie.

6.1.1. Autorité émettrice

Le HFDS ou ses représentants sont autorité émettrice. A ce titre, ils élaborent un guide de classification ministériel qui regroupe les informations et thématiques que le ministère de la Justice entend protéger. En lien avec les officiers centraux de sécurité (OCS), ce guide agrège les sujets portés par les directions, services et entités qu'ils représentent. Ces différents sujets sont regroupés dans un guide de classification propre à chacune de ces directions, services ou entités et est transmis par l'OCS au HFDS ou ses représentants.

6.1.2. Elaboration des informations et supports classifiés

La présente instruction met en œuvre les principes de classification énoncés au chapitre 7.1.1.2 de l'IGI 1300.

Pour l'élaboration d'un document classifié, en lien avec son OCS ou ses représentants, l'agent habilité doit apposer le timbre de classification selon le niveau requis et suivre les règles définies par le guide de classification ministériel. La création d'un ISC doit se faire sur un support classifié correspondant au niveau requis.

Cas particulier : Un ensemble d'informations ou de supports peut être classifié même si aucun d'eux ne l'est individuellement. Cet ensemble, appelé agrégat peut également être classifié à un niveau supérieur.

La présente instruction met en œuvre les dispositions relatives au marquage mentionnées au chapitre 7.1.2. de l'IGI 1300.

Chaque ISC doit comporter un timbre de classification indiquant le niveau de classification des informations qu'il contient. Les informations suivantes doivent figurer en première page :

- le timbre de classification (également présent sur chaque page) et les éventuelles mentions de protection ;
- la date d'échéance de la classification ;
- les références de l'autorité émettrice et de l'auteur de l'information ou du support ;
- la date d'émission ;
- le numéro d'enregistrement de l'information ou du support ;
- le nombre total de pages y compris les annexes. Chaque page doit être numérotée selon le format « numéro de la page/nombre total de pages ».

6.2. TRAITEMENT DES INFORMATIONS ET SUPPORTS CLASSIFIES

6.2.1. Cas particulier de la gestion des ISC de niveau *Très Secret*

Cette présente instruction ministérielle n'aborde pas la gestion des ISC de niveau *Très secret*.

L'OCS informe le HFDS ou ses représentants dès réception des ISC de ce niveau afin de connaître les règles de gestion appropriées.

6.2.2 Conservation, traçabilité et reproduction

Les ISC sont placés sous la responsabilité du détenteur et de l'OCS ou de ses représentants. Les ISC sont conservés dans un meuble de sécurité (coffre-fort ou armoire forte) conforme aux dispositions de l'IGI 1300 (cf. Annexe 30).

Afin d'en assurer la traçabilité, un inventaire est réalisé annuellement par les détenteurs, sous le contrôle de l'OCS ou de ses représentants. Les informations classifiées dématérialisées (sur ISIS) ne sont pas soumises à cette obligation.

A chaque mutation de personnel, un inventaire contradictoire est effectué entre l'ancien et le nouveau détenteur. Cet inventaire doit être signé par les intéressés et contresigné par l'OCS ou ses représentants.

Les supports classifiés, y compris les supports de stockage d'informations classifiées dématérialisées, font l'objet d'un suivi permanent afin d'assurer leur traçabilité et leur prise en compte par des détenteurs habilités.

La reproduction numérique (impression, scan ou photocopie) d'informations classifiées est autorisée uniquement sur un matériel classifié, connecté au réseau ISIS ou hors réseau à usage dédié, et sous la responsabilité de l'utilisateur, détenteur du document original. En cas de reproduction, les exemplaires doivent être numérotés (« copie n° X ») et inscrits à l'inventaire.

6.2.3 Transmission des informations et supports classifiés

L'envoi d'un ISC s'effectue par un système d'information classifié (SIC) ou sous double enveloppe, avec présence de bordereaux d'envoi (cf. paragraphe 7.3.1.2 de l'IGI 1300) :

- Enveloppe extérieure : sont uniquement indiquées les adresses de l'émetteur et du destinataire ;
- Enveloppe intérieure : sont mentionnés le timbre du niveau de classification, la référence des supports transmis, le cachet de l'autorité expéditrice, le nom et la fonction du destinataire ainsi que l'indication de l'organisme dans lequel il est affecté. L'enveloppe de sécurité est à privilégier.

Le destinataire doit être habilité. Il revient à l'émetteur du document de s'assurer du niveau d'habilitation de son interlocuteur.

L'expédition des ISC peut être effectuée par :

- Le détenteur lui-même ;

- Un tiers, clairement identifié auprès de l'OCS ou de ses représentants ; Il doit signer une déclaration de convoyage par laquelle il s'engage à respecter les obligations liées à la protection des documents transportés. Il n'a pas besoin d'être habilité ;
- Un convoyeur agréé, opérateur postal agréé par le ministère de la Justice.

Le transport des ISC depuis ou vers l'étranger est autorisé selon les modalités précisées dans l'IGI 1300 (CF. 7.3.2.1 c). Les OCS ou leurs représentants sont invités à se rapprocher du HFDS ou de ses représentants.

Cas particulier de la transmission des cartes ISIS par envoi postal :

L'envoi postal des cartes ISIS sur le territoire national s'effectue en deux temps, avec accusé de réception : le premier envoi concerne la carte et le second le code. Ces éléments doivent être envoyés sous double enveloppe avec présence de bordereaux d'envoi.

6.3. DESTRUCTION DES INFORMATIONS ET SUPPORTS CLASSIFIES

En lien avec chaque détenteur, l'OCS ou ses représentants identifient les ISC ne présentant plus d'utilité administrative courante et procèdent à leur destruction selon les modalités définies au 7.5.1 de l'IGI 1300. Cette destruction est réalisée sur un équipement conforme à la réglementation (cf. Arrêté du 20 août 2024 relatif aux normes techniques de destruction des informations et supports classifiés ou protégés).

6.4. VERSEMENT DES INFORMATIONS ET SUPPORTS CLASSIFIES AUX ARCHIVES

En lien avec chaque détenteur, l'OCS identifie les ISC ne présentant plus d'utilité administrative courante et procède à leur versement aux archives selon les modalités définies au 7.5.4 de l'IGI 1300. Le service ministériel des archives devient responsable de ces ISC. Il peut en recevoir jusqu'au niveau *Très Secret* hors classification spéciale.

6.4.1. Communicabilité des informations et supports classifiés ayant fait l'objet d'une mesure de classification versés aux archives

Ces ISC ne sont pas communicables en l'état, sauf règles mentionnées dans l'article L. 213-2 du code du patrimoine.

6.4.2 Demande de consultation d'une information ou support classifié par une personne habilitée

La consultation des ISC est soumise à l'autorisation du HFDS ou de ses représentants après qu'ils ont été saisis par le service ministériel des archives sauf pour les ISC créés par le ministère. Dans ce cas, le service ministériel des archives autorise cette consultation, sous réserve que la personne soit habilitée et qu'elle appartienne au ministère.

Le service ministériel informe annuellement le HFDS ou ses représentants de ces consultations.

6.4.3 Demande de consultation d'une information ou support classifié par une personne non habilitée

La consultation d'un ISC par une personne non habilitée nécessite sa déclassification, qui suit une procédure dédiée. Selon l'article L. 213-3 du code du patrimoine, des autorisations de consultation peuvent être accordées si cela ne nuit pas aux intérêts protégés par la loi.

6.5. DECLASSIFICATION DES INFORMATIONS ET SUPPORTS CLASSIFIES

La déclassification d'une ISC peut résulter d'une initiative de l'autorité émettrice, d'une demande d'un détenteur à ladite autorité émettrice (lors d'une révision annuelle de l'inventaire ou lors du versement aux archives), être provoquée par une requête en déclassification judiciaire, par une demande de communication d'archives ou intervenir à l'issue du délai mentionné lors de la classification du document.

6.5.1 Déclassification automatique

Sont déclassifiés et deviennent communicables sans intervention du HFDS ou de ses représentants, de l'OCS ou de ses représentants, les ISC dont la durée de classification est échue (date d'échéance de classification, délai de 50 ou de 100 ans).

6.5.2 Déclassification nécessitant une décision formelle matérialisée par un timbre de déclassification

La décision de déclassification d'un ISC est prise par l'autorité émettrice. En conséquence, l'autorité émettrice ministérielle ne peut déclassifier que les ISC qu'elle a créés.

La déclassification d'un ISC est matérialisée par l'apposition d'un timbre de déclassification. Par ce timbre la déclassification est officielle.

6.5.3 Démarche de demande de déclassification auprès du service émetteur

Toute demande de communication d'un ISC doit être adressé au HFDS ou à ses représentants. Le demandeur est informé de l'incommunicabilité des ISC au titre de la protection du secret de la défense nationale et de la procédure pour obtenir sa déclassification.

ANNEXE

Guide de classification

La notion de secret de la défense nationale est difficile à cerner. Elle dépend des dossiers et sujets de chaque direction et service. En conséquence, il revient à chaque officier de sécurité de définir, avec ses responsables hiérarchiques et les détenteurs d'informations et de supports, ce qui relève du secret de la défense nationale et doit donc être classifié. A cet effet, il doit établir un guide de classification, document qui permettra d'aider les acteurs de son périmètre à définir quelles informations et quels documents doivent être classifiés et à quel niveau de classification (*Secret* ou *Très Secret*).

La présente annexe propose un cadre général sur les informations qui peuvent être classifiées et une procédure d'élaboration du guide de classification.

Procédure d'élaboration du guide de classification

Chaque officier central de sécurité (OCS) est responsable de cette élaboration. Dans la limite des éléments de cadrage généraux propres au ministère, il définit les thèmes, sujets et informations nécessitant une classification, en s'appuyant sur les détenteurs d'informations et de supports classifiés (ISC) et les accompagne dans la réflexion. Il supervise et coordonne le guide de classification de son périmètre.

Dans le cas de l'existence d'un réseau, l'OCS demande à ses officiers locaux de contribuer à ce document sur des points spécifiques qui pourraient être intégrés au guide de classification de son périmètre. Ces derniers établissent leur guide en s'appuyant sur les besoins et les thèmes de chaque rédacteur. L'officier central agrège l'ensemble des thématiques et soumet le document final au haut fonctionnaire de défense et de sécurité ou à ses représentants. Cette étape vise à vérifier notamment l'harmonisation des thèmes et sujets retenus.

Les guides des OCS constituent le guide de classification ministériel. Ce guide doit être classifié et actualisé.

Etablissement du guide de classification

Pour élaborer le guide de classification, il est essentiel de prendre en compte des éléments généraux qui constituent un socle commun, tout en intégrant les spécificités de chaque direction, service ou entité. Ces éléments incluent :

- la réciprocité : une réponse à un ISC doit être elle-même classifiée au niveau requis ;
- les obligations réglementaires, qui imposent le secret et donc la classification du document ou de la réponse ;
- la confidentialité des informations traitées, qu'elles soient connues ou non, et ce, quelle qu'en soit la source.

Dans la réflexion, en vue de l'élaboration du guide de classification, plusieurs pistes peuvent être étudiées :

- La protection des sources d'information ;
- La dimension diplomatique de l'information, notamment pour des informations confidentielles, en cas de menaces d'acteurs de la communauté internationale, pays, acteurs économiques... ;

- La protection de la personne, objet de la note, notamment si les éléments la concernant ont une incidence sur son image, son profil ou ses agissements ;
- Les activités en lien avec des services de renseignement, selon le degré de précision et de confidentialité des informations traitées. Cela inclut la protection de la confidentialité d'un service particulier ou de ses activités, notamment les parquets spécialisés, les établissements pénitentiaires spécifiques ;
- Des domaines plus favorables à une classification : la diplomatie secrète ou confidentielle ; le domaine militaire, notamment lié à la dissuasion ou aux systèmes d'armement ; les négociations commerciales et économiques. Toutefois, dans ces domaines, il convient de veiller à la stricte application du principe de modération dans la classification, c'est-à-dire d'éviter l'automatisme et de classer ce qui ne doit pas l'être, notamment des informations connues du grand public, qui n'ont pas été classifiées.

Pour rappel, le marquage est essentiel pour définir le secret de la défense nationale. La classification d'un document implique des contraintes et obligations avec des conséquences pénales.