



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

Objectifs et règles de sécurité numérique du ministère de l'Intérieur

PGSN – B02

**Classification, marquage et traitement de
l'information**

Version 1.0

TABLE DES MATIERES

1.	Règles générales	4
1.1.	Plan de classification	4
1.2.	Marquage de l'information.....	7
2.	Règles relatives à la gestion documentaire	8
2.1	Solutions autorisées	8
2.2	Rédaction des documents.....	8
2.3	Validation des documents	8
2.4	Approbation des documents.....	8
2.5	Consultation des documents.....	9
2.6	Retrait des versions obsolètes	10
2.7	Règle de nommage des documents	10
2.8	Suivi de la documentation	11
2.9	Impression de documents	11
3.	Règles relatives à la diffusion de l'information.....	12
3.1	Limitation des destinataires.....	12
3.2	Format numérique	12
3.3	Format papier	13
4.	Règles relatives au stockage et à l'archivage de l'information ...	13
4.1	Format numérique	13
4.2	Format papier	14
5.	Règles relatives à la destruction de l'information	15
6.	Rappels des sanctions en cas de divulgation de l'information ...	15

Préambule

Le présent document est une composante à part entière de la politique générale de sécurité numérique du ministère de l'Intérieur (PGSN-MI). Il décrit les règles relatives à la classification, au marquage et au traitement des informations (qu'elles soient automatisées, informatisées ou au format papier), applicables à toutes les directions et services du ministère de l'Intérieur. A ce titre, il remplace la doctrine du 20 avril 2016 relative à la protection des données sensibles du ministère.

Les règles définies dans la suite du document ont pour objectifs de permettre l'identification, l'élaboration, le contrôle, l'acceptation ou l'approbation, la diffusion, le classement et l'archivage des données qu'ils contiennent. A ce titre, elles ont vocation à préciser, pour chaque type de données à produire ou traiter, le niveau de classification adapté, les principes liés à son marquage, son acceptation ou à son approbation, ses modalités de diffusion, de stockage ou d'archivage, le type de contrôle interne auquel il est soumis.

Tous les documents du ministère de l'Intérieur, et ce quel que soit le support utilisé, sont soumis aux règles du présent document, aux mêmes titres que les autres exigences applicables de la PGSN.

1. Règles générales

1.1. Plan de classification

L'information est considérée sensible dès lors que sa divulgation au public entraîne ou pourrait conduire à un préjudice substantiel (dans le domaine financier, juridique, dans le cadre de l'activité et des missions de l'entité, en terme de perception de l'institution ...) qui oblige à restreindre l'accès à l'information selon le principe du besoin d'en connaître.

Le niveau de sensibilité de l'information doit être clairement identifiable. En conséquence, il est nécessaire d'apposer un marquage qui ne laisse aucune ambiguïté quant au niveau de sensibilité des données ou des informations qu'ils contiennent et permettre ainsi leur traitement dans les conditions requises par ses destinataires.

Le niveau de classification de l'information doit être affecté dès sa création, en fonction des exigences réglementaires et de sa sensibilité.

Au sein du ministère, les niveaux de classification applicables sont listés dans le tableau suivant :

Marquage	Sensibilité	Définition	Libellé
Public	Non sensible	Les informations ont vocation à être accessibles à la sphère publique.	PUB
Non Protégé	Non sensible	Les informations peuvent être diffusées volontairement ou dont la diffusion involontaire à la sphère publique ne porte pas de préjudice au ministère ou à ses partenaires du secteur public ou privé.	NP
Interne <MI/Entité/Projet>	Peu sensible	L'information ne peut être connue que par les personnels et prestataires d'un projet, d'une entité du ministère ou du ministère lui-même.	INT
Diffusion Contrôlée	Sensible	L'information n'est connue que par des personnes formellement désignées et les mesures de protection et d'identification tendent à respecter l'II 901. Les informations portant cette mention sont soumises à une restriction de diffusion impliquant une communication qu'aux personnes ayant le besoin d'en connaître dans l'exercice de leurs attributions. Cette mention concerne particulièrement les échanges entre différentes parties dont la conformité au niveau « Diffusion Restreinte » ne peut être garantie.	DC
Diffusion Restreinte	Sensible	L'information n'est connue que par des personnes formellement désignées et les mesures de protection et d'identification associées se conforment à l'II 901. Les informations portant cette mention sont soumises à une restriction de diffusion ne devant être communiquées qu'aux personnes ayant le besoin d'en connaître dans l'exercice de leurs attributions.	DR

Marquage	Sensibilité	Définition	Libellé
Secret	Classifié IGI 1300	Les modalités de traitement, d'identification et de diffusion doivent être conformes aux exigences de l'IGI 1300. L'information n'est connue que par des personnes formellement désignées et habilitées au niveau « Secret ». Le traitement informatique de ces informations ne peut être effectué que sur un système d'information homologué, par exemple un poste ISIS. Les exigences de ce niveau de classification s'appliquent aux documents Confidentiel et Secret UE/OTAN.	NS
Très Secret	Classifié IGI 1300	Les modalités de traitement, d'identification et de diffusion doivent être conformes aux exigences de l'IGI 1300. L'information n'est connue que par des personnes formellement désignées et habilitées au niveau « Très Secret ».	NTS

Au sein du ministère de l'intérieur, les informations suivantes sont considérées comme sensibles par défaut :

- Données sensibles à caractère personnel au sens du règlement général sur la protection des données¹ ;
- Informations à caractère personnel des personnels dits « sensibles » du ministère ;
- Informations des marchés relevant de la 3^{ème} partie du code des marchés publics (ex : marché de défense et de sécurité) ;
- Informations contribuant aux missions essentielles du ministère ou vitales de la nation ;
- Informations contribuant aux fonctionnements ou à la sécurité des activités et actifs du ministère (mots de passe, fichiers de configuration, ...) ;
- Informations produites en temps de crise ;
- Informations sur la sécurité des bâtiments (vidéo-protection, contrôle d'accès physique, etc.) ;
- Informations liées au dossier d'homologation des systèmes d'information du ministère (Analyse de risques, rapports d'audit, documents d'architecture, ...) ;
- Informations métiers et codes sources des applications traitant des informations ou données mentionnées précédemment.

Cette liste n'est pas exhaustive et chaque entité relevant du ministère de l'Intérieur a pour responsabilité de préciser, pour son périmètre de responsabilité, les familles d'informations considérées comme sensibles.

¹ Se référer à la politique de conformité des données personnelles du ministère de l'Intérieur (PCDP-MI), disponible à l'adresse : <http://sg.minint.fr/index.php/rgpd/pcdp-mi>

Pour les documents, le créateur en est par défaut le propriétaire. A ce titre, il est responsable du choix du niveau de classification du document :

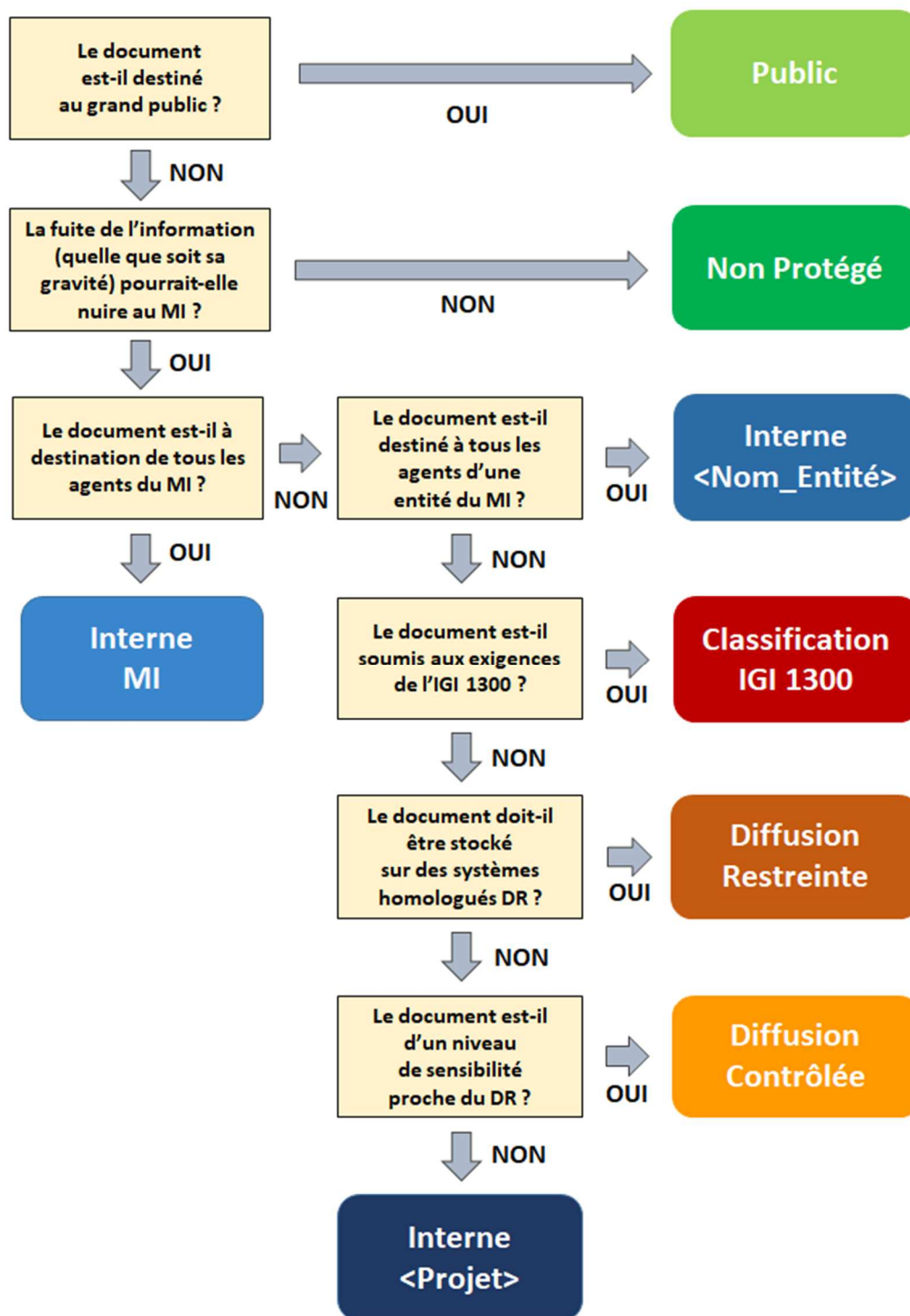


Figure 1 : Principe décisionnel général de classification

En fonction du niveau retenu, le document fait l'objet d'un marquage et des règles de protection adaptées. Par défaut, les documents ne portant aucune mention de classification sont réputés non protégés et leur diffusion dans le domaine public ne devrait entraîner aucun préjudice pour le ministère ou ses partenaires du secteur public ou privé.

Des déclinaisons locales de la PGSN peuvent néanmoins avoir leur propre exigence sur le niveau par défaut des documents liés au projet ne comportant aucune mention de classification.

1.2. Marquage de l'information

Dans le but d'éviter toute ambiguïté, tout marquage d'un document sensible doit apparaître distinctement en haut de chaque page. Pour les documents d'un niveau de sensibilité inférieur, le marquage doit obligatoirement apparaître sur chaque page du document mais son positionnement reste à la discrétion de son rédacteur.

La mention « Spécial France » doit être employée pour les documents ou supports d'informations que l'entité du ministère estime devoir être divulgués aux seuls ressortissants français et qui ne sauraient, en aucune circonstance, être communiqués, en tout ou partie, à un État étranger ou à l'un de ses ressortissants, à une organisation internationale ni à une entreprise de droit étranger, même s'il existe avec cet État ou cette organisation un accord de sécurité.

Le timbre « Spécial France » est apposé selon les règles en vigueur (IGI 1300), que le document soit électronique ou papier, selon le modèle suivant :

SPECIAL FRANCE

Cette mention doit figurer immédiatement à droite ou au-dessous du timbre de classification ou de la mention de protection de l'information.

Les informations sensibles portant la mention « Diffusion Restreinte » sont marquées conformément au modèle ci-dessous :

DIFFUSION RESTREINTE

Ce marquage est applicable selon les mêmes modalités pour les documents portant la mention « Diffusion Contrôlée ».

Les informations suivantes doivent systématiquement être marquées à minima par la mention « Diffusion Restreinte » :

- Les analyses de risques ;
- Les rapports d'audit ;
- Les documents d'architecture technique ;
- Les plan d'actions issus des documents précédents ;
- Les supports de présentation des pré-commissions et commissions d'homologation.



Pour les informations très sensibles, regroupant les informations classifiées de défense, les exigences de l'IGI 1300 doivent s'appliquer sans mesure dérogatoire possible.

2. Règles relatives à la gestion documentaire

2.1 Solutions autorisées

Tous les documents produits, différents du format standard *PDF*, doivent par défaut être compatibles avec la solution *LibreOffice*.

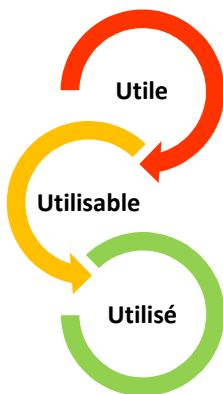
La suite *Microsoft Office* peut être utilisée dès lors que le document est enregistré au format *LibreOffice* ou qu'une version *LibreOffice* du document est disponible.

2.2 Rédaction des documents

Tout le personnel a la possibilité de rédiger un document afin de proposer sa mise en œuvre. Le nom du rédacteur doit apparaître en première page du document ou dans l'historique des versions.

Le conseiller de la sécurité numérique (CSN) de l'entité (ou son représentant) est le seul acteur qui doit obligatoirement être présent dans la chaîne de validation des documents du dossier de sécurité.

Dès sa conception, il est recommandé que tout document respecte la « règle des 3 U » afin qu'il soit adapté à son public cible :



1. **Utile** : document informatif ou explicatif qui est non redondant ;
2. **Utilisable** : document compréhensible, exploitable et structuré. Le langage est adapté au public visé et le cas échéant, son application a été testée ;
3. **Utilisé** : document connu, accessible, apprécié, lisible et compris par le public cible. Il doit pouvoir faire l'objet de critiques pour être sujet à des améliorations.

2.3 Validation des documents

La finalisation d'un document passe par une étape de validation par l'ensemble des acteurs de la chaîne métier et sécurité le cas échéant. La finalisation peut donner lieu à des réunions ad-hoc permettant de statuer sur le document en vue de sa finalisation.

Il convient que les représentants des différentes chaînes doivent signer le document pour attester de l'acceptation de son contenu.

L'étape de validation est un préalable à toute communication du document à l'approbateur final.

2.4 Approbation des documents

Une fois le document validé, il convient qu'il soit soumis pour approbation à un responsable disposant du niveau hiérarchique suffisant pour imposer son application et autoriser sa diffusion au public cible.

Chaque entité du ministère doit élaborer sa propre procédure d'approbation de la documentation et la mettre à disposition de l'ensemble de ses personnels.

Remarque :

- Conformément à l'IGI 1300, il est rappelé que tout document classifié, qu'il soit en émission ou en réception d'un service de l'administration, doit faire l'objet d'un référencement par l'officier de sécurité de l'entité.
- Les documents contenant des données à caractère personnel n'ont pas vocation à faire l'objet d'une validation particulière. Ils ne peuvent être initiés que dans le strict respect des exigences du RGPD en suivant les prescriptions de la politique de conformité des données personnelles du ministère de l'intérieur. En cas de besoin, vous pouvez contacter le correspondant à la protection des données (CPD) de votre entité pour plus d'informations.

2.5 Consultation des documents

2.5.1 Format numérique

En fonction du marquage apposé, les modalités de diffusion doivent respecter les règles suivantes :

- **« Public » ou « Non Protégé »** : Aucune mesure de protection particulière n'est obligatoire pour leur consultation.
- **« Interne »** : La consultation de ces documents doit se faire dans des locaux maîtrisés² et sur un poste du ministère. En situation de nomadisme, l'utilisation d'un filtre de confidentialité est obligatoire.
- **« Diffusion Contrôlée » et « Diffusion Restreinte »** : La consultation de ces documents doit se faire dans des locaux maîtrisés et sécurisés³, sur un poste du ministère de l'intérieur. En situation de nomadisme, un filtre de confidentialité doit être utilisé et toute consultation dans des lieux publics est à proscrire.
- **« Secret »** : L'utilisation d'un poste ISIS est obligatoire pour la consultation d'information classifiée à ce niveau.
- **« Très Secret »** : Se référer aux exigences de l'IGI 1300. Il n'existe pas de dispositifs particuliers pour gérer ce niveau d'information.

2.5.2 Format papier

Selon le marquage apposé, les modalités de diffusion des documents papiers doivent respecter les règles suivantes :

- **« Public » ou « Non Protégé »** : Aucune mesure de protection particulière n'est obligatoire pour leur consultation.
- **« Interne »** : La consultation de ces documents doit se faire dans des locaux maîtrisés.
- **« Diffusion Contrôlée » et « Diffusion Restreinte »** : La consultation de ces documents doit se faire dans des lieux maîtrisés et sécurisés.
- **« Secret » ou « Très Secret »** : la consultation de ces documents doit se faire dans des locaux sécurisés répondant aux exigences de l'IGI 1300.

² Le terme « Local maîtrisé » désigne un espace sous la gestion exclusive de la personne qui consulte la documentation (bureau de l'agent, domicile, ...)

³ Le terme « Local sécurisé » désigne un espace dont les accès et les dispositifs de surveillance sont gérés par le ministère de l'Intérieur ou tout autre entité mettant en œuvre des dispositifs de sécurité physique de même niveau.

2.6 Retrait des versions obsolètes

Dans le but d'éviter la poubellisation des bases documentaires, les versions obsolètes doivent être supprimées ou archivées. Dans le cas où les documents contiennent des informations confidentielles, il est nécessaire de les chiffrer avant suppression ou archivage en s'assurant de la disponibilité dans le temps de la clé de chiffrement et des outils utilisés. Une vigilance particulière devra être apportée sur la compatibilité des nouvelles versions des outils avec les archives générées à partir d'anciennes versions.

2.7 Règle de nommage des documents

Afin de pouvoir identifier rapidement et clairement la sensibilité d'un fichier bureautique (texte, tableur, image, présentation, vidéo, ...), **il est obligatoire d'indiquer dans le libellé de son nommage l'abréviation de la mention de protection associée.**

Chaque document doit être identifié de manière unique. Le nom d'un fichier ne doit pas comporter d'espace et être composé uniquement des caractères [0-9], [a-z], [A-Z], « _ » et « - ». Les caractères accentués ou spécifiques sont proscrits.

Le tableau des attributs ci-après peut être utilisé pour définir la nomenclature des documents :

Attributs	Présence
Référence à l'entité propriétaire du document (MI par défaut).	Obligatoire
Le libellé de la classification du fichier (PUB = Public, NP = Non Protégé, INT = Interne, DC = Diffusion Contrôlée, DR = Diffusion Restreinte, ...). La mention « Spécial France » peut être rajoutée à la suite du libellé précédent par les deux lettres « SF ».	Obligatoire
Le nom du projet concerné (ou de l'entité émettrice si le document à une visée transverse).	Obligatoire
L'acronyme du document (CR, FEB, AR, DAT, CIT, PES, ...).	Optionnelle
Le titre du document.	Obligatoire
▪ La version du document : ○ Version de travail : v0.1, v0.2, ... ; ○ Version applicable : v1.0.	Obligatoire
La date de livraison du document.	Optionnelle

Il est vivement recommandé que le nom d'un document soit limité à une longueur maximale de 80 caractères. Chaque attribut est concaténé par le caractère « _ » et le caractère « - » est utilisé pour séparer les informations à l'intérieur d'un attribut.

Les exemples suivants illustrent la cible attendue en termes de nomenclature des documents :

- MI_DRSF_Projet-test1_AR_Analyse-de-risques_v1.0_20201015
- MI_INT_Projet-test2_SH_Stratégie-d'homologation_v0.1_20201015

2.8 Suivi de la documentation

L'ensemble de la documentation doit être répertorié en vue de pouvoir en assurer un suivi permanent, notamment pour permettre de garantir le maintien en condition de sécurité des livrables des dossiers d'homologation. Cet inventaire doit être communiqué, autant que de besoin, à l'ensemble des acteurs clés du projet.

Il permet de s'assurer que tous les acteurs concernés sont informés de l'existence (ou disposeront directement) de l'information, à jour, qui leur est nécessaire pour mener à bien leurs tâches. Il prendra en compte les éventuelles exigences de confidentialité concernant certaines informations.

Quelle que soit la forme retenue pour réaliser cet inventaire ou sa périodicité de mise à jour, il doit recenser à minima :

- Le nom du document ;
- L'auteur du document ;
- Le numéro de version ;
- La classification du document.

Cette opération de suivi doit permettre une réévaluation de la classification des documents.

2.9 Impression de documents

L'impression des documents, autres que ceux portant la mention « Public » ou « Non Protégé », doit être effectuée de manière sécurisée en respectant les exigences édictées par la DNUM et le ST(SI)².

L'utilisateur doit garder le contrôle de l'impression du déclenchement jusqu'à la récupération du document papier.

Les imprimantes et copieurs multifonctions sont des ressources informatiques à part entière qui doivent être gérées en tant que tels et ne doivent pas pouvoir communiquer avec l'extérieur du réseau du ministère.

Les imprimantes et copieurs multifonctions doivent faire l'objet d'un durcissement en termes de sécurité prenant en compte à minima les éléments suivants :

- Changement des mots de passe initialement fixés par le « constructeur » ;
- Désactivation des interfaces réseau inutiles ;
- Suppression des services inutiles ;
- Chiffrement des données sur le disque dur lorsque cette fonctionnalité est disponible ;
- Configuration réseau statique.

Enfin lorsqu'elle est activée la fonction de numérisation sur les copieurs multifonctions les mesures complémentaires suivantes doivent être appliquées :

- Envoi de documents uniquement à destination d'une adresse de messagerie interne à l'entité ;
- Envoi uniquement à une seule adresse de messagerie.

3. Règles relatives à la diffusion de l'information

3.1 Limitation des destinataires

Il est recommandé d'identifier clairement les destinataires (personnes ou entités) d'un document dès les premières pages. Cette mesure vise à permettre à n'importe quelle personne en possession du document d'identifier les destinataires dudit document et de limiter sa diffusion par négligence.

3.2 Format numérique

En fonction du marquage apposé, les modalités de diffusion doivent respecter les règles suivantes :

- **« Public » ou « Non Protégé »** : Aucune mesure de chiffrement n'est obligatoire.
- **« Interne »** :
 - Pour les envois par courriel ou via des solutions de partage document (Envol, FileMI, ...), à des personnels externes au ministère : l'utilisation d'un logiciel certifié par l'ANSSI est obligatoire pour l'envoi des documents (par exemple via ACID ou Zed!) ;
 - Pour le partage de documents en visioconférence : Aucune mesure particulière n'est obligatoire ;
 - Pour les envois par courriel à des personnels internes au ministère : Aucune mesure de chiffrement particulière n'est obligatoire, mais reste une recommandation à privilégier ;
 - Pour les transferts machine à machine : L'accès aux données doit être protégé en accès aux seuls personnels du ministère.
- **« Diffusion Contrôlée » et « Diffusion Restreinte »** :
 - Pour les envois par courriel ou via des solutions de partage document (Envol, FileMI, ...) : l'utilisation d'un logiciel certifié par l'ANSSI est obligatoire pour l'envoi des documents (par exemple via ACID ou Zed!) ;
 - Pour le partage de documents en visioconférence ou via des outils de travail collaboratif : l'utilisation de solutions homologuées « Diffusion Restreinte » est obligatoire. A défaut, le support devra être échangé par courriel selon les modalités applicables.
 - Pour les transferts machine à machine :
 - Les données transmises doivent nécessairement faire l'objet de mesures de chiffrement appropriées dont il conviendra de maintenir à jour pour garantir leur robustesse dans la durée :
 - Utilisation de protocoles sécurisés (HTTPS, SFTP, ...),
 - Chiffrement des données à la source et déchiffrement par le destinataire légitime,
 - Cumul des deux mesures précédentes.
 - A défaut, la machine hébergeant les données doit être coupée de tout réseau tiers et protégée physiquement contre tout accès illégitime (local avec porte blindée, accès biométrique...).
- **« Secret »** : L'utilisation d'un poste ISIS est obligatoire pour l'échange et le partage d'information classifiée à ce niveau. Les échanges téléphoniques ou par visioconférences peuvent être réalisés par le biais des systèmes OSIRIS et HORUS.

- « **Très Secret** » : Il n'existe pas d'équivalent au poste ISIS pour la gestion de ce niveau classification. Il convient de se référer directement aux exigences de l'IGI 1300. Les échanges téléphoniques peuvent être réalisés par le biais du réseau RIMBAUD.

3.3 Format papier

Selon le marquage apposé, les modalités de diffusion des documents papiers doivent respecter les règles suivantes :

- « **Public** » ou « **Non Protégé** » : Aucune mesure de protection particulière n'est obligatoire.
- « **Interne** » : La communication des documents doit se faire de mains à mains ou par courrier sous enveloppe scellée.
- « **Diffusion Contrôlée** » et « **Diffusion Restreinte** » : La communication des documents doit se faire de mains à mains ou par courrier sous enveloppe scellée avec remise contre signature du destinataire.
- « **Secret** » ou « **Très Secret** » : la communication de documents classifiés ne peut se faire que de mains à mains. Une vérification de l'habilitation du destinataire est un préalable à la communication de documents classifiés. Le niveau d'habilitation des personnes doit être proportionné au marquage des documents classifiés traités.

La transmission par voie postale des documents sensibles sous format papier doit être effectuée sous double enveloppe : l'enveloppe intérieure portant la mention de protection et les références du document, l'enveloppe extérieure ne comportant que les indications nécessaires à la transmission. Cet envoi doit être réalisé par un moyen garantissant la bonne réception du document.

4. Règles relatives au stockage et à l'archivage de l'information

Les informations dépassant le niveau « Non Protégé » ne doivent être accessibles qu'aux seules personnes ayant le besoin d'en connaître. L'étude des scénarios de risque pouvant affecter les systèmes traitant l'information doit être réalisée conformément à la démarche d'intégration de la SSI dans les projets (DISSIP) afin d'identifier les mesures de remédiation adéquates.

Toute dérogation aux règles de stockage et de protection des informations doit être expressément validée par le CSN de l'entité.

4.1 Format numérique

En fonction du marquage apposé, les modalités de conservation doivent respecter les règles suivantes :

- « **Public** » ou « **Non Protégé** » : Aucune mesure de conservation particulière n'a besoin d'être mise en œuvre.
- « **Interne** » : Conservation des données avec une limitation des accès aux seuls agents du ministère.
 - Pour le stockage en local, sur un support amovible, sur un serveur partagé ou au sein d'un outil de gestion électronique des documents : l'utilisation d'une solution labélisée par l'ANSSI est recommandée pour le stockage des documents (par exemple via ACID ou Zed!) ;
 - Pour les systèmes d'information : Aucune mesure de chiffrement particulière n'est obligatoire, mais reste une recommandation à privilégier.

- « **Diffusion Contrôlée** » : Conservation des données de manière chiffrée par une solution certifiée par l'ANSSI.
 - Pour le stockage en local, sur un support amovible, sur un serveur partagé ou au sein d'un outil de gestion électronique des documents : l'utilisation d'une solution labélisée par l'ANSSI est obligatoire pour le stockage des documents (par exemple via ACID ou Zed!) ;
 - Pour les systèmes d'information : en fonction du besoin en confidentialité déterminé dans l'analyse de risques, l'utilisation d'un boîtier cryptographique peut être privilégiée pour chiffrer les données.
- « **Diffusion Restreinte** » : Conservation des données de manière chiffrée par une solution qualifiée par l'ANSSI.
 - Pour le stockage en local, sur un support amovible, sur un serveur partagé ou au sein d'un outil de gestion électronique des documents : l'utilisation d'une solution labélisée par l'ANSSI est obligatoire pour le stockage des documents (par exemple via ACID ou Zed!) ;
 - Pour les systèmes d'information : l'utilisation d'un boîtier cryptographique est requise pour le chiffrement de ce type de données.
- « **Secret** » : L'utilisation d'un poste ISIS est recommandée. A défaut, les exigences de l'IGI 1300 doivent obligatoirement être appliquées.
- « **Très Secret** » : Obligation de se référer aux exigences de l'IGI 1300.

4.2 Format papier

En fonction du marquage apposé, les modalités de conservation doivent respecter les règles suivantes :

- « **Public** » ou « **Non Protégé** » : Aucune mesure de conservation particulière n'a besoin d'être mise en œuvre.
- « **Interne** » : Conservation des données dans un tiroir ou une armoire fermant à clé.
- « **Diffusion Contrôlée** » : Conservation des données dans une armoire forte ou un coffre-fort.
- « **Diffusion Restreinte** » : Conservation des données dans un coffre-fort.
- « **Secret** » ou « **Très Secret** » : Ces données doivent être obligatoirement conservées dans un coffre-fort conforme aux exigences de l'IGI 1300. Toute sortie doit être tracée au travers d'une main courante gérée par l'officier de sécurité de l'entité.

Tout document potentiellement utile aux autorités administratives ou judiciaires qui en requièrent l'usage, doit réunir les trois critères suivants pour garantir sa valeur juridique :

- Le document doit être parfaitement intelligible ;
- L'auteur du document peut être dûment authentifié ;
- Le document a été établi et conservé dans des conditions de nature à en garantir l'intégrité (toute altération ou modification du document originel doit être détectable).

5. Règles relatives à la destruction de l'information

Conformément au cadre légal en vigueur, les informations ne doivent pas être conservées au-delà des durées prévues. Elles doivent être détruites à partir de moyens permettant d'éviter toute exploitation ultérieure.

Par nécessité de service, certaines informations peuvent déroger à cette exigence et être archivées de manière définitive et pérenne. Cette nécessité doit être évaluée pour chaque traitement.

Les supports (disques durs, cartes mémoire, clés USB, ...) ayant contenu des données ou informations considérées comme sensibles doivent faire systématiquement l'objet d'un effacement sécurisé par le service informatique local, selon une procédure validée par le CSN de la direction concernée, avant leur stockage temporaire dans l'attente de leur destruction.

6. Rappels des sanctions en cas de divulgation de l'information

Il est rappelé que tout auteur d'une divulgation d'informations ou de données sensibles non classifiées de défense, auprès de la sphère publique ou privée, s'expose à des sanctions disciplinaires et/ou professionnelles (Article 26 de la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires, article 226-13 du Code Pénal relatif au secret professionnel), sans préjuger de l'application éventuelle des dispositions spécifiques au traitement et à la protection de données à caractère personnel⁴.

⁴ 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.

FIN DU DOCUMENT