



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

PGSN – A03

Gestion des biens

Version 1.0

Préambule

Le présent document est une composante à part entière de la politique générale de sécurité numérique du ministère de l'Intérieur (PGSN-MI).

Les principes stratégiques de la PGSN-MI et les dispositions générales de l'instruction sont traduits au sein du présent document en objectifs à atteindre, reprenant la structure de la politique de sécurité des systèmes d'information de l'Etat (PSSI-E).

Des règles techniques ou non techniques permettant de contribuer à la réalisation de chaque objectif sont énoncées au sein du présent document :

- Les mesures préfixées par « PSSI- », suivies de la nomenclature seule, sont des règles inchangées de la PSSI de 2014. Des modifications peuvent néanmoins y être effectuées sur l'appellation de certaines fonctions propres au ministère.
- Les mesures préfixées « MI- » sont des mesures venant préciser la règle originale ou définir des règles propres au ministère de l'Intérieur, formulées par le SHFD.

Toute dérogation à un objectif ou une règle du présent document, doit se faire en conformité avec la règle [MI-ORG-PGSN-DEROG] du document [PGSN-A01] du corpus de la sécurité numérique.

Dans la suite du document, le terme « DSI ministérielles » regroupe la direction du numérique et le service des technologies et des systèmes d'information de la sécurité intérieure.

Cartographie et protection de l'information

Objectif A3-1 : cartographie des SI. Tenir à jour une cartographie détaillée et complète des SI.

PSSIE-GDB-INVENT : inventaire des ressources informatiques. Chaque entité établit et maintient à jour un inventaire des ressources informatiques sous sa responsabilité, en s'appuyant sur un outillage adapté. Cet inventaire est tenu à disposition du CSN, ainsi que du SHFD et de l'ANSSI en cas de besoin de coordination opérationnelle. Il comprend la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes. Il est constitué d'une base de données de configuration, maintenue à jour et tenue à disposition du CSN.

L'historique des attributions des biens inventoriés doit être conservé, dans le respect de la législation.

MI-GDB-CARTO : cartographie. La cartographie¹ de chaque système d'information est élaborée dans le cadre de la démarche d'homologation et contribue au maintien en condition de sécurité. Elle vise à apporter une connaissance approfondie du fonctionnement d'un SI, à faciliter la compréhension, la conception et l'implémentation des mesures de protection et ainsi à simplifier la gestion des crises cyber.

Dans le cadre de la démarche d'homologation, cette cartographie est formalisée au travers du dossier d'architecture technique du système dans lequel doit être précisé les centres informatiques, les architectures des réseaux (sur lesquelles sont identifiés les points névralgiques et la sensibilité des informations manipulées) et qualifie le niveau de sécurité attendu.

Cette cartographie doit être maintenue à jour et tenue à disposition du CSN, ainsi que du SHFD et de l'ANSSI notamment en cas de besoin de coordination opérationnelle (crise cyber).

Objectif A3-2 : qualification et protection de l'information. Qualifier l'information de façon à adapter les mesures de protection.

MI-GDB-QUALIF-SENSI : qualification des informations. La sensibilité de toute information doit être évaluée et faire l'objet d'une classification adaptée² par le service émetteur ou le responsable de traitement.

La sensibilité des données traitées par un système d'information doit être expressément formalisée (Par exemple, dans une procédure d'exploitation de la sécurité).

Pour les documents, le marquage systématique en fonction du niveau de sensibilité est obligatoire. Dans le cas d'un SIE, les rapports d'audits et les fiches de déclaration des incidents doivent se voir apposer à minima les mentions de protection « Diffusion Restreinte » et « Spécial France ». La classification des autres documents du SIE est laissée à la libre appréciation du service émetteur en fonction de ses besoins opérationnels.

¹ <https://www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation/>

² Se référer à au document [PGSN-B01] du corpus de la sécurité numérique.

MI-GDB-PROT-IS : protection des informations. L'utilisateur doit protéger les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité et tout au long de leur cycle de vie. Il appartient au service émetteur de définir les règles de protection de l'information, depuis la création du brouillon jusqu'à son éventuelle destruction, en conformité avec les mesures prévues par la réglementation applicable.

MI-GDB-PROT-TIER : protection des informations confiées à des Tiers. La qualification de l'information et son marquage doit permettre à des Tiers de connaître sans ambiguïté les règles de protection qu'il aura à appliquer conformément à la politique de classification du ministère.

MI-GDB-OUTILS-PRO : emploi de solutions ministérielles. Pour les agents permanents, les informations professionnelles doivent être traitées et stockées uniquement sur le matériel et les solutions mis à disposition ou validés par les DSI ministérielles.

Pour les agents non permanents. Il convient de privilégier l'utilisation des moyens du ministère ou, à défaut, de prévoir les clauses contractuelles permettant d'apporter les mêmes garanties. Toute utilisation de matériels personnels est proscrite.

MI-GDB-EXP-DONNEES : export de données de production vers un SI. L'export de données de production vers un système d'information tiers est limité au strict nécessaire. Les données exportées doivent être chiffrées par un dispositif respectant la règle *PSSIE-INT-AQ-PSL* du document [PGSN-A04].

Dans le cas où le système tiers est d'un niveau de sécurité inférieur au système d'information d'origine, une revue de l'homologation des deux systèmes doit être menée.

Dans le cas du transfert des données réelles d'une plateforme de production vers une préproduction (ou qualification, métrologie, test, ...), les données doivent être systématiquement anonymisées selon un procédé validé par le CSN.