



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

PGSN – A01

Politique, organisation, gouvernance

Version 1.0

NON PROTEGE

Préambule

Le présent document est une composante à part entière de la politique générale de la 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.

Organisation et gouvernance de la sécurité numérique

Objectif A1-1 : Organisation de la sécurité numérique. Mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité.

1. Organisation SN

MI-ORG-SSI : organisation SN. Une organisation dédiée à la est déployée dans toutes les directions, services, écoles, établissements publics administratifs et administrations territoriales du ministère de l'intérieur suivant les principes de l'IGI 1300¹. Cette organisation, établie selon les directives du haut fonctionnaire de défense, définit les responsabilités internes et à l'égard des tiers, les modalités de coordination avec les autorités externes, ainsi que les modalités d'application des mesures de protection. Des procédures d'applications sont écrites et portées à la connaissance de tous.

2. Acteurs SN

MI-ORG-ACT-SN : identification des acteurs. L'organisation de la sécurité numérique du ministère s'appuie sur des acteurs SN clairement identifiés, à tous ses niveaux d'organisation. Les acteurs responsables en matière de SN et les agents chargés de les assister dans cette mission sont responsables de la mise en application générale de la PGSN-MI. Ils sont expressément désignés par l'autorité compétente et référencés dans un annuaire ministériel. Cette organisation s'appuie sur le haut fonctionnaire de défense adjoint (HFDA), assisté du fonctionnaire de sécurité des systèmes d'information (FSSI).

3. Responsabilités internes

MI-ORG-CSN : désignation du CSN. Chaque autorité qualifiée de la sécurité des systèmes d'information (AQSSI) d'une direction du ministère s'appuie sur un ou plusieurs conseillers à la sécurité du numérique (CSN), chargé(s) de l'assister dans le pilotage et la gestion de la SN. Des assistants locaux (ALSN) peuvent être désignés, le cas échéant, afin de constituer un relais et appui du CSN. Les missions des CSN sont définies dans le descriptif de la chaîne fonctionnelle de sécurité numérique, présent au sein du corpus de la PGSN. Leur désignation est formalisée par un arrêté ou une note en fonction des cas. Dans tous les cas, le CSN reste responsable de l'encadrement de ses assistants locaux et doit s'assurer de la bonne exécution de leurs missions.

MI-ORG-RSSI : désignation du RSSI. Chaque responsable d'un service opérationnel numérique s'appuie sur un ou plusieurs responsables de la sécurité des systèmes d'information, chargé(s) de l'assister dans la mise en œuvre opérationnelle de la sécurité numérique. Le RSSI conseille techniquement les autorités et les CSN dans la mise en œuvre opérationnelle de la sécurité numérique. Des assistants locaux (ALSSI) peuvent être désignés, le cas échéant, afin de constituer un relais et appui du RSSI. Les

¹ Instruction générale interministérielle n°1300/SGDSN/PSE/PSD du 9 août 2021 sur la protection du secret de la défense nationale.

missions des RSSI sont définies dans le descriptif de la chaîne opérationnelle de sécurité numérique, présent au sein du corpus de la PGSN. Leur désignation est formalisée par un arrêté ou une note en fonction des cas. Dans tous les cas, le RSSI reste responsable de l'encadrement de ses assistants locaux et doit s'assurer de la bonne exécution de leurs tâches.

MI-ORG-RESP : formalisation des responsabilités. Une note d'organisation interne précise la mise en œuvre de la PGSN-MI à l'échelle de la structure et fixe la répartition des responsabilités et rôles en matière de sécurité numérique au sein de chaque entité et au niveau local. Cette note sera, le plus souvent, proposée par le CSN et validée par l'autorité hiérarchique responsable du périmètre concerné.

MI-ORG-SEP : séparation des tâches. Les tâches et les domaines de responsabilité incompatibles doivent être séparés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des ressources. C'est notamment le cas de la délivrance des moyens d'accès et des autorisations associées aux ressources.

MI-ORG-REL-AUT : relations avec les autorités. Le SHFD est en charge, pour le ministère, des relations avec l'ANSSI. Le délégué ministériel à la protection des données (DMPD) est en charge, pour le ministère, des relations avec la CNIL.

4. Responsabilités vis-à-vis des tiers

MI-ORG-TIERS : gestion contractuelle des tiers. Le CSN coordonne les actions permettant l'intégration des clauses liées à la sécurité numérique dans tout contrat ou convention impliquant un accès par des tiers à des informations ou à des ressources informatiques. A ce titre, il veille à intégrer les exigences et recommandations en s'appuyant sur le document [PGSN-E01] du corpus de sécurité numérique de la PGSN-MI.

Le CSN veille également à ce que soient organisées des revues régulières de l'application de ces clauses.

5. PGSN ministérielle

MI-ORG-PIL-PGSN-MI : définition et pilotage de la PGSN ministérielle. La PGSN-MI est placée sous la responsabilité du HFD. Cette politique reprend le socle commun établi par la PSSIE. La PGSN-MI s'applique à toutes entités du ministère de l'Intérieur ou placées sous sa tutelle, qui doivent la décliner pour leur propre périmètre. L'entité est alors responsable de sa mise à place, de son évolution, de son suivi et de son contrôle.

MI-ORG-PGSN-DEROG : dérogation à une des règles de la PGSN. Toute dérogation à l'une des règles de la PGSN ou d'une doctrine de sécurité du ministère doit être formellement approuvée par l'AQSSI. Cette approbation peut apparaître directement dans la décision d'homologation du système concerné. Il est également vivement recommandé de justifier dans la stratégie d'homologation les raisons détaillées pour lesquelles une règle de sécurité de la PGSN-MI ne sera pas respectée.

6. Application des mesures de sécurité au sein de l'entité

MI-ORG-APP-INSTR : application de l'instruction dans l'entité. Le CSN ou le RSSI planifie les actions de mise en application de la PGSN-MI. Il rend compte régulièrement de la mise en application des mesures de sécurité auprès de son autorité et du SHFD. En cas d'écart ou de non-conformité, le CSN ou le RSSI propose à son autorité actions, en lien avec les équipes métiers, un plan d'action en priorisant les en fonction de leur efficacité face aux risques, leur complexité de réalisation et leur coût budgétaire.

MI-ORG-APP-DOCS : plan d'application. Le CSN ou le RSSI formalise et tient à jour le plan d'action en application de la PGSN-MI sur son périmètre. Ce document est approuvé par l'autorité qualifiée de l'entité notamment en vue de la prise en compte des mesures ayant un impact budgétaire et humain lors des dialogues de gestion. Le cas échéant, il s'appuie sur des assistants locaux pour les actions de sensibilisation et de contrôle de ce plan d'application.