



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

PGSN-MI

**Organisation du corpus
de la sécurité numérique**

Version 1.0

NON PROTEGE

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 vise à clarifier l'organisation du corpus documentaire de la sécurité numérique du ministère de l'Intérieur. A ce titre, il constitue le document socle de tous les livrables amenés à compléter ce corpus.

Organisation du corpus de la sécurité numérique

Le corpus de sécurité numérique, de par la pluralité des sujets qu'il peut être amené à traiter, est scindé en plusieurs catégories. Chaque catégorie permet de séparer les éléments du corpus en fonction des thématiques abordées ou du niveau de granularité du document (exigences obligatoires, préconisations, principes stratégiques, procédures opérationnelles, etc.).

1. Catégorie A - Documents applicables concernant les objectifs et règles élémentaires de sécurité

Cette catégorie regroupe les exigences de la PSSI-E déclinées dans le contexte du ministère de l'Intérieur. Aucune des modifications apportées n'a pour objectif de déroger aux exigences de la PSSI-E, elles visent dans la très grande majorité des cas à durcir les exigences en conformité avec les enjeux spécifiques du ministère en matière de sécurité numérique.

Les documents constitutifs de cette catégorie sont les suivants :

- [PGSN-A01]. Exigences d'organisation et gouvernance permettant la mise en application de la PGSN.
- [PGSN-A02]. Exigences relatives au recrutement, à la sensibilisation et à la formation des agents, permanents ou non, du ministère.
- [PGSN-A03]. Exigences relatives à la cartographie des SI, l'inventaire des ressources et la qualification de l'information.
- [PGSN-A04]. Exigences relatives à la gestion des risques et des homologations.
- [PGSN-A05]. Exigences relatives à la sécurité des locaux et des centres informatiques.
- [PGSN-A06]. Exigences relatives aux usages, accès et mécanismes des réseaux du ministère.
- [PGSN-A07]. Exigences relatives pour la conception et la mise en œuvre des systèmes d'information du ministère.
- [PGSN-A08]. Exigences relatives aux procédures d'exploitation de la sécurité à mettre en place. Ce document aborde des exigences majeures sur la protection des informations sensibles, la sécurité des ressources, la gestion des habilitations et des accès, les revues de compte et de configuration, etc.
- [PGSN-A09]. Exigences relatives à la sécurité du poste de travail, que ce soit dans l'enceinte du ministère ou en nomadisme.
- [PGSN-A10]. Exigences relatives à la sécurité du développement des systèmes, permettant d'inclure la notion de risque dès la phase de conception des systèmes d'information (concept dit de « Security by design »).
- [PGSN-A11]. Exigences relatives au traitement des incidents de sécurité.
- [PGSN-A12]. Exigences relatives à la continuité des activités des SI.
- [PGSN-A13]. Exigences relatives aux audits.

2. Catégorie B - Documents opérationnels de la PGSN

Cette catégorie regroupe les documents faisant office de doctrines opérationnelles dans l'application des règles élémentaires de sécurité ou détaillant certains points spécifiques de la PGSN sur la gestion des acteurs de la sécurité numérique.

A ce titre, les documents de cette catégorie visent à lever toute ambiguïté sur certaines règles ou attentes du ministère sur certains thèmes précis de la sécurité numérique.

Les documents constitutifs de cette catégorie sont les suivants :

- [PGSN-B01]. Missions des acteurs de la sécurité numérique.
- [PGSN-B02]. Classification, marquage et traitement de l'information.
- [PGSN-B03]. Exigences spécifiques aux systèmes d'information essentiels.
- [PGSN-B04]. Exigences spécifiques au périmètre de l'Administration Territoriale de l'Etat.
- [PGSN-B05]. Dispositif opérationnel et plan ministériel de gestion de crise cyber.

3. Catégorie C - Documents spécifiques à certains périmètres du ministère

Cette catégorie liste l'ensemble des politiques de sécurité numérique des entités du ministère. Ces politiques visent à détailler l'organisation, la gouvernance et les exigences spécifiques applicables.

Les documents constitutifs de cette catégorie sont les suivants :

- [PGSN-C01]. Politique spécifique au périmètre de l'ATE.
- [PGSN-C02]. Politique spécifique au périmètre de la Police Nationale. < A venir >
- [PGSN-C03]. Politique spécifique au périmètre de la Gendarmerie Nationale. < A venir >

4. Catégorie D - Démarche d'intégration de la sécurité des SI dans les projets (DISSIP)

Cette catégorie est exclusive à la Démarche historique du ministère permettant de guider les équipes projets dans le processus d'homologation de leur système d'information. A ce titre, la DISSIP permet une mise en pratique de la gestion des risques et une revue de conformité des exigences de la PGSN.

Les documents constitutifs de cette catégorie sont les suivants :

- [PGSN-D01]. Présentation de la démarche.
- [PGSN-D02]. Métriques de la démarche.
- [PGSN-D03]. Note d'orientation permettant de déterminer la sensibilité du SI et les livrables nécessaires à son homologation.

La DISSIP et son corpus sont publiés à l'adresse : <http://ssi.minint.fr>

5. Catégorie E - Documents de bonnes pratiques de sécurité numérique

Cette catégorie vise à regrouper les bonnes pratiques de sécurité dont l'application est fortement recommandée. Ces documents ont vocation à apporter conseil et assistance sur certains thèmes précis mais n'ont pas vocation à être force de loi.

Cette catégorie permet également de regrouper les offres de services propres au ministère en matière de sécurité numérique.

Les documents constitutifs de cette catégorie sont les suivants :

- [PGSN-E01]. Clauses de sécurité types des marchés publics ou accords-cadres.
- [PGSN-E02]. Préconisations à la mise en place d'un programme de Bug Bounty.
- [PGSN-E03]. Rapport annuel Type - Etat des lieux de la sécurité numérique. < A venir >
- [PGSN-E04]. Offre de service « Bilan de Maturité Cyber ». < A venir >