



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

PGSN – A04

**Intégration de la SN dans le cycle de vie
des systèmes d'information**

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).

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-E », suivies de la nomenclature seule, sont des règles inchangées de la PSSI-E 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.

Intégration et suivi de la sécurité numérique

1. Gestion des risques et homologation

Objectif A4-1 : risques. Apprécier, traiter, et communiquer sur les risques relatifs à la sécurité des systèmes d'information.

MI-INT-HOMOLOG-SI : Homologation des systèmes d'information. Tout système d'information doit faire l'objet d'une décision d'homologation de sécurité avant sa mise en service opérationnel, dans les conditions d'emploi définies par l'autorité responsable du traitement. L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité définis dans l'analyse de risques¹, conformément à la démarche d'intégration de la SSI dans les projets (DISSIP)² du ministère dont l'application doit être systématique pour toute procédure d'homologation d'un système d'information.

La décision d'homologation, qui précise les conditions d'emploi et les plans d'action à suivre, est prise par l'autorité d'homologation qui peut s'appuyer sur l'avis d'une commission d'homologation.

Pour tous les systèmes d'information en production non homologués, une décision d'homologation doit être formalisée dans les 3 ans à compter de la date d'entrée en vigueur de la PGSN-MI.

MI-INT-HOMOLOG-AVIS : Avis du SHFD pour l'homologation des SI. Le SHFD, membre de droit de la commission d'homologation, doit obligatoirement disposer du dossier d'homologation au minimum 1 mois avant la tenue de la commission. Ce délai est nécessaire pour que le SHFD formalise sa position sur le fond du dossier d'homologation et la pertinence des éléments d'aide à la décision proposés à l'autorité d'homologation.

Pour tous les SIE, un avis négatif du SHFD fait autorité et ne peut en aucun cas être considéré comme consultatif pour leur homologation. Dans tous les cas, le haut fonctionnaire de défense rend compte au ministre de l'intérieur de tout traitement pouvant faire peser un risque inacceptable pour le ministère.

MI-INT-HOMOLOG-REF : Homologation de référence. Certains systèmes, conçus et développés par une autorité, peuvent être instanciés et mis en œuvre dans différentes entités du ministère. Il peut s'agir par exemple d'offre de service d'infrastructure (téléphonie, réseau, etc.). L'autorité d'homologation reste unique et signe alors une décision d'homologation dite « *de référence* ». Cette dernière doit être accompagnée d'une déclaration d'applicabilité référençant l'ensemble des dispositions et des mesures de sécurité dont les autorités locales devront attester de la bonne mise en œuvre.

En cas de difficultés ou de non-conformité, l'autorité locale doit en informer sans délai l'autorité d'homologation afin soit de mettre en œuvre des mesures de substitution équivalentes, soit solliciter une homologation provisoire (délivrée par l'AH) dans l'attente de la mise en œuvre des mesures de protection dans des délais contraints, soit d'en interdire son déploiement.

¹ <https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/>

² L'ensemble des documents de la DISSIP est disponible sur le site : <http://ssi.minint.fr/>

MI-INT-HOMOLOG-TIERS : homologation des SI tiers. Si un projet s'appuie sur un système d'information transverse ou sur une offre de service applicative, l'autorité d'homologation doit s'assurer que ces briques soient dûment homologuées et leurs niveaux de sécurité conformes à celui du projet en cours d'homologation. Pour ce faire, le sous-traitant doit communiquer à l'autorité d'homologation une synthèse des risques résiduels, ainsi que les éventuels plans d'action associés visant à les réduire (le cas échéant, la décision d'homologation doit également être communiquée).

2. Maintien en condition de sécurité des systèmes d'information

Objectif A4-2 : maintien en condition de sécurité. Gérer dynamiquement les mesures de protection, tout au long de la vie du SI.

PSSIE-INT-SN : intégration de la sécurité dans les projets. La sécurité numérique doit être prise en compte dans toutes les phases des projets informatiques, sous le contrôle de l'autorité d'homologation, de la conception et de la spécification du système jusqu'à son retrait du service.

MI-INT-QUOT-SN : mise en œuvre au quotidien de la SN. La sécurité numérique se traite au quotidien par des pratiques d'hygiène informatique. Des procédures écrites définissent les actes élémentaires du maintien en condition de sécurité (MCS) lors des phases de conception, évolution ou retrait d'un système. Dans des cas de sous-traitance, les supports contractuels doivent prévoir les conditions de ce MCS.

MI-INT-MCS : utilisation de produits à jour. L'ensemble des produits matériels et logiciels déployés doivent obligatoirement faire l'objet d'un support éditeur. Un processus technique de déploiement des correctifs de sécurité, notamment en cas d'urgence, est obligatoirement défini dans les procédures d'exploitation et de sécurité.

PSSIE-INT-TDB : créer un tableau de bord SN. Un tableau de bord de la sécurité numérique est mis en place et tenu à jour par les CSN. Il leur permet de fournir aux autorités une vision générale du niveau de sécurité et de son évolution, rendant ainsi plus efficace le pilotage de la SN. Au niveau stratégique, le tableau de bord SN permet de suivre l'application de la politique de sécurité et de disposer d'éléments propres à qualifier les ressources devant être allouées à la SN.

Au niveau du pilotage, la mise en place de ce tableau de bord permet de contrôler la réalisation d'objectifs opérationnels, d'améliorer la qualité de service et de détecter au plus tôt les retards dans la réalisation de certains objectifs de sécurité.

3. Produits et services labellisés

Objectif A4-3 : produits et services qualifiés ou certifiés. Utiliser des produits et services dont la sécurité est évaluée et attestée selon des procédures reconnues par l'ANSSI, afin de renforcer la protection des SI.

MI-INT-AQ-PSL : acquisition de produits et services de confiance. Lorsqu'ils sont disponibles, des produits ou des services de sécurité labellisés (certifiés, qualifiés) par l'ANSSI doivent être utilisés³. Il convient de prioriser l'emploi de produits ou services qualifiés et, à défaut, prioriser ceux certifiés.

³ <https://www.ssi.gouv.fr/liste-produits-et-services-qualifies/>

MI-INT-AQ-CPSNL : choix de produits et services de confiance non labellisés. Dans le cas où n'existe pas de produit ou de service labellisé (certifié, qualifié) par l'ANSSI pour le besoin concerné, le SHFD et les DSI ministérielles doivent être sollicités pour avis.

4. Gestion des prestataires

Objectif A4-4 : maîtrise des prestations. Veiller aux exigences de sécurité lorsqu'il est fait appel à de la prestation par des tiers.

MI-INT-PRES-CS : clauses de sécurité. Toute prestation dans le domaine des SI doit être encadrée par des clauses de sécurité et qualité. Ces clauses spécifient les mesures de sécurité que le prestataire doit respecter dans le cadre de ses activités et les processus qu'il met en œuvre pour garantir la qualité des éléments produits. Un plan d'assurance sécurité (PAS) peut être exigé dans les accords contractuels avec les sous-traitants afin de s'assurer que les mesures qu'ils mettent en place permettent de répondre aux exigences de l'administration en termes de disponibilité, intégrité, confidentialité et traçabilité⁴.

PSSIE-INT-PRES-CNTRL : suivi et contrôle des prestations fournies. Le maintien d'un niveau de sécurité au cours du temps nécessite un double contrôle :

- L'un, effectué périodiquement par l'équipe encadrant la prestation, qui porte sur les actions du sous-traitant et la conformité au cahier des charges ou au plan d'assurance sécurité ;
- L'autre, effectué par une équipe externe, qui porte sur la pertinence du cahier des charges en amont des projets, la conformité des réponses apportées par le sous-traitant en phase de recette et le niveau de sécurité global obtenu en production.

Chaque contrôle peut inclure une revue du plan d'assurance sécurité du sous-traitant.

PSSIE-INT-REX-AR : analyse de risques. Toute opération d'externalisation s'appuie sur une analyse de risques préalable, de façon à formaliser des objectifs de sécurité et définir des mesures adaptées. L'ensemble des objectifs de sécurité ainsi formalisés permet de définir une cible de sécurité servant de cadre au contrat établi avec le prestataire.

MI-INT-REX-HB : hébergement. Les données du ministère de l'Intérieur identifiées comme sensibles doivent être hébergées par des offres de services validées par les DSI ministérielles, sous réserve qu'elles soient homologuées et que leur niveau de sécurité soit conforme aux enjeux de sécurité du traitement, notamment en matière de gestion de crise cyber.

Dans tous les cas, l'hébergement des données du ministère doit être réalisé sur le territoire national, sauf accord du HFD et dérogation dûment motivée et précisée dans la décision d'homologation. Cette règle s'étend aux sauvegardes, aux infrastructures de supervision et d'administration des prestataires.

MI-INT-REX-HS : hébergement et clauses de sécurité. Pour les informations non sensibles, tout contrat d'hébergement externalisé détaille les dispositions mises en œuvre pour prendre en compte la sécurité numérique. Ce sont notamment les mesures prises pour vérifier la prise en compte des besoins de sécurité du projet, s'assurer du maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace (conditions d'accès aux journaux, mise en place d'astreintes, etc.) lors de l'intervention par le C2MI.

⁴ Se référer à au document [PGSN-B02] du corpus de la sécurité numérique.

MI-INT-PRES-CLOUD : recours aux prestataires de service d'informatique en nuage. La politique ministérielle relative aux technologies d'informatique en nuage n'autorise l'hébergement des informations sensibles du ministère qu'aux seules offres de services labélisées, conformément au référentiel *SecNumCloud* de l'ANSSI⁵.

MI-INT-PRES-LOC : localisation des prestataires. Les personnels employés par des tiers pour l'administration, l'exploitation ou la supervision des systèmes d'information traitant de données sensibles du ministère doivent obligatoirement être localisés sur le territoire national.

⁵ <https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/>