



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

PGSN – A02

Ressources humaines

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-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.

Gestion des ressources humaines

Objectif A2-1 : ressources humaines. Faire des personnes les maillons forts des SI du ministère de l'Intérieur.

1. Utilisateurs

PSSIE-RH-SSI : charte d'application SN. Une charte d'application de la politique générale de sécurité numérique, récapitulant les mesures pratiques d'utilisation sécurisée des ressources informatiques et élaborée sous le pilotage de la chaîne fonctionnelle SN, est communiquée à l'ensemble des agents de chaque entité. Cette charte doit être opposable juridiquement et, si possible, intégrée au règlement intérieur de l'entité. Le personnel non permanent (stagiaires, intérimaires, prestataires...) est informé de ses devoirs dans le cadre de son usage des SI de l'État.

MI-RH-SAN : Sanctions. La charte d'application de la politique générale de sécurité numérique, pour toute personne permanente ou non permanente, doit préciser les sanctions civiles et pénales qui peuvent être encourues en cas de violation des législations et réglementations applicables en matière de sécurité numérique.

MI-RH-SENS : Sensibilisation régulière et contrôlée. Les CSN doivent mettre en place et maintenir des plans de sensibilisation adaptés, afin de maintenir la vigilance des personnels sur la sécurité numérique. Les CSN, ALSN et RSSI doivent mettre en place des moyens permettant de mesurer l'efficacité des actions de sensibilisation à la sécurité numérique.

2. Personnel permanent

MI-RH-MOTIV : choix et sensibilisation des personnes tenant les postes clés de la SN. Une attention particulière doit être portée au recrutement des personnes clés contribuant à la sécurité des systèmes d'information du ministère : CSN, assistants SSI locaux et administrateurs des SI. Les CSN et leurs assistants locaux doivent être spécifiquement formés à la sécurité numérique.

Les administrateurs des SI doivent être régulièrement sensibilisés aux devoirs liés à leur fonction, et doivent veiller à respecter les règles d'hygiène informatique dans leur domaine de compétence et les exigences de sécurité particulières dans leurs activités quotidiennes. Pour ce faire, la section « conseil, assistance, formation » du SHFD propose des cursus de formation adaptés aux emplois de la SN.

MI-RH-AUTORITE : sensibilisation des autorités à la SSI. Dans le cadre de leurs missions et au vu de leurs responsabilités, une sensibilisation adaptée doit être dispensée aux autorités lors de leur prise de fonction. Pour les directeurs généraux et centraux, le service du haut fonctionnaire de défense est en charge de cette mission d'information en collaboration avec les cabinets et les CSN.

MI-RH-CONF : personnels de confiance. Toutes les personnes manipulant des informations sensibles, notamment celles relevant du secret de la défense nationale, doivent le faire avec une attention et une probité particulière, dans le respect du cadre légal applicable. Les sanctions éventuelles s'appliquant aux cas de négligence ou de malveillance leur sont rappelées, dans la charte d'utilisation signée antérieurement.

MI-RH-HABILIT : habilitation des agents permanents. Les agents ayant accès à un nombre important d'informations sensibles, voire « Diffusion Restreinte », ou ceux dont les missions touchent à la protection du secret de la défense nationale, sont référencés dans le catalogue d'emploi de l'entité et doivent être habilités conformément à l'IGI 1300¹. Le nombre de personnes habilitées pour des opérations d'administration doit être connu de l'autorité, de l'officier de sécurité et du CSN. En particulier, les administrateurs de systèmes d'information intervenant sur un SIE, doivent pouvoir être habilités au premier niveau de classification de l'IGI 1300.

MI-RH-UTIL : sensibilisation des utilisateurs des systèmes d'information. Afin de contribuer à promouvoir la culture de la sécurité du numérique, les CSN organisent régulièrement des sensibilisations à la SSI pour les agents et en particulier pour les nouveaux arrivants. Chaque utilisateur est régulièrement informé des exigences de sécurité le concernant et motivé à leur respect. Il doit être formé également à l'utilisation des outils de travail conformément aux règles SSI. D'autres supports peuvent être utilisés en complément par le CSN (notes, vidéo, mail, etc.).

3. Mouvement de personnel

MI-RH-MOUV : gestion des arrivées, des mutations et des départs. Une procédure permettant de gérer les arrivées, les mobilités, les mutations et les départs des collaborateurs dans le SI doit être formalisée, appliquée strictement et mise à jour régulièrement. Cette procédure doit couvrir au minimum :

- La gestion/révocation des comptes (utilisateurs, administrateurs, services, ...) et des droits d'accès aux SI, y compris pour les partenaires et les prestataires externes ;
- La gestion du contrôle d'accès aux locaux ;
- La gestion des équipements nomades ou mobiles ;
- La gestion du contrôle des habilitations.

La liste des personnels issue de cette procédure doit être maintenue à jour et tenue à disposition du SHFD et de l'ANSSI, notamment en cas de besoin de crise cyber. Cette recommandation est obligatoire pour les SIE du ministère.

MI-RH-REVUE : revue des personnels. Une revue des personnels du SI doit être réalisée a minima annuellement. Il convient qu'un procès-verbal apportant la preuve de cette revue soit réalisé afin de pouvoir être présenté lors d'éventuels audits.

4. Personnel non permanent

MI-RH-NPERM : gestion du personnel non permanent (stagiaires, intérimaires, prestataires ...). Les règles de la PGSN-MI s'appliquent à tout personnel non permanent utilisateur d'un SI du ministère. Les dispositions contractuelles régissant l'emploi de ce personnel et intégrant les problématiques SSI sont amendées à la commande publique et au contrat. Pour tout personnel non permanent, un tutorat par un agent permanent (CSN, ALSN, ...) est mis en place afin de le sensibiliser à la sécurité numérique et de l'informer des règles en vigueur. Le CSN contrôle régulièrement l'application de ces règles.

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

MI-RH-NPERM_HABILIT : habilitation des agents non permanents. Les agents non permanents ayant accès à un nombre important d'informations sensibles, voire Diffusion Restreinte, ou ceux dont les missions touchent à la protection du secret de la défense nationale doivent être habilités conformément à l'IGI 1300. Le nombre de personnes habilitées pour des opérations d'administration doit être connu de l'autorité, de l'officier de sécurité et du CSN. En particulier, les administrateurs de systèmes d'information intervenant sur un SIE, doivent pouvoir être habilités au premier niveau de classification de l'IGI 1300.

MI-RH-NPERM-SITE : accès physique du personnel non permanent (stagiaires, intérimaires, prestataires ...). Tout personnel non permanent devant accéder ponctuellement à un site du ministère doit être accompagné par un agent du ministère. Pour le personnel non permanent devant travailler pour une durée plus ou moins longue sur un site ministériel, une demande d'autorisation d'accès doit être réalisée.

5. Relations avec des groupes externes.

MI-RH-REL-GTS : relations avec des groupes de travail spécialisés. Tout acteur SN est libre de se mettre en relation avec des groupes ou forums spécialisés dans la sécurité numérique sous réserve que celles-ci soient appropriées et validées par son autorité hiérarchique. Tout acteur SN a un devoir de discrétion et de loyauté vis-à-vis du ministère, particulièrement lors des échanges qu'il pourrait avoir avec ces groupes.

MI-RH-COM-MEDIA : Communications médiatiques. Tout échange auprès d'organes de presse, sous quelque forme que ce soit, sans autorisation formelle de la DICOM, est strictement proscrit.