



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

PGSN – A09

Sécurité du poste de travail

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.

Sécurité du poste de travail

Objectif A9-1 : sécurisation des postes de travail. Durcir les configurations des postes de travail en protégeant les utilisateurs.

1. Sécurisation du poste de travail

1.1. Mise à disposition du poste

MI-PDT-GEST : fourniture et gestion des postes de travail. Les postes de travail utilisés dans le cadre professionnel sont fournis et gérés par l'équipe locale chargée des SI suivant les consignes et les procédures définies par les DSI ministérielles pour les postes Windows et Linux. Il en est de même pour tout support amovible et compte de connexion nominatif afin de garantir la traçabilité des actions.

MI-PDT-ID-UNI : identification unique des postes de travail. Tout poste de travail doit se voir attribuer un identifiant unique. Une étiquette apposée sur le poste doit rappeler cet identifiant.

MI-PDT-INV : inventaire des postes de travail. Tous les postes de travail doivent faire l'objet d'un inventaire permettant d'identifier l'utilisateur du poste. Dans le cas où le poste de travail est directement fourni par une DSI ministérielle, l'inventaire doit également identifier l'entité attributaire.

PSSIE-PDT-CONFIG : formalisation de la configuration des postes de travail. Une procédure formalisée de configuration des postes de travail est établie par chaque entité, conformément aux directives nationales existantes.

MI-PDT-LOG-AUTO : systèmes et logiciels autorisés. Le CSN doit maintenir la liste des systèmes d'exploitation autorisés sur les terminaux, en fonction de leur typologie. De même, un catalogue des logiciels autorisés est maintenu afin de diminuer les problèmes d'interopérabilité et une sécurité SI accrue.

1.2. Sécurité physique des postes de travail

PSSIE-PDT-VEROUIL-FIXE : verrouillage de l'unité centrale des postes fixes. Lorsque l'unité centrale d'un poste fixe est peu volumineuse, donc susceptible d'être facilement emportée, elle doit être protégée contre le vol par un système d'attache (par exemple un câble antivol).

PSSIE-PDT-VEROUIL-PORT : verrouillage des postes portables. Un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs doivent être sensibilisés à son utilisation.

1.3. Réaffectation du poste et récupération d'informations

MI-PDT-REAFFECT : réaffectation du poste de travail. Une procédure doit définir les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur les postes réaffectés. En aucun cas, les postes de travail ne doivent être réaffectés à des personnes ou des services externes au ministère de l'intérieur sans en extraire préalablement les supports de stockage.

1.4. Gestion des privilèges sur les postes de travail

MI-PDT-PRIVIL : privilèges des utilisateurs sur les postes de travail. La gestion des privilèges des utilisateurs sur leurs postes de travail doit suivre le principe du « moindre privilège » : chaque utilisateur ne doit disposer que des privilèges strictement nécessaires à la conduite des actions relevant de sa mission.

PSSIE-PDT-PRIV : utilisation des privilèges d'accès « administrateur ». Les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant.

PSSIE-PDT-ADM-LOCAL : gestion du compte « administrateur local ». L'accès au compte « administrateur local » sur les postes de travail doit être strictement limité aux équipes en charge de l'exploitation et du support sur ces postes de travail. Pour les solutions Microsoft, le mécanisme de protection LAPS doit être mis en œuvre.

MI-PDT-BIOS-ACCES : protection contre l'accès au BIOS. L'accès au BIOS ou à l'UEFI, ainsi que leur paramétrage, ne doit pas être possible pour les personnels permanents et non-permanents non autorisés.

MI-PDT-MACRO : Exécution automatique de tâches dans les outils bureautiques. Les fonctions d'exécution automatique de tâches (ou « macro ») présentent dans les outils bureautiques doivent systématiquement faire l'objet d'un consentement de l'utilisateur avant exécution.

1.5. Protection des informations

MI-PDT-STOCK : stockage des informations. Dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences des entités et en accord avec les règles de sécurité en vigueur, selon les recommandations de l'ANSSI. Des droits d'accès sont prévus pour n'autoriser uniquement que les personnes ayant le besoin d'en connaître.

PSSIE-PDT-SAUV-LOC : sauvegarde / synchronisation des données locales. Dans le cas où des données doivent être stockées en local sur le poste de travail, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs.

PSSIE-PDT-PART-FIC : partage de fichiers. Le partage de répertoires ou de données hébergées localement sur les postes de travail n'est pas autorisé.

PSSIE-PDT-SUPPR-PART : suppression des données sur les postes partagés. Les données présentes sur les postes partagés (portable de prêt, par exemple) doivent être supprimées entre deux utilisations, dès lors que les utilisateurs ne disposent pas du même besoin d'en connaître.

MI-PDT-AMOV : fourniture de supports de stockage amovibles. Les supports de stockage amovibles (clés USB et disque durs externes, notamment) doivent être uniquement fournis aux utilisateurs par l'équipe locale chargée des SI. Les supports extérieurs sont interdits, sauf après vérification par l'équipe locale en étroite collaboration avec le CSN. Pour faciliter la gestion des supports amovibles et renforcer la protection des postes de travail, les services locaux sont invités à mettre en œuvre la solution de verrouillage des clés USB par GPO proposée par les DSI ministérielles.

MI-PDT-CHIFF-SENS : chiffrement des données sensibles. Les solutions de chiffrement labélisées par l'ANSSI, agréées au niveau « Diffusion Restreinte », doivent être mises à disposition des utilisateurs et des administrateurs afin de chiffrer les données sensibles stockées sur les postes de travail, les serveurs, les espaces de travail ou les supports amovibles.

Ces solutions doivent notamment permettre :

- Le chiffrement intégral du disque dur (ou chiffrement surfacique) ;
- Le chiffrement des données stockées dans les répertoires et sous-répertoires associés (incluant le cas des serveurs de partage) ;
- Le chiffrement des données communiquées par courriel, via des plateformes de partage (Par exemple : Envol, FileMI, ...) ou des supports amovibles.

Toute solution doit, quand cela est possible, être configurée pour utiliser la carte agent du ministère.

Ces solutions doivent être mises en œuvre à travers les infrastructures de gestion centralisée des DSI ministérielles.

MI-PDT-DECONT : décontamination des supports de stockage amovibles. Pour les supports de stockage amovibles dont la confiance n'est plus garantie, toute connexion aux postes de travail est proscrite sans passage préalable par une station de décontamination. En cas de doute, il convient de se tourner vers l'équipe locale chargée des SI.

MI-PDT-USB : interdiction de connecter un support USB non autorisé sur un ordinateur professionnel. Il est interdit de connecter un support ou câble USB non autorisé pour charger un matériel (téléphone, cigarette électronique...) sur un appareil professionnel. Seuls des câbles de charge uniquement (pas d'échange de données) sont admissibles, vérifiés au préalable par le service local SIC de l'entité.

MI-PDT-MAIL : interdiction d'utiliser une boîte mail personnelle. Pour éluder tout risque de compromission d'information sensible, toute utilisation de boîtes mails personnelles est proscrite. A ce titre, il est interdit de rediriger (automatiquement ou non) les mails professionnels issus de la messagerie du ministère vers des boîtes mails personnelles.

MI-PDT-DEP-MSJ : déploiement des mises à jour sécurité. Les mises à jour des systèmes et des logiciels du catalogue doivent être déployées automatiquement, y compris dans le cas d'utilisation des postes en nomadisme et des postes dédiés pour des activités de sécurité, d'administration ou de développement.

MI-PDT-NAV-WEB : configuration des navigateurs Web. Le ministère doit maintenir la liste des navigateurs web autorisés, par typologie de poste. La configuration de ces navigateurs doit être imposée et relative au type de terminal (poste de travail, mobile, etc.). Un utilisateur ne doit pas être en mesure de modifier cette configuration.

MI-PDT-VEILLE : mise en veille des terminaux. Une durée de verrouillage automatique des terminaux doit être fixée au bout d'une certaine période d'inactivité. Celle-ci doit être inférieure à 15 minutes. Elle peut être réduite en fonction du type de terminal et de la nature et sensibilité des informations manipulées et stockées par le terminal. Cette durée ne doit pas être modifiable par l'utilisateur.

MI-PDT-PMAD : prise en main à distance des postes de travail. La prise en main à distance des terminaux doit se faire impérativement avec l'accord de l'utilisateur et implique une action manuelle de

sa part pour valider l'opération. L'outil utilisé pour la prise en main à distance doit être autorisé par le CCT et le cas échéant, validé par le CSN.

MI-PDT-TRACE : traçabilité des actions sur le terminal. Une journalisation des événements doit être en place afin de permettre une analyse des activités d'un terminal, si nécessaire. Tous les logs doivent être conservés un an et être protégés contre tout accès ou modification non autorisé.

1.6. Nomadisme

MI-PDT-NOMAD-ACCESS : accès à distance aux Systèmes d'Information de l'entité. Les accès à distance aux SI de l'entité (accès dits « nomades ») doivent être réalisés via la solution homologuée par les DSI ministérielles.

Lorsque l'accès à distance utilise d'autres infrastructures, l'usage de réseaux privés virtuels (VPN) de confiance, utilisant le protocole IPSec est nécessaire. Lorsque l'accès est réalisé par des prestataires, des clauses contractuelles, validées par le CSN, doivent permettre de garantir la sécurité des accès et le durcissement des postes utilisés.

MI-PDT-NOMAD-INTERCO : interdiction de connexion des postes. Il est interdit de connecter son ordinateur portable professionnel, disjoint des solutions nomades homologuées par les DSI ministérielles, sur un autre réseau que celui du ministère de l'Intérieur. Les connexions par câble croisé sur un autre équipement sont également interdites.

PSSIE-PDT-NOMAD-PAREFEU : pare-feu local. Un pare-feu local conforme aux directives nationales doit être installé sur les postes nomades. Ce pare-feu local doit être configuré pour interdire toutes connexions entrantes sur le poste, sauf celles explicitement autorisées par les DSI ministérielles à des fins de gestion, et autoriser tous les flux sortants.

PSSIE-PDT-NOMAD-STOCK : stockage local d'information sur les postes nomades. Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement labellisé.

MI-PDT-NOMAD-FILT : filtre de confidentialité. Pour les dispositifs nomades manipulant des données sensibles (ordinateur, tablette NEO ou téléphone ERCOM), un filtre de confidentialité doit être fourni et être positionné sur l'écran dès lors que l'appareil est utilisé en dehors de l'entité.

PSSIE-PDT-NOMAD-CONNEX : configuration des interfaces de connexion sans fil. Pour tous les postes de travail du ministère, la configuration des interfaces de connexion sans fil doit interdire les usages dangereux de ces interfaces.

PSSIE-PDT-NOMAD-DESACTIV : Désactivation des interfaces de connexion sans fil. Des règles de configuration des interfaces de connexion sans fil (Wifi, Bluetooth, 4G/5G, etc.), permettant d'interdire les usages non maîtrisés et d'éviter les intrusions via ces interfaces, doivent être définies et appliquées. Les interfaces sans fil ne doivent être activées qu'en cas de besoin.

MI-PDT-NOMAD-IOT : objets connectés. L'usage d'objets connectés est interdit sauf dans le cadre d'un projet mené par une DSI ministérielle en collaboration avec le SHFD.

MI-PDT-NOMAD-DEPLAC : déplacement professionnel. Des règles de sécurité lors de déplacement professionnel, notamment à l'étranger, doivent être appliquées, selon les recommandations de l'ANSSI¹. Les CSN doivent sensibiliser particulièrement les agents concernés avant leur mission.

MI-PDT-DESACT-DIST : désactivation à distance. Les équipements mobiles accédant au SI doivent pouvoir être désactivés à distance, notamment en cas de perte ou vol de l'équipement.

MI-PDT-CONF-VIRTUEL : Configuration des terminaux virtuels. Tout terminal virtualisé doit être conforme aux mesures de sécurité SI appliquées à un terminal physique.

MI-PDT-WEBMAIL : Utilisation du Webmail ministériel. L'accès à ses mails professionnels à partir d'un équipement personnel ne doit être réalisé qu'au travers de la solution Webmail NOMADE 2.

2. Sécurisation des imprimantes et copieurs multifonctions

Objectif A9-2 : sécurisation des copieurs multifonctions. Paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d'attaque.

MI-PDT-MUL-DURCISS : durcissement des imprimantes et copieurs multifonctions. Les services doivent mettre en œuvre les dispositions d'exploitation et de sécurité prévues par la DNUM dans le cadre du projet SOLIMP et par la directive du SHFD².

PSSIE-PDT-MUL-SECNUM : sécurisation de la fonction de numérisation. Lorsqu'elle est activée, la fonction de numérisation sur les copieurs multifonctions hébergés dans une entité doit être sécurisée. L'envoi de documents depuis le copieur vers des adresses électroniques externes au ministère de l'intérieur est interdit. Plus précisément, l'envoi de document par la fonction « Scan to mail » n'est autorisé que vers des boîtes mails nominatives du ministère et uniquement à une seule adresse de messagerie à la fois.

MI-PDT-MUL-STOCK : stockage des copieurs. Les supports de stockage (disques durs, mémoires flash, etc.) des copieurs sont la propriété de l'administration et sont considérés comme sensibles. Lors d'une maintenance nécessitant le retour du matériel ou son remplacement, ils doivent être conservés par l'administration et protégés comme il se doit.

MI-PDT-MUL-SCAN : maintenance. Lors d'une maintenance nécessitant le retour du matériel ou son remplacement, les adresses mails nominatives paramétrées pour la fonction « scan to mail » doivent être effacées.

MI-PDT-MUL-FILE : impression dans un fichier. Si les documents scannés sont envoyés vers un serveur de fichier (fonction « scan to file », des droits d'accès appropriés doivent être mis en œuvre de manière à s'assurer que le document ne sera accessible que de son propriétaire.

¹ Passeport de conseils de l'ANSSI aux voyageurs : https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf

² Se référer à la directive d'emploi des copieurs multifonctions du 27 mai 2014 disponible sur le site <http://ssi.mint.fr/>

MI-PDT-MUL-INT : interfaces communicantes. Les interfaces de communications sans fil, de type USB ou firewire doivent être désactivées.

MI-PDT-MUL-FAX : fonction d'envoi de FAX. La fonction FAX ne doit pas être directement connectée au réseau téléphonique. Les directives et les architectures d'interconnexion prévues par les DSI ministérielles doivent être respectées.

MI-PDT-MUL-IMP : impression d'informations sensibles. Pour les documents sensibles, il est obligatoire de mettre en œuvre la fonction d'impression sécurisée consistant à ce que l'impression ne soit traitée par le copieur après que l'utilisateur ait saisi son code PIN personnel sur le copieur ou présenté la puce sans contact de sa carte agent.

3. Sécurisation de la téléphonie

Objectif A9-3 : sécurisation de la téléphonie. Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes.

PSSIE-PDT-TEL-MINIM : sécuriser la configuration des autocommutateurs. Les autocommutateurs doivent être maintenus à jour au niveau des correctifs de sécurité. Leur configuration doit être durcie. La définition et l'affectation des droits d'accès et des privilèges aux utilisateurs (transfert départ-départ, entrée en tiers, interphonie, autorisation de déblocage, renvoi sur numéro extérieur, substitution, substitution de privilège, interception d'appel dirigé, etc.) doivent faire l'objet d'une attention particulière. Une revue de la programmation téléphonique doit être organisée périodiquement.

PSSIE-PDT-TEL-CODES : codes d'accès téléphoniques. Il est nécessaire de sensibiliser les utilisateurs au besoin de modifier le code d'accès de leur téléphone et de leur messagerie vocale.

PSSIE-PDT-TEL-DECT : limiter l'utilisation du DECT. Les communications réalisées au travers du protocole DECT sont susceptibles d'être interceptées, même si les mécanismes d'authentification et de chiffrement que propose ce protocole sont activés. Il est recommandé d'attribuer des postes téléphoniques filaires aux utilisateurs dont les échanges sont les plus sensibles.

MI-PDT-TEL-TOIP : sécurisation de la fonction de ToIP. Tout déploiement de systèmes de téléphonie sur IP doit être conforme aux procédures d'exploitation de la sécurité édictées par les DSI ministérielles dans le cadre de l'homologation de référence en vigueur.

MI-PDT-TEL-PFAU : sécurisation des appels d'urgence. Les systèmes de téléphonie utilisés pour le traitement des appels d'urgence, au regard de la sensibilité des informations qu'ils traitent, doivent protéger ces informations avec des moyens de chiffrements labélisés par l'ANSSI.

MI-PDT-TEL-TELECONF : sécurisation des accès aux téléconférences. En fonction du niveau de sensibilité des informations affichées ou échangées, un code d'accès aux visioconférences ou conférences téléphoniques doit être paramétré et transmis uniquement aux participants ayant le besoin d'en connaître. Tout agent du ministère se doit d'utiliser uniquement les outils de téléconférence autorisés par les DSI ministérielles.

4. Contrôles de conformité

Objectif A9-4 : contrôle de la conformité des postes de travail. Contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail.

MI-PDT-CONF-VERIF : utiliser des outils de vérification automatique de la conformité. Les outils mis en œuvre au niveau des infrastructures ministérielles pour la gestion des postes de travail Windows et Linux, opérées par les DSI ministérielles, doivent permettre de réaliser des contrôles de la conformité des postes déployés dans les services du ministère.