



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

PGSN – B04

**Exigences spécifiques au périmètre de
L'Administration Territoriale de l'Etat**

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).

Le présent document liste des exigences techniques ou organisationnelles permettant de contribuer à la réalisation de chaque objectif. Ces exigences sont organisées de la manière suivante :

- Les exigences préfixées « [MI-XXX-YYY] ATE- » viennent préciser les exigences élémentaires du corpus de la sécurité numérique sur le périmètre défini à l'article 3 de la PGSN-MI ;
- Les exigences préfixées « ATE- » sont propres au périmètre défini à l'article 3 de la PGSN-MI.

S'agissant des mesures ne faisant pas l'objet d'une précision pour l'ATE dans ce document, le terme « entité » doit être substitué par « des services déconcentrés mentionnés à l'article 3 de la PSN-ATE à l'échelle du département ».

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.

Administration Territoriale de l'Etat

1. Organisation et gouvernance de la sécurité numérique

Tous les modèles d'arrêté et de lettres se trouvent à l'adresse : <http://ssi.minint.fr/index.php/parcours-des-acteurs-ssi/nominationcessation/82-lettres-type-de-designation-et-arrete-de-nomination>.

Les modèles d'arrêté et de lettres désignés ci-dessus sont les seuls autorisés pour la constitution des dossiers de désignation et pour les cessations de fonction.

[MI-ORG-CSN] ATE-ORG-CSN : désignation du CSN. Le dossier de nomination du CSN transmis au SHFD doit comporter les éléments suivants :

1. La lettre de désignation du CSN signée par l'acteur désigné et par le préfet de département ;
En cas de nomination d'un CSN pour plusieurs départements, chaque préfet de département signe la lettre de désignation ;
2. Une copie de l'arrêté signé par le préfet de département ;
En cas de nomination d'un CSN pour plusieurs départements, chaque préfet de département signe l'arrêté ;
3. La lettre de mission signée par l'acteur désigné ;
4. Un certificat de sécurité attestant de l'habilitation au niveau requis ;
A défaut, du bordereau d'envoi de la demande d'habilitation ;

Tout dossier incomplet sera refusé.

ATE-ORG-CESSATION-CSN : cessation de fonction d'un CSN. La cessation de fonction du CSN doit faire l'objet d'une lettre de cessation signée par le préfet de département et transmise au SHFD, a minima, 1 mois avant la date de fin effective de l'acteur sur ses missions. En cas de CSN exerçant ses fonctions sur plusieurs départements, chaque préfet de département signe la lettre de cessation ;

[MI-ORG-RSSI] ATE-ORG-RSSI : désignation du RSSI. Le dossier de nomination du RSSI transmis au SHFD doit comporter les éléments suivants :

1. La lettre de désignation signée par l'acteur désigné, le directeur du SGC(D) et visé par le CSN ;
2. Un certificat de sécurité attestant de l'habilitation au niveau requis ;
A défaut, du bordereau d'envoi de la demande d'habilitation ;
3. Les adresses de messagerie individuelle et fonctionnelle et les numéros de téléphone.

Tout dossier incomplet sera refusé.

ATE-ORG-CESSATION-RSSI : cessation de fonction d'un RSSI. La cessation de fonction du RSSI doit faire l'objet d'une lettre de cessation signée par le directeur du SGC(D), visée par le CSN et transmise au SHFD, a minima, 1 mois avant la date de fin effective de l'acteur sur ses missions.

ATE-ORG-ALSN : désignation d'un ALSN. Le dossier de nomination d'un ALSN transmis au SHFD doit comporter les éléments suivants :

1. La lettre de désignation signée par l'acteur désigné, par le directeur du service déconcentré où il exercera ses fonctions et visé par le CSN ;
En cas de nomination d'un ALSN exerçant ses responsabilités sur plusieurs services déconcentrés mentionnées à l'article 3 de la PSN-ATE, chaque directeur de service signe la lettre de mission ;
2. Un certificat de sécurité attestant de l'habilitation au niveau requis ;

A défaut, du bordereau d'envoi de la demande d'habilitation ;

3. Les adresses de messagerie individuelle et fonctionnelle et les numéros de téléphone.

Tout dossier incomplet sera refusé.

ATE-ORG-CESSATION-ALSN : cessation de fonction d'un ALSN. La cessation de fonction d'un ALSN doit faire l'objet d'une lettre de cessation signée par le directeur du service déconcentré où il exerce ses fonctions, visée par le CSN et transmise au SHFD, a minima, 1 mois avant la date de fin effective de l'acteur sur ses missions.

En cas de nomination d'un ALSN exerçant ses responsabilités sur plusieurs services déconcentrés mentionnées à l'article 3 de la PSN-ATE, chaque directeur de service signe la lettre de cessation ;

ATE-ORG-ALSSI : désignation d'un ALSSI. Le dossier de nomination d'un ALSSI transmis au SHFD doit comporter les éléments suivants :

1. La lettre de mission signée par l'acteur désigné, par son autorité hiérarchique et visé par le CSN et le RSSI ;
2. Un certificat de sécurité attestant de l'habilitation au niveau requis;
A défaut, du bordereau d'envoi de la demande d'habilitation ;
3. Les adresses de messagerie individuelle et fonctionnelle et les numéros de téléphone.

Tout dossier incomplet sera refusé.

ATE-ORG-CESSATION-ALSSI : cessation de fonction d'un ALSSI. La cessation de fonction d'un ALSSI doit faire l'objet d'une lettre de cessation signée par le directeur du SGC(D), visée par le CSN et transmise au SHFD, a minima, 1 mois avant la date de fin effective de l'acteur sur ses missions.

2. Sécurité physique

[MI-PHY-TEC] ATE-PHY-AUDIT : Audit de site sur les sites hébergeant des services relevant du ministère de l'intérieur et d'autres services de l'Etat ou autres. En cas de mutualisation des locaux physiques entre des services relevant du ministère de l'intérieur et d'autres services de l'Etat ou autres, un audit de site doit être effectué. Il doit permettre de relever les vulnérabilités en fonction des besoins de sûreté émis par les autorités compétentes des services relevant du ministère de l'intérieur.

[MI-PHY-TEC] ATE-PHY-TECH-ABATTOIR : sécurité physique des locaux d'hébergement des ressources informatiques en abattoir. Les agents des services vétérinaires en abattoirs disposent d'un poste de travail d'un niveau de sécurité au moins équivalent aux postes NOEMI permettant une connexion au SI du ministère via le réseau mobile. En cas d'absence de couverture de réseau mobile alors un point d'accès à internet est mis à disposition. Il est géographiquement situé dans le local hébergeant les services vétérinaires ([Règlement n°853/2004 du 29 avril 2004 fixant des règles spécifiques d'hygiène applicables aux denrées alimentaires d'origine animale](#), annexe III, section I, chapitre II, point 9).

3. Sécurité des réseaux

[PSSIE-RES-INTERNET-SPECIFIQUE] ATE-RES-INTERNET-SPECIFIQUE : Cas particulier des accès spécifiques dans une entité. Pour les besoins d'enquête des services, les accès internet spécifiques sont autorisés sur des machines isolées physiquement et séparées du réseau de l'entité. Les possibilités de connexions sans fil sont désactivées.

[MI-RES-ARCHI-INTERNET] ATE-RES-ARCHI-INTERNET : passerelle Internet utilisateur. Les accès internet utilisateur à vocations professionnelle et personnelle, permettant une navigation Web, sont uniquement autorisés au travers de la plate-forme Orion et en profil sécurisé. Seuls les cas particuliers peuvent être envisagés en profil spécial après autorisation exclusive du CSN ([Description des profils](#)

[ORION](#)).

[MI-RES-ARCHI-INTERNET] ATE-RES-ARCHI-INTERNET-EQUIPEMENT : passerelle Internet pour les dispositifs nécessitant une connexion à internet. Les accès internet des dispositifs nécessitant une connexion à Internet sont uniquement autorisés au travers de la plate-forme Orion et en profil sécurisé. Seuls les cas particuliers peuvent être envisagés en profil spécial après autorisation exclusive du CSN ([Description des profils ORION](#)).

[MI-RES-SSFIL] ATE-RES-SSFIL-PUBLIC-PHY : Limitation des rayonnements des réseaux sans fil à destination des usagers ou visiteurs d'une entité. Les rayonnements des réseaux sans fil à destination des usagers ou visiteurs (personnes ne relevant pas du ministère de l'intérieur) doivent se limiter aux locaux de l'entité. Dans le cas contraire, une déclaration à l'ARCEP est nécessaire (Code des postes et des communications électroniques, [art. L. 33-1, I](#)).

[MI-RES-SSFIL] ATE-RES-SSFIL-PUBLIC-LOG : Conservation des données des communications électroniques des réseaux sans fil à destination des usagers ou visiteurs d'une entité. Toute entité mettant en œuvre des réseaux sans fil à destination des usagers ou visiteurs doit s'assurer de la conservation des données suivantes ([décret n°2006-358 du 24 Mars 2006](#) ; Code des postes et des communications électroniques, [art L. 34-1](#)) :

1. Les informations permettant d'identifier l'utilisateur et non les informations sur ces derniers ;
2. Les données relatives aux équipements terminaux de communication utilisés à l'exclusion des données de géolocalisation ;
3. Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
4. Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
5. Les données permettant d'identifier le ou les destinataires de la communication.

[MI-RES-SSFIL] ATE-RES-SSFIL-PUBLIC-DUREE : Durée de conservation des données des communications électroniques des réseaux sans fil à destination des usagers ou visiteurs d'une entité. La durée de conservation des données mentionnées dans la règle [ATE-RES-SSFIL-PUBLIC-LOG] est d'un an pour les besoins de recherche, de la constatation, et de la poursuite pour les infractions pénales ([décret n°2006-358 du 24 Mars 2006](#)).

4. Architecture des SI

ATE-ARCHI-CLOUD : Usage de l'informatique en nuage. Les usages des technologies dits « cloud » doivent respecter les recommandations de la [circulaire N°6282/SG du Premier Ministre relative à la doctrine de l'informatique en nuage par l'Etat \(« cloud au centre »\)](#).

ATE-CONF-CCT : Conformité aux CCT. Les développements informatiques locaux doivent respecter le cadre technique fixé par le cadre de cohérence technique du ministère ([CCT MI](#)).

5. Sécurité du poste de travail

ATE-LOG-PROCESSUS : Processus de demande de logiciels à installer sur le poste de travail. L'utilisation de logiciel sur le poste de travail doivent faire l'objet d'une demande d'avis suivant un processus défini où les acteurs suivants sont sollicités :

- 1° CSN du périmètre concerné ;

2° Correspondant RGPD du périmètre concerné (le cas échéant, le délégué à la protection des données du ministère, delegue-protection-donnees@interieur.gouv.fr) ;

3° DZSN du périmètre concerné ;

4° La MPSSI de la DNUM (dnum-mpssi@interieur.gouv.fr).

ATE-NIV-ACTIVE-DIRECTORY : Niveau des annuaires Active Directory. Le niveau des annuaires Active Directory sont a minima de niveau 3 au sens du recueil des points de contrôle de l'ANSSI ([Points de contrôles de l'annuaire Active Directory](#)).

6. Traitement des incidents

[MI-TI-INC-REM] ATE-TI-INC-REM : remontée des incidents.

Tout incident de sécurité ayant un impact sur la confidentialité, l'intégrité ou la disponibilité des systèmes d'informations, même apparemment mineur, doit faire l'objet d'un compte-rendu immédiat au C2MI, via la chaîne SSI locale. Le C2MI est chargé de la qualification de l'incident et de définir les mesures conservatoires et correctives. Si un incident est susceptible d'avoir un impact sur des systèmes d'information autre que ceux du ministère de l'intérieur, le C2MI est le seul habilité à communiquer l'information à la Sous-direction Opérations (SDO) de l'ANSSI ou aux correspondants du ou des ministères concernés.

La remontée d'incidents par les services déconcentrés participe à la posture permanente de vigilance, en complément du service de détection des incidents H24 mis en œuvre par le C2MI. Cette remontée est immédiate pour les incidents dont la portée est susceptible de dépasser à court terme le périmètre défini à l'article 3 de la PSN-ATE à l'échelle du département ou du ministère. La remontée prend la forme d'une synthèse mensuelle du CSN vers le C2MI pour les autres incidents.

Les critères et procédures précis de remontée d'incidents sont élaborés sous le pilotage du SHFD. Les CSN effectuent cette remontée au sein de leur périmètre jusqu'au C2MI, conseillés si besoin par les DZSN de leurs zones.

Le CSN ou, par délégation, un membre de la chaîne fonctionnelle départementale de la sécurité numérique doit maintenir à jour un historique clair des suites liées à l'escalade de chaque incident, afin de capitaliser les enseignements associés à la résolution (ou non) de ces incidents, auprès du C2MI.

L'aspect difficile de la caractérisation des attaques (ambiguïté de la source, du dommage, du moyen, de la finalité) rend nécessaire les échanges d'informations interministériels - même sur des « signaux faibles » - ainsi que la coordination continue des actions. Cette coordination est assurée par le C2MI.

7. Contrôles

[MI-CONTR-SSI] ATE-CONTR-LOCAUX : Points de contrôle locaux. Les points de contrôle trimestriels sont :

1. Le nombre de systèmes d'information locaux restants à homologuer ;
2. Le nombre de comptes disposant de profil spécial ([Description des profils ORION](#)) ;
3. Le nombre total d'événements de l'anti-virus relevés et classés par catégorie* ;
4. Le nombre d'événement de l'anti-virus ayant fait l'objet d'une intervention* ;
5. Les pourcentages des niveaux de mise à jour des postes de travail* ;
6. Les pourcentages des versions de moteur de l'anti-virus des postes de travail* ;

* Ces points de contrôle sont issus du tableau de bords GOUPIIL.

7. Les pourcentages de l'état des comptes utilisateurs* ;
8. Les pourcentages de l'état des mots de passe* ;
9. Les pourcentages de répartition des versions de systèmes d'exploitation des postes de travail* ;
10. Le niveau des annuaires Active Directory au sens du recueil des points de contrôle de l'ANSSI ([Points de contrôles de l'annuaire Active Directory](#)) et la liste des écarts ;
11. Le pourcentage de tests de restauration réussis de la dernière sauvegarde de moins d'un mois des serveurs de fichiers des services déconcentrés ;
12. Le pourcentage des serveurs, équipements actifs de réseau et des postes de travail à jour des derniers correctifs de sécurité publiés par la DNUM ;
13. Le pourcentage des serveurs, équipements actifs de réseau et des postes de travail des systèmes de sûreté à jour des derniers correctifs publiés par la DNUM (vidéo-protection, gestion des accès physique, etc.) ;
14. Les points de contrôle annuels sont :
15. Le nombre de séances de sensibilisation effectuées et le nombre d'agents couverts ;
16. Le nombre de comptes d'administration fonctionnelle des applications métier :
17. A minima, les paramètres suivants sont évalués :
18. Pour chaque groupe : nombre de comptes présents ;
 - a. Pour chaque compte présent dans ces groupes : l'évaluation de la conformité avec les usages métier en respectant le principe de frugalité ;
19. Comptes d'administration fonctionnelle des applications pilotant les systèmes de sûreté (vidéo-protection, gestion des accès physique, etc.) ;
20. A minima, les paramètres suivants sont évalués :
 - a. Pour chaque groupe : le nombre de comptes présents ;
 - b. Pour chaque compte présent dans ces groupes : l'évaluation de la conformité avec les usages métier en respectant le principe de frugalité ;