



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

PGSN – B03

**Exigences spécifiques aux systèmes
d'information essentiels (SIE)**

Version 1.0

TABLE DES MATIERES

1.	Classification de l'information	4
2.	Politique de sécurité des systèmes d'informations	4
3.	Homologation de sécurité.....	4
4.	Cartographie.....	5
5.	Maintien en condition de sécurité	5
6.	Journalisation	6
7.	Corrélation et analyse de journaux	7
8.	Détection	7
9.	Traitement des incidents de sécurité	7
10.	Traitement des alertes.....	8
11.	Gestion de crise	8
12.	Identification.....	9
13.	Authentification	9
14.	Droits d'accès	10
15.	Comptes d'administration	10
16.	Systèmes d'information d'administration	11
17.	Cloisonnement.....	12
18.	Filtrage	12
19.	Accès à distance.....	13
20.	Installation de services et d'équipements	13

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 détaille les exigences spécifiques applicables aux systèmes d'information essentiels (SIE) du ministère, conformément à l'article 33 de la PGSN-MI.

La notion de système d'information essentiel est propre au ministère de l'Intérieur et diffère donc de celle issue de la directive NIS¹.

Un système d'information est désigné par l'AQSSI concernée, en concertation avec le haut fonctionnaire de défense.

¹ <https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/>

1. Classification de l'information

MI-SIE-MARQUAGE-AUDIT : Les rapports d'audits sont marqués à minima avec les mentions de protection « Diffusion Restreinte » et « Spécial France ».

MI-SIE-MARQUAGE-FICHE-INCIDENT : Les fiches d'incidents sont marquées à minima avec les mentions de protection « Diffusion Restreinte » et « Spécial France ».

2. Politique de sécurité des systèmes d'informations

MI-SIE-PSSI : L'entité élabore, tient à jour et met en œuvre une PSSI qui décrit l'ensemble des moyens organisationnels et techniques mis en œuvre afin d'assurer la sécurité de ses SIE. En particulier, elle :

- Précise les objectifs et les orientations stratégiques en matière de sécurité des SIE ;
- Décrit l'organisation de la gouvernance de la sécurité et notamment les rôles et les responsabilités du personnel interne et du personnel externe ;
- Prévoit un plan de sensibilisation à la sécurité des SIE au profit de l'ensemble du personnel ainsi qu'un plan de formation à la sécurité des SIE au profit des personnes ayant des responsabilités particulières ;
- Fixe les mesures de sécurité générales, notamment en matière de contrôle du personnel interne et du personnel externe, de sécurité physique des SIE.

MI-SIE-PROCEDURES-SSI : L'entité définit les procédures suivantes :

- La procédure d'homologation de sécurité des SIE ;
- Les procédures de contrôle et d'audit de la sécurité des SIE ;
- La procédure de maintien en conditions de sécurité des ressources des SIE ;
- La procédure de traitement des incidents de sécurité ;
- Les procédures de gestion de crises en cas d'attaques informatiques et de continuité d'activité.

MI-SIE-SHFD-PSSI : La PSSI, ses documents d'application et les rapports sur leur mise en œuvre sont tenus à la disposition du service du haut fonctionnaire de Défense.

3. Homologation de sécurité

MI-SIE-HOMOLOGATION : L'entité procède à l'homologation de sécurité de chaque système d'information essentiel (SIE), en mettant en œuvre la procédure d'homologation prévue par sa politique de sécurité des systèmes d'information (PSSI).

MI-SIE-HOMOLOGATION-AUDIT : Dans le cadre de l'homologation, un audit de la sécurité du SIE doit être réalisé. Cet audit vise à vérifier l'application et l'efficacité des mesures de sécurité du SIE et notamment le respect des règles de sécurité mentionnées dans le présent référentiel. L'audit doit permettre d'évaluer le niveau de sécurité du SIE au regard des menaces et des vulnérabilités connues.

Le dossier d'homologation doit comporter a minima la réalisation d'un test d'intrusion couplé à un audit de configuration.

Dans le cas où le SI est exposé sur Internet, le dossier d'homologation doit également inclure un rapport d'audit de code et un rapport d'audit d'architecture.

Note : La réalisation d'un audit de code est fortement recommandée pour tous les développements applicatifs dont le ministère est propriétaire du code.

MI-SIE-HOMOLOGATION-DUREE : L'homologation est valable pour une durée maximale de trois ans et est renouvelée au terme de cette période. Toutefois, la validité de l'homologation est réexaminée par l'entité lors de chaque événement ou évolution de nature à modifier le contexte décrit dans le dossier d'homologation.

MI-SIE-SHFD-HOMOLOGATION : L'entité tient à la disposition du service du haut fonctionnaire de défense les décisions et dossiers d'homologation, notamment les rapports d'audit.

4. Cartographie

MI-SIE-SHFD-CARTO : L'entité doit être en mesure de fournir au service du haut fonctionnaire de défense, pour chaque système d'information essentiel (SIE), les éléments de cartographie suivants :

- Les noms et les fonctions des applications, supportant les activités de l'entité, installées sur le SIE ;
- Le cas échéant, les plages d'adresses IP de sortie du SIE vers internet ou un réseau tiers, ou accessibles depuis ces réseaux ;
- Le cas échéant, les plages d'adresses IP associées aux différents sous-réseaux composant le SIE ;
- La description fonctionnelle et les lieux d'installation du SIE et de ses différents sous-réseaux ;
- La description fonctionnelle des points d'interconnexion du SIE et de ses différents sous-réseaux avec des réseaux tiers, notamment la description des équipements et des fonctions de filtrage et de protection mis en œuvre au niveau de ces interconnexions ;
- L'inventaire et l'architecture des dispositifs d'administration du SIE permettant de réaliser notamment les opérations d'installation à distance, de mise à jour, de supervision, de gestion des configurations, d'authentification ainsi que de gestion des comptes et des droits d'accès ;
- La liste des comptes disposant de droits d'accès privilégiés (appelés « comptes privilégiés ») au SIE. Cette liste précise pour chaque compte le niveau et le périmètre des droits d'accès associés, notamment les comptes sur lesquels portent ces droits (comptes d'utilisateurs, comptes de messagerie, comptes de processus, etc.) ;
- L'inventaire, l'architecture et le positionnement des services de résolution de noms d'hôte, de messagerie, de relais internet et d'accès distant mis en œuvre par le SIE.

MI-SIE-SHFD-CARTO-SUPPORT : Sur demande du service du haut fonctionnaire de défense, l'entité lui communique les éléments de cartographie mis à jour sur un support électronique, dans un format qui peut être lu par les principaux logiciels bureautiques accessibles au public.

5. Maintien en condition de sécurité

MI-SIE-MCS : L'entité élabore, tient à jour et met en œuvre une procédure de maintien en conditions de sécurité des ressources matérielles et logicielles de ses systèmes d'information essentiels (SIE).

MI-SIE-MCS-VULNERABILITE : L'entité se tient informé des vulnérabilités et des mesures correctrices de sécurité susceptibles de concerner les ressources matérielles et logicielles de ses SIE, qui sont

diffusées notamment par les fournisseurs ou les fabricants de ces ressources ou par des centres de prévention et d'alerte en matière de cyber sécurité tels que le CERT-FR (www.cert.ssi.gouv.fr).

MI-SIE-MCS-MAINTENANCE : Sauf en cas de difficultés techniques ou opérationnelles justifiées, l'entité installe et maintient toutes les ressources matérielles et logicielles de ses SIE dans des versions supportées par leurs fournisseurs ou leurs fabricants et mises à jour du point de vue de la sécurité.

MI-SIE-MCS-VERIFICATION : Préalablement à l'installation de toute nouvelle version, l'entité s'assure de l'origine de cette version et de son intégrité, et analyse l'impact de cette version sur le SIE concerné d'un point de vue technique et opérationnel.

MI-SIE-MCS-INSTALLATION : Dès qu'il a connaissance d'une mesure correctrice de sécurité concernant une de ses ressources, et sauf en cas de difficultés techniques ou opérationnelles justifiées, l'entité en planifie l'installation après avoir effectué les vérifications mentionnées à l'alinéa précédent, et procède à cette installation dans les délais prévus par cette procédure.

MI-SIE-MCS-MESURES : Lorsque des raisons techniques ou opérationnelles le justifient, l'entité peut décider, pour certaines ressources de ses SIE, de ne pas installer une version supportée par le fournisseur ou le fabricant de la ressource concernée ou de ne pas installer une mesure correctrice de sécurité. Dans ce cas, l'entité met en œuvre des mesures techniques ou organisationnelles prévues par cette procédure pour réduire les risques liés à l'utilisation d'une version obsolète ou comportant des vulnérabilités connues.

MI-SIE-MCS-DOSSIER-HOMOLOGATION : L'entité décrit dans le dossier d'homologation du SIE concerné ces mesures de réduction des risques et les raisons techniques ou opérationnelles ayant empêché l'installation d'une version supportée ou d'une mesure correctrice de sécurité.

6. Journalisation

MI-SIE-JOURNAUX : L'entité met en œuvre sur chaque système d'information essentiel (SIE) un système de journalisation qui enregistre les événements relatifs à l'authentification des utilisateurs, à la gestion des comptes et des droits d'accès, à l'accès aux ressources, aux modifications des règles de sécurité du SIE ainsi qu'au fonctionnement du SIE.

MI-SIE-JOURNAUX-EQUIP : Le système de journalisation porte sur les équipements suivants lorsqu'ils génèrent les événements mentionnés au 1^{er} alinéa :

- Les serveurs applicatifs supportant les activités d'importance vitale ;
- Les serveurs d'infrastructure système ;
- Les serveurs d'infrastructure réseau ;
- Les équipements de sécurité ;
- Les postes d'ingénierie et de maintenance des systèmes industriels ;
- Les équipements réseau ;
- Les postes d'administration.

MI-SIE-JOURNAUX-HORODATE : Les événements enregistrés par le système de journalisation sont horodatés au moyen de sources de temps synchronisées. Ils sont, pour chaque SIE, centralisés et archivés pendant une durée d'au moins six mois. Le format d'archivage des événements permet de réaliser des recherches automatisées sur ces événements.

7. Corrélation et analyse de journaux

MI-SIE-JOURNAUX-CORREL : L'entité met en œuvre un système de corrélation et d'analyse de journaux qui exploite les événements enregistrés par le système de journalisation installé sur chacun des systèmes d'information essentiels (SIE), afin de détecter des événements susceptibles d'affecter la sécurité des SIE.

MI-SIE-JOURNAUX-SI : Le système de corrélation et d'analyse de journaux est installé et exploité sur un système d'information mis en place exclusivement à des fins de détection d'événements susceptibles d'affecter la sécurité des systèmes d'information.

MI-SIE-JOURNAUX-EXPLOIT : L'entité ou le prestataire mandaté à cet effet installe et exploite ce système de corrélation et d'analyse de journaux selon les règles fixées par le référentiel en matière de détection des incidents de sécurité prévu à l'article 10 du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale.

8. Détection

MI-SIE-DETECTION : L'entité met en œuvre, en application de l'article R. 1332-41-3 du code de la défense, un système de détection qualifié de type « sonde d'analyse de fichiers et de protocoles ».

MI-SIE-DETECTION-SONDE : Les sondes d'analyse de fichiers et de protocoles analysent les flux de données transitant par ces sondes afin de rechercher des événements susceptibles d'affecter la sécurité des systèmes d'information essentiels (SIE). Elles sont positionnées de manière à pouvoir analyser l'ensemble des flux échangés entre les SIE et les systèmes d'information tiers à ceux de l'entité.

MI-SIE-DETECTION-LISTE : Les systèmes de détection qualifiés de ce type sont choisis parmi ceux figurant sur la liste prévue à l'article R. 1332-41-9 du code de la défense.

MI-SIE-DETECTION-EXPLOIT : Ces systèmes de détection sont exploités selon les règles fixées par le référentiel en matière de détection des incidents de sécurité prévu à l'article 10 du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale. Ils sont exploités par un service de l'Etat ou un prestataire qualifié à cet effet dans les conditions prévues par le décret précité.

9. Traitement des incidents de sécurité

MI-SIE-INCIDENT : L'entité élabore, tient à jour et met en œuvre une procédure de traitement des incidents affectant le fonctionnement ou la sécurité de ses systèmes d'information essentiels.

MI-SIE-INCIDENT-TRAITEMENT : L'entité ou le prestataire mandaté à cet effet procède au traitement des incidents selon les règles fixées par le référentiel en matière de réponse aux incidents de sécurité prévu à l'article 10 du décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale.

MI-SIE-INCIDENT-SI : Un système d'information spécifique doit être mis en place pour traiter les incidents, notamment pour stocker les relevés techniques relatifs aux analyses des incidents. Ce système est cloisonné vis-à-vis du SIE concerné par l'incident.

MI-SIE-INCIDENT-DUREE : L'entité conserve les relevés techniques relatifs aux analyses des incidents pendant une durée d'au moins six mois.

10. Traitement des alertes

MI-SIE-ALERTE-C2MI : L'entité met en place un service de permanence lui permettant de prendre connaissance, à tout moment et sans délai, d'informations transmises par le centre de cyberdéfense du ministère de l'Intérieur.

MI-SIE-ALERTE-INCIDENT : L'entité met en place un service de permanence lui permettant de prendre connaissance, à tout moment et sans délai, d'information relatives à des incidents, des vulnérabilités et des menaces. Il met en œuvre une procédure pour traiter les informations ainsi reçues et le cas échéant prendre les mesures de sécurité nécessaires à la protection de ses SIE.

MI-SIE-ALERTE-PERMANENCE : L'entité communique au centre de cyberdéfense du ministère de l'Intérieur les coordonnées (nom du service, numéro de téléphone et adresse électronique) tenues à jour du service de permanence prévu à l'alinéa précédent.

11. Gestion de crise

MI-SIE-CRISE-PROCEDURE : L'entité élabore, tient à jour et met en œuvre une procédure de gestion de crises en cas d'attaques informatiques majeures.

Cette procédure décrit les moyens techniques et organisationnels dont dispose l'entité pour mettre en œuvre les mesures décidées par le Premier ministre en cas de crises, notamment les mesures suivantes :

- Appliquer une configuration système afin d'éviter les attaques ou d'en limiter les effets. Cette configuration peut viser notamment :
 - o À proscrire l'utilisation de supports de stockage amovibles ou la connexion d'équipements nomades aux systèmes d'information de l'entité ;
 - o À installer une mesure correctrice de sécurité sur un système d'information particulier ;
 - o À imposer un protocole de routage ;
- Mettre en place des règles de filtrage sur les réseaux ou des configurations particulières sur les équipements terminaux. Cette mesure peut viser notamment :
 - o À effectuer des restrictions d'accès sous forme de listes blanches et de listes noires d'utilisateurs ;
 - o À bloquer les échanges de fichiers d'un type particulier ;
 - o À isoler de tout réseau des sites internet, des applications, ou des équipements informatiques de l'entité en sollicitant le cas échéant l'appui des entités publiques de communications électroniques ;
- Isoler du réseau internet les systèmes d'information de l'entité. Cette mesure impose de déconnecter physiquement ou logiquement les interfaces réseau des systèmes d'information concernés.

MI-SIE-CRISE-CONDITION : La procédure précise les conditions dans lesquelles ces mesures peuvent être appliquées compte tenu des contraintes notamment techniques et organisationnelles de mise en œuvre.

12. Identification

MI-SIE-IDENT-COMPTE-INDIV : L'entité crée des comptes individuels pour les utilisateurs et pour les processus automatiques accédant aux ressources de ses SIE.

MI-SIE-IDENT-COMPTE-PARTAGE : Lorsque des raisons techniques ou opérationnelles ne permettent pas de créer de comptes individuels pour les utilisateurs ou pour les processus automatiques, l'entité met en place des mesures permettant de réduire le risque lié à l'utilisation de comptes partagés et d'assurer la traçabilité de l'utilisation de ces comptes. Dans ce cas, l'entité décrit ces mesures dans le dossier d'homologation du SIE concerné et les raisons justifiant le recours à des comptes partagés.

MI-SIE-IDENT-COMPTE-DESACTIV : L'entité désactive sans délai les comptes qui ne sont plus nécessaires.

13. Authentification

MI-SIE-AUTHENT-PROTECT : L'entité protège les accès aux ressources de ses SIE, que ce soit par un utilisateur ou par un processus automatique, au moyen d'un mécanisme d'authentification basé sur un élément secret.

MI-SIE-AUTHENT-REGLES : L'entité définit, conformément à sa politique de sécurité des systèmes d'information, les règles de gestion des éléments secrets d'authentification mis en œuvre dans ses SIE.

MI-SIE-AUTHENT-SECRET : Lorsque la ressource le permet techniquement, les éléments secrets d'authentification doivent pouvoir être modifiés par l'entité chaque fois que cela est nécessaire. Dans ce cas, l'entité respecte les règles suivantes :

- L'entité doit modifier les éléments secrets d'authentification lorsqu'ils ont été installés par le fabricant ou le fournisseur de la ressource, avant sa mise en service. A cet effet, l'entité s'assure auprès du fabricant ou du fournisseur qu'il dispose des moyens et des droits permettant de réaliser ces opérations ;
- L'élément secret d'authentification d'un compte partagé doit être renouvelé régulièrement et à chaque retrait d'un utilisateur de ce compte ;
- Les utilisateurs qui n'en ont pas la responsabilité, ne peuvent pas modifier les éléments secrets d'authentification. Ils ne peuvent pas non plus accéder à ces éléments en clair ;
- Lorsque les éléments secrets d'authentification sont des mots de passe, les utilisateurs ne doivent pas les réutiliser entre comptes privilégiés ou entre un compte privilégié et un compte non privilégié ;
- Lorsque les éléments secrets d'authentification sont des mots de passe, ceux-ci sont conformes aux règles de l'art telles que celles préconisées par l'Agence nationale de la sécurité des systèmes d'information, en matière de complexité (longueur du mot de passe et types de caractères), en tenant compte du niveau de complexité maximal permis par la ressource concernée, et en matière de renouvellement.

MI-SIE-AUTHENT-CONTROLE-ACCES : Lorsque la ressource ne permet pas techniquement de modifier l'élément secret d'authentification, l'entité met en place un contrôle d'accès physique à la ressource concernée ainsi que des mesures de traçabilité des accès et de réduction du risque lié à l'utilisation d'un élément secret d'authentification fixe. L'entité décrit dans le dossier d'homologation du SIE concerné ces mesures et les raisons techniques ayant empêché la modification de l'élément secret d'authentification.

14. Droits d'accès

MI-SIE-DROIT-ACCESS-REGLES : L'entité définit, conformément à sa politique de sécurité des systèmes d'information, les règles de gestion et d'attribution des droits d'accès aux ressources de ses SIE, et respecte les règles suivantes :

- L'entité n'attribue à un utilisateur ou à un processus automatique les droits d'accès à une ressource que si cet accès est strictement nécessaire à l'exercice des missions de l'utilisateur ou au fonctionnement du processus automatique ;
- L'entité définit les accès aux différentes fonctionnalités de cette ressource et en attribue les droits uniquement aux utilisateurs et aux processus automatiques qui en ont strictement le besoin ;
- Les droits d'accès sont révisés périodiquement, au moins tous les ans, par l'entité. Cette révision porte sur les liens entre les comptes, les droits d'accès associés et les ressources ou les fonctionnalités qui en font l'objet ;
- L'entité établit et tient à jour la liste des comptes privilégiés. Toute modification d'un compte privilégié (ajout, suppression, suspension ou modification des droits associés) fait l'objet d'un contrôle formel de l'entité destiné à vérifier que les droits d'accès aux ressources et fonctionnalités sont attribués selon le principe du moindre privilège (seuls les droits strictement nécessaires sont accordés) et en cohérence avec les besoins d'utilisation du compte.

15. Comptes d'administration

MI-SIE-COMPTE-ADMIN-CREATION : L'entité crée des comptes (appelés « comptes d'administration ») destinés aux seules personnes (appelées administrateurs) chargées d'effectuer les opérations d'administration (installation, configuration, gestion, maintenance, supervision, etc.) des ressources de ses SIE.

MI-SIE-COMPTE-ADMIN-REGLES : L'entité définit, conformément à sa politique de sécurité des systèmes d'information, les règles de gestion et d'attribution des comptes d'administration de ses SIE, et respecte les règles suivantes :

- L'attribution des droits aux administrateurs respecte le principe du moindre privilège. En particulier, afin de limiter la portée de ces droits individuels, ils sont attribués à chaque administrateur en les restreignant autant que possible au périmètre fonctionnel et technique dont cet administrateur est responsable ;
- Un compte d'administration est utilisé exclusivement pour se connecter à un système d'information d'administration (système d'information utilisé pour les opérations d'administration des ressources) ou à une ressource administrée ;

- Les opérations d'administration sont effectuées exclusivement à partir de comptes d'administration, et inversement, les comptes d'administration sont utilisés exclusivement pour les opérations d'administration ;
- Lorsque l'administration d'une ressource ne peut pas techniquement être effectuée à partir d'un compte spécifique d'administration, l'entité met en place des mesures permettant d'assurer la traçabilité et le contrôle des opérations d'administration réalisées sur cette ressource et des mesures de réduction du risque lié à l'utilisation d'un compte non spécifique à l'administration. Il décrit dans le dossier d'homologation du SIE concerné ces mesures ainsi que les raisons techniques ayant empêché l'utilisation d'un compte d'administration ;
- L'entité établit et tient à jour la liste des comptes d'administration de ses SIE et les gère en tant que comptes privilégiés.

16. Systèmes d'information d'administration

MI-SIE-SI-ADMIN-REGLES : L'entité applique les règles suivantes aux systèmes d'information utilisés pour effectuer l'administration de ses SIE, qui sont appelés « systèmes d'information d'administration » :

- Les ressources matérielles et logicielles des systèmes d'information d'administration sont gérées et configurées par l'entité ou, le cas échéant, par le prestataire qu'il a mandaté pour réaliser les opérations d'administration ;
- Les ressources matérielles et logicielles des systèmes d'information d'administration sont utilisées exclusivement pour réaliser des opérations d'administration. Cependant, lorsque des raisons techniques ou organisationnelles le justifient, le poste de travail physique de l'administrateur peut être utilisé pour réaliser des opérations autres que des opérations d'administration. Dans ce cas, des mécanismes de durcissement du système d'exploitation du poste de travail et de cloisonnement doivent être mis en place pour permettre d'isoler l'environnement logiciel utilisé pour ces autres opérations de l'environnement logiciel utilisé pour les opérations d'administration ;
- Un environnement logiciel utilisé pour effectuer des opérations d'administration ne doit pas être utilisé à d'autres fins, comme l'accès à des sites ou serveurs de messagerie sur internet ;
- Un utilisateur ne doit pas se connecter à un système d'information d'administration au moyen d'un environnement logiciel utilisé pour d'autres fonctions que des opérations d'administration ;
- Les flux de données associés à des opérations autres que des opérations d'administration doivent, lorsqu'ils transitent sur les systèmes d'information d'administration, être cloisonnés au moyen de mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information ;
- Les systèmes d'information d'administration sont connectés aux ressources à administrer au travers d'une liaison réseau physique utilisée exclusivement pour les opérations d'administration. Ces ressources sont administrées au travers de leur interface d'administration physique. Lorsque des raisons techniques empêchent d'administrer une ressource au travers d'une liaison réseau physique ou de son interface d'administration physique, l'entité met en œuvre des mesures de réduction du risque telles que des mesures

de sécurité logique. Dans ce cas, il décrit ces mesures et leurs justificatifs dans le dossier d'homologation du SIE concerné ;

- Lorsqu'ils ne circulent pas dans le système d'information d'administration, les flux d'administration sont protégés par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information. Si le chiffrement et l'authentification de ces flux ne sont pas possibles pour des raisons techniques, l'entité met en œuvre des mesures permettant de protéger ces flux en confidentialité et en intégrité et de renforcer le contrôle et la traçabilité des opérations d'administration. Dans ce cas, il décrit ces mesures et leurs justificatifs dans le dossier d'homologation du SIE concerné ;
- Les journaux enregistrant les événements générés par les ressources utilisées par les administrateurs ne contiennent aucun mot de passe en clair ou sous forme de condensat.

17. Cloisonnement

MI-SIE-CLOISONNEMENT-REGLES : L'entité procède au cloisonnement de ses SIE afin de limiter la propagation des attaques informatiques au sein de ses systèmes ou ses sous-systèmes. Il respecte les règles suivantes :

- Chaque SIE est cloisonné physiquement ou logiquement vis-à-vis des autres systèmes de l'entité ou des systèmes tiers ;
- Lorsqu'un SIE est lui-même constitué de sous-systèmes, ceux-ci sont cloisonnés entre eux physiquement ou logiquement. Un sous-système peut être constitué pour assurer une fonctionnalité ou un ensemble homogène de fonctionnalités d'un SIE ou encore pour isoler des ressources d'un SIE nécessitant un même besoin de sécurité ;
- Seules les interconnexions strictement nécessaires au bon fonctionnement et à la sécurité d'un SIE sont mises en place entre le SIE et les autres systèmes ou entre les sous-systèmes du SIE.

MI-SIE-CLOISONNEMENT-HOMOLOG : L'entité décrit dans le dossier d'homologation de chaque SIE les mécanismes de cloisonnement qu'il met en place.

18. Filtrage

MI-SIE-FILTRAGE-REGLES : L'entité met en place des mécanismes de filtrage des flux de données circulant dans ses SIE afin de bloquer la circulation des flux inutiles au fonctionnement de ses systèmes et susceptibles de faciliter des attaques informatiques. Il respecte les règles suivantes :

- L'entité définit les règles de filtrage des flux de données (filtrage sur adresse réseau, sur protocole, sur numéro de port, etc.) permettant de limiter autant que possible la circulation des flux aux seuls flux de données nécessaires au fonctionnement et à la sécurité de ses SIE ;
- Les flux entrants et sortants des SIE ainsi que les flux entre sous-systèmes des SIE sont filtrés au niveau de leurs interconnexions de manière à ne permettre que la circulation des seuls flux strictement nécessaires au fonctionnement et à la sécurité des SIE. Les flux qui ne sont pas conformes aux règles de filtrage sont bloqués ;
- L'entité établit et tient à jour une liste des règles de filtrage mentionnant l'ensemble des règles en vigueur ou supprimées depuis moins d'un an. Cette liste précise pour chaque règle :

- o Le motif et la date de la mise en œuvre, de la modification ou de la suppression de la règle ;
- o Les modalités techniques de mise en œuvre de la règle.

MI-SIE-FILTRAGE-HOMOLOG : L'entité décrit dans le dossier d'homologation de chaque SIE les mécanismes de filtrage qu'il met en place.

19. Accès à distance

MI-SIE-ACCES-DISTANT-REGLES : L'entité protège les accès à ses SIE effectués à travers des réseaux tiers. En particulier, lorsque l'entité ou un prestataire qu'il a mandaté à cet effet accède à un SIE à travers un réseau tiers à ceux de l'entité ou du prestataire, l'entité applique ou fait appliquer à son prestataire les règles suivantes :

- L'accès au SIE est protégé par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information ;
- Les équipements utilisés pour accéder au SIE sont gérés et configurés par l'entité ou, le cas échéant, par le prestataire. Les mémoires de masse de ces équipements sont en permanence protégées par des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'Agence nationale de la sécurité des systèmes d'information.

20. Installation de services et d'équipements

MI-SIE-INSTALL-SERVICE-EQUIP-REGLES : L'entité respecte les règles suivantes lorsqu'il installe des services et des équipements sur ses SIE :

- L'entité installe sur ses SIE les seuls services et fonctionnalités qui sont indispensables au fonctionnement ou à la sécurité de ses SIE. L'entité désactive les services et les fonctionnalités qui ne sont pas indispensables, notamment ceux installés par défaut, et les désinstalle si cela est possible. Lorsque la désinstallation n'est pas possible, l'entité le mentionne dans le dossier d'homologation du SIE concerné en précisant les services et fonctionnalités concernés et les mesures de réduction du risque mises en œuvre ;
- L'entité ne connecte à ses SIE que des équipements, matériels périphériques et supports amovibles qu'il a dûment répertoriés et qui sont indispensables au fonctionnement ou à la sécurité de ses SIE ;
- Les supports amovibles inscriptibles connectés aux SIE sont utilisés exclusivement pour les besoins de ces SIE ;
- L'entité procède, avant chaque utilisation de supports amovibles, à l'analyse de leur contenu, notamment à la recherche de code malveillant. L'entité met en place, sur les équipements auxquels sont connectés ces supports amovibles, des mécanismes de protection contre les risques d'exécution de code malveillant provenant de ces supports.

FIN DU DOCUMENT