



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

PGSN – A05

Sécurité physique

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- », 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.

Sécurité physique

1. Sécurité physique des locaux abritant les SI

Objectif A5-1 : sécurité physique des locaux abritant les SI. Inscire la sécurisation physique des SI dans la sécurisation physique des locaux et dans les processus associés.

1.1. Règles générales

PSSIE-PHY-ZONES : découpage des sites en zones de sécurité. Un découpage des sites en zones physiques de sécurité doit être effectué, en liaison avec le CSN, les correspondants locaux SN et les services en charge : de l'immobilier, de la sécurité et des moyens généraux. Pour chaque zone de sécurité, des critères précis d'autorisation d'accès sont établis.

1.2. Règles de sécurité s'appliquant aux zones d'accueil du public

PSSIE-PHY-PUBL : accès réseau en zone d'accueil du public. Tout accès réseau installé dans une zone d'accueil du public doit être filtré ou isolé du reste du réseau informatique de l'entité.

MI-PHY-SENS : protection des informations sensibles au sein des zones d'accueil. Le traitement d'informations sensibles au sein des zones d'accueil est à éviter. Si un tel traitement est strictement nécessaire, il doit rester ponctuel, exceptionnel et motivé. Des mesures particulières sont alors adoptées, notamment en matière de protection audiovisuelle, ainsi qu'en matière de protection des informations stockées sur les supports.

1.3. Règles de sécurité complémentaires s'appliquant aux locaux techniques

MI-PHY-TECH : sécurité physique des locaux techniques. L'accès aux locaux techniques abritant des équipements d'alimentation et de distribution d'énergie, des équipements de réseau et de téléphonie, ou des ressources informatiques du ministère de l'intérieur doivent être physiquement protégés. Ces locaux doivent n'être accessibles qu'à du personnel du ministère de l'intérieur ou dûment autorisé par lui.

PSSIE-PHY-TELECOM : protection des câbles électriques et de télécommunications. Il convient de protéger le câblage réseau contre les dommages et les interceptions des communications qu'ils transmettent. En complément, les panneaux de raccordements et les salles des câbles doivent être placés en dehors des zones d'accueil du public et leur accès doit être contrôlé.

PSSIE-PHY-CTRL : contrôles anti-piégeages. Sur les SI particulièrement sensibles, il convient de mener des contrôles anti-piégeages réguliers, effectués par du personnel formé. Il peut être fait appel à des services spécialisés (opérations dites de « dépoussiérage »).

2. Sécurité physique des centres informatiques

Objectif A5-2 : sécurité physique des centres informatiques. Dimensionner les protections physiques des centres informatiques en fonction des enjeux liés à la concentration des moyens et données abrités.

2.1. Règles générales

PSSIE-PHY-CI-LOC : découpage des locaux en zones de sécurité. Un découpage du centre informatique en zones physiques de sécurité doit être effectué, en liaison avec le CSN et les services en charge de l'immobilier, de la sécurité et des moyens généraux. Des règles doivent fixer les conditions d'accès à ces différentes zones.

MI-PHY-CI-SOUSTRAIT : convention de service en cas sous-traitance. Dans le cas où un tiers gère tout ou partie des locaux du centre informatique, une convention de service, définissant précisément les responsabilités mutuelles en matière de sécurité, relatives à la confidentialité, l'intégrité et la disponibilité des données, doit être établie entre ce tiers et l'entité ou le ministère.

2.2. Règles de sécurité complémentaires s'appliquant aux zones internes et restreintes

PSSIE-PHY-CI-CTRLACC : contrôle d'accès physique. L'accès aux zones internes (autorisées uniquement au personnel du centre informatique ou aux visiteurs accompagnés) et restreintes (autorisées aux seules personnes habilitées ou aux visiteurs accompagnés) doit reposer sur un dispositif de contrôle d'accès physique. Ce dispositif doit s'appuyer sur des produits qualifiés, lorsqu'ils sont disponibles, et bénéficier d'un maintien en condition de sécurité rigoureux.

MI-PHY-CI-MOYENS : délivrance des moyens d'accès physique. La délivrance des moyens d'accès physique doit respecter un processus formel permettant de s'assurer de l'identité de la personne, s'appuyant sur le processus d'arrivée et de départ du personnel. Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones sensibles (entretien ou réparation des bâtiments, des équipements non informatiques, nettoyage, visiteurs, ...), intervient systématiquement et impérativement sous surveillance permanente d'un agent habilité.

PSSIE-PHY-CI-TRACE : traçabilité des accès. Une traçabilité des accès, par les visiteurs externes, aux zones restreintes doit être mise en place. Ces traces sont alors conservées un an, dans le respect des textes protégeant les données personnelles.

2.3. Règles de sécurité complémentaires s'appliquant aux salles informatiques et aux locaux techniques

PSSIE-PHY-CI-ENERGIE : local énergie. L'alimentation secteur des équipements devra être conforme aux règles de l'art, de façon à se prémunir des atteintes à la sécurité des personnes et équipements liées à un défaut électrique.

PSSIE-PHY-CI-CLIM : climatisation. Un dispositif de climatisation dimensionné en fonction des besoins énergétiques du système informatique doit être installé. Des procédures de réaction en cas de panne, connues du personnel, doivent être élaborées et vérifiées annuellement.

Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

PSSIE-PHY-CI-INC : lutte contre l'incendie. L'installation de matériel de protection contre le feu est obligatoire. Des procédures de réaction à un incendie sont définies et régulièrement testées. Les salles techniques doivent être propres. Aucun carton, papier, ou autre source potentielle de départ de feu ne doit être entreposé dans ces locaux.

PSSIE-PHY-CI-EAU : lutte contre les voies d'eau. Une étude sur les risques dus aux voies d'eau doit être réalisée. Cette étude doit notamment prendre en compte le risque de fuite sur un collecteur d'eau douce.

MI-PHY-CI-ELEC : protection de l'alimentation électrique. Pour les salles serveurs et les locaux techniques, des mesures spécifiques et adaptées aux risques de panne ou perturbation du réseau électrique doivent être mises en place et les procédures associées connues du personnel. La bonne exécution de ces procédures doit être vérifiée au moins annuellement.

Ces dispositions visent à prévenir toute défaillance des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

3. Systèmes d'information de sûreté

Objectif A5-3 : sécurité du SI de sûreté. Traiter de manière globale la sécurité des systèmes d'information et de communication qui assurent la sûreté d'un site.

Les entités sensibles du ministère s'appuient sur des systèmes d'information dits de sûreté pour assurer la protection des biens et des personnes. Dans ce cadre, l'appellation « *SI de sûreté* » regroupe :

- Les systèmes de contrôle d'accès et détection d'intrusion (CTA), permettant au personnel de sûreté :
 - o d'authentifier, d'autoriser et de tracer l'accès à une ressource physique (contrôle d'accès) ;
 - o de détecter, d'alerter et de tracer en cas de tentative d'accès non autorisé (détection d'intrusion).
- Les systèmes de vidéosurveillance (VS), fournissant au personnel de sûreté un système de caméras disposées sur l'ensemble du site, de transport des flux vidéo, d'enregistrement, d'archivage et de visionnage de ces vidéos ;
- Les systèmes de gestion technique des bâtiments (GTB), permettant de superviser et de gérer l'ensemble des équipements des bâtiments du site, et d'avoir une vue globale de l'état de ces bâtiments ;
- Les systèmes de sécurité incendie (INC), regroupant l'ensemble des moyens informatiques mis en œuvre pour détecter, informer, intervenir et/ou évacuer tout ou partie du site en cas d'incendie.

PSSIE-PHY-SI-SUR : sécurisation du SI de sûreté. Pour les sites physiques considérés comme importants, des mesures de protection doivent être définies et appliquées en se basant sur les conclusions d'une analyse de risques. L'analyse de risques conduit à la désignation des briques essentielles dont il faut assurer la protection contre des actes malveillants. Un système de gestion de la sécurité du SI de sûreté (s'inspirant de la norme ISO 27001) assure le maintien en condition de sécurité.

L'emploi de produits labellisés, quand ils existent ou ceux recommandés par l'ANSSI, est fortement recommandé.

MI-PHYS-SI-SUR-CLOIS : cloisonnement physique des SI de sûreté. Les SI de sûreté sont spécifiques par leur nature et les missions qu'ils assurent. Chacun de ces systèmes doit être déployé sur des réseaux de communication et des équipements physiquement distincts de tout autre système d'information. Aucune interconnexion, même pour des raisons de télémaintenance, n'est autorisée.