



**MINISTÈRE
DE L'INTÉRIEUR**

*Liberté
Égalité
Fraternité*

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

PGSN – A11

Traitement des incidents de sécurité

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.

Traitement des incidents de sécurité

1. Chaînes opérationnelles

Objectif A11-1 : chaînes opérationnelles. Partager l'information (alertes, incidents) dans le respect des règles de prudence et mutualiser les opérations de remise en état, de façon à lutter efficacement contre les attaques.

MI-TI-OPS-SN : chaînes opérationnelles SN. La structure de commandement de droit commun du ministère, soutenue par leurs CSN, concourt à l'effort national de cyberdéfense. Les alertes et les incidents sont gérés selon des procédures définies et testées lors d'exercices. La coordination des compétences est organisée à l'échelon ministériel par le SHFD.

Les situations d'urgences peuvent faire appel à des mesures définies préalablement dans le cadre des plans gouvernementaux, type Vigipirate/Piranet. En cas de crise, le centre de cyberdéfense du ministère de l'Intérieur (C2MI) assure la gestion et le pilotage des services concernés par l'événement ou la crise cyber.

MI-TI-PLAINTÉ : dépôt de plainte. Les entités victimes d'un acte de malveillance cyber doivent envisager de déposer plainte auprès des services compétents. La circulaire « plainte » permet d'orienter les autorités et le CSN sur la nécessité ou non de déposer plainte suivant la gravité de la malveillance¹.

2. Traitement des alertes de sécurité émises par les instances nationales (ANSSI)

MI-TI-MOB : mobilisation en cas d'alerte. En cas d'alerte de sécurité identifiée au niveau national, les CSN de chaque entité ou leurs suppléants, s'assurent de la bonne application des exigences formulées par le C2MI, dans les meilleurs délais. Un annuaire des CSN et des ALSN est tenu à jour par le C2MI.

3. Remontée des incidents de sécurité rencontrés

PSSIE-TI-QUAL-TRAIT : qualification et traitement des incidents. La chaîne fonctionnelle SN est informée par la chaîne opérationnelle de tout incident de sécurité, et contribue si nécessaire à la qualification de l'incident et au pilotage de son traitement.

MI-TI-INC-SIGN : signalement des incidents. Toute entité met en place et informe l'ensemble de ses personnels permanents et non permanents de leur obligation de signaler tout incident de sécurité et des moyens à employer pour effectuer ce signalement. Les incidents peuvent être des mesures inefficaces, une violation de sécurité logique ou physique, une erreur humaine, un non-respect des politiques ou procédures de sécurité, un changement non contrôlé apporté au système ou un dysfonctionnement.

¹ Se référer à la procédure de dépôt de plainte dans les cas d'atteinte aux systèmes d'information et de communication du MI du 17 février 2017, disponible sur le site <https://ssi.minint.fr/>

MI-TI-INC-REM : remontée des incidents. Tout incident de sécurité ayant un impact sur la confidentialité, l'intégrité ou la disponibilité des systèmes d'information, même apparemment mineur, doit faire l'objet d'un compte-rendu immédiat au C2MI, via la chaîne SN locale. Le C2MI est chargé de la qualification de l'incident et de définir les mesures conservatoires et correctives. Si l'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.

La remontée d'incidents par les services locaux participe à la posture permanente de vigilance, en complément du service de détection des incidents 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 de l'entité ou du ministère, et pour les incidents correspondant à des signalements spécifiques, notamment de la part du C2MI. Pour les autres incidents, la remontée prend la forme d'une synthèse mensuelle des CSN vers le C2MI.

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 CZSN de leurs zones ou les CSN généraux ou centraux de tête de chaîne.

Chaque entité 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.

MI-TI-INC-PREUVE : collecte des informations et archivage. Les informations relatives à l'incident de sécurité et son contexte d'apparition doivent être collectées. Les tâches liées à la réponse sont correctement journalisées en vue d'une analyse ultérieure. En l'absence d'une durée imposée par le cadre légal applicable, il est recommandé que l'ensemble des informations soit archivé de manière sécurisée pour une durée minimale de 1 an.