

Instruction ministérielle
relative à la définition et à la mise en œuvre
de la
Politique Générale de Sécurité des
Systèmes d'Information (PGSSI)



MINISTÈRE DE L'ÉCOLOGIE,
DU DÉVELOPPEMENT DURABLE
ET DE L'ÉNERGIE
www.developpement-durable.gouv.fr

MINISTÈRE DU LOGEMENT,
DE L'ÉGALITÉ DES TERRITOIRES
ET DE LA RURALITÉ
www.territoires.gouv.fr

Préambule

Les termes « ministère » et « entité » désignent respectivement les ministères mentionnés dans l'entête de la présente instruction et toute « autorité administrative » les constituant.

Les activités vitales de la nation, la recherche et l'innovation, les informations stratégiques des entités privées et publiques s'appuient sur des systèmes d'information de plus en plus exposés à de multiples attaques motivées par le profit et la malveillance.

Face à ces menaces, le législateur s'est doté d'un corpus réglementaire adapté.

Les directives nationales de sécurité renouvelées, la loi de programmation militaire (LPM) contraignent dorénavant les opérateurs d'importance vitale (OIV) à un renforcement de la protection des systèmes d'information d'importance vitale (SIIV).

A ce titre, le ministère coordonnateur assure la gestion et l'animation de plus d'une centaine d'OIV appartenant à une dizaine de secteurs très variés tels que l'énergie et les transports. Par ailleurs, certaines directions générales et déconcentrées sont des OIV.

Les SIIV devront répondre aux exigences de la LPM et à celles de la présente instruction.

Le patrimoine informationnel « sensible », quant à lui, est désormais encadré par la réglementation en matière de protection du potentiel scientifique et technique (PPST), la politique de sécurité des SI de l'État (PSSIE) et diverses instructions interministérielles.

Dans ce contexte, la mise en application de la politique générale de sécurité des systèmes d'information (PGSSI) du ministère concourt à la continuité des activités, prévient la fuite d'informations sensibles et renforce la confiance des citoyens et des entreprises dans les téléprocédures.

La présente instruction et ses directives d'accompagnement ne sont que des référentiels, qui, sans définition d'un plan d'action opérationnel et contrôlé, n'auraient que peu d'intérêt.

Ensemble, au regard des responsabilités de chacun, il convient de veiller à l'atteinte des quatre objectifs prioritaires de la PGSSI, qui visent :

- le renforcement des actions de gouvernance et de contrôle ;
- la conformité de l'environnement du poste de travail ;
- la maîtrise des systèmes d'information et l'accroissement de la résilience de nos activités ;
- le maintien du niveau de protection des infrastructures de réseau et des centres d'hébergement informatique.

Fait à Paris, le 27 JAN. 2016

Le Secrétaire Général,
Haut Fonctionnaire de défense et de sécurité



Francis ROL-TANGUY

Titre I. Dispositions générales

Article 1. Objet

La présente instruction énonce la politique générale de sécurité des systèmes d'information du ministère (PGSSI) en conformité avec la PSSIE et en définit la mise en œuvre.

Elle précise notamment :

- le périmètre d'application ;
- l'organisation et le corpus documentaire SSI ;
- les dispositions de mise en application ;
- la gestion des alertes, des incidents et situations d'urgence ;
- le contrôle et le suivi de la mise en application.

Article 2. Entités et personnes

La PGSSI s'applique :

- aux cabinets ministériels et à leurs secrétaires d'État ;
- aux entités définies dans l'article 1 du décret n°2008-680 du 9 juillet 2008 portant organisation de l'administration centrale du ministère et décret n°2013-872 du 27/09/13 modifiant le décret n°2008-680 du 9 juillet 2008 ;
- au conseil général de l'environnement et du développement durable ;
- au secrétariat général ;
- au commissariat général au développement durable ;
- aux directions générales ;
- aux services techniques centraux ;
- aux services déconcentrés, centres de formation et écoles.

En revanche, elle ne s'applique pas au périmètre interministériel et aux établissements publics.

Article 3. Systèmes d'information concernés

Un système d'information est un ensemble organisé de ressources (données, procédures, matériels, logiciels, personnels, etc.) permettant d'acquérir, de traiter, de stocker, de diffuser ou de détruire les informations utilisées par les entités dans leurs métiers, et ceci quel que soit le support des informations (sous forme numérique, papier ou orale).

La PGSSI s'applique à tout type de systèmes d'information du ministère, notamment industriels, de gestion ou bureautiques, etc.

Certains systèmes, classifiés de défense ou industriels sont soumis à un corpus réglementaire spécifique. Ils doivent répondre à ces règlements spécifiques. Sauf exigences contradictoires, ils devront aussi se conformer aux recommandations et exigences de la présente instruction.

Article 4. Date d'entrée en vigueur

La présente instruction entre en vigueur à compter de sa date de signature.

Titre II. Organisation et corpus documentaire SSI

Article 5. Dispositif organisationnel

Une organisation spécifique, destinée à assurer le pilotage et la coordination de la sécurité des SI, est mise en place à tous les niveaux de l'État.

- **Au niveau interministériel**

- L'agence nationale de sécurité des systèmes d'information (ANSSI) assure la mission d'autorité nationale en matière de défense et de sécurité des SI conformément aux décrets n° 2009-834 du 7 juillet 2009 et n° 2011-170 du 11 février 2011. Elle coordonne l'action gouvernementale dans le cadre des orientations fixées par le Premier ministre.
- L'ANSSI préside un groupe permanent chargé du pilotage de la PSSIE. Ce groupe composé des fonctionnaires de la sécurité des systèmes d'information (FSSI) et des personnes assurant ces fonctions au sein de la Présidence de la République, a pour principales missions de mettre en œuvre et de faire évoluer la PSSIE, de participer à l'élaboration et au suivi des plans d'action.
- L'ANSSI s'appuie au sein de chaque ministère sur le haut fonctionnaire de défense et de sécurité (HFDS) assisté par un fonctionnaire de sécurité des systèmes d'information (FSSI).

- **Au niveau ministériel**

- Le HFDS et le FSSI le représentant sont responsables de la cohérence globale de la PGSSI du ministère et de sa conformité à la PSSIE.
- Le comité de la sécurité des systèmes d'information (CSSI), coprésidé par le service de défense, de sécurité et d'intelligence économique (SDSIE) et le service des politiques support et des systèmes d'information (SPSSI), réunit des représentants des entités du ministère. Il a pour principales missions l'élaboration et l'évolution de la présente instruction et de ses annexes. Il propose le plan d'action national.

Le CSSI rend compte au comité stratégique des systèmes d'information (COSSI) du ministère.

- Le directeur d'entité est autorité qualifiée des systèmes d'information (AQSSI). Il est responsable de la mise en œuvre de la présente instruction dans son champ de compétence. Il valide le plan d'action et en assure le contrôle.

Il nomme au moins un responsable de la sécurité des systèmes d'information (RSSI) pour l'assister dans sa fonction et il désigne une ou plusieurs autorités d'homologation (AH).

- Le RSSI assure la mise en œuvre de la PGSSI dans le périmètre de son entité, propose le plan d'action et en assure le suivi.

Il anime un groupe de pilotage en charge de la SSI.

Cette chaîne fonctionnelle s'appuie sur une chaîne opérationnelle qui lui rend compte et qui contribue à la protection et à la défense des SI du ministère. La chaîne opérationnelle, constituée d'équipes directement en charge des SI :

- organise, applique la posture permanente de vigilance et assure la capacité opérationnelle de détection et de traitement des incidents ;
- assure la circulation des informations à la fois du ministère vers l'ANSSI (incidents, données techniques d'éléments suspects, traces, cartographie) et de l'ANSSI vers le ministère (vulnérabilités, alertes, mesures).

Les rôles des acteurs sont détaillés au sein de l'annexe A. La liste officielle des RSSI nommée est consultable sur l'Intranet.

Article 6. Corpus documentaire SSI

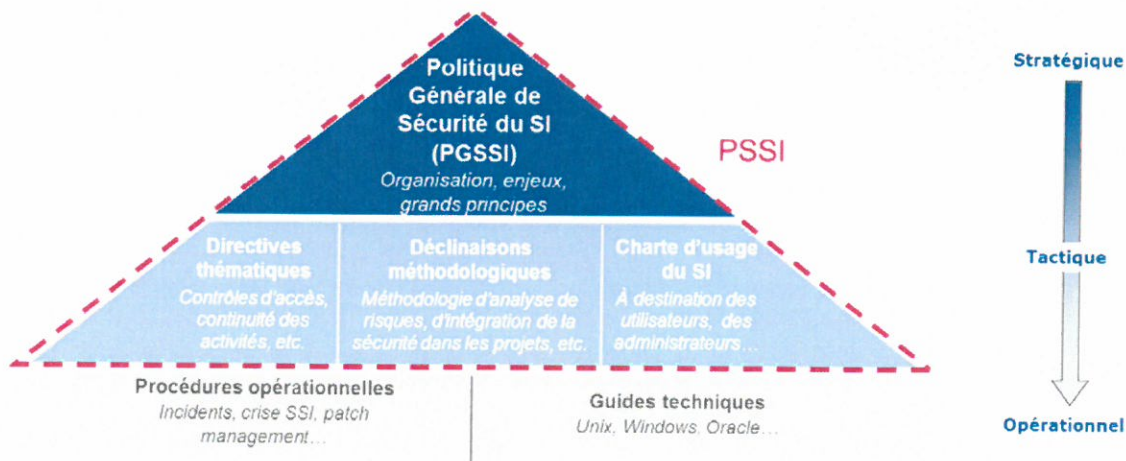
Le ministère a mis en place des principes et des normes formalisés afin d'atteindre ses objectifs.

La présente instruction, ses annexes, ses directives opérationnelles seront revues chaque année pour prendre en compte l'évolution des techniques, des métiers et des menaces.

Quatre annexes, en révision ou en cours d'élaboration, complètent la présente instruction :

- Annexe A : Obligations des acteurs en matière de sécurité des systèmes d'information. (révision);
- Annexe B : Exigences de conduite des contrôles et d'établissement du bilan annuel de sécurité des systèmes d'information. En cours d'élaboration, elle sera soumise à l'avis du CSSI et validé par le SG/HFDS ;
- Annexe C : Lois et textes de référence ;
- Annexe D : Liste détaillée des documents constituant le corpus documentaire SSI.

L'Instruction et ses annexes constituent la Politique Générale de sécurité des Systèmes d'information du ministère. La PGSSI et les directives associées ainsi que les procédures opérationnelles et les guides techniques constituent un ensemble dit « corpus documentaire SSI » structuré de la manière suivante :



Article 7. Mise à jour du corpus documentaire SSI

Les services SDSIE et SPSSI sont chargés de la mise à jour du corpus documentaire SSI.

Le service SPSSI établit les directives et les documents de référence complémentaires permettant de faciliter et/ou de préciser la mise en œuvre de la PGSSI.

Après avis du CSSI, les documents applicables sont mentionnés en annexe D et mis à la disposition des entités sur l'intranet.

Titre III. Dispositions de mise en application

Article 8. Dispositif de maîtrise des risques de sécurité

Chaque entité applique un dispositif de maîtrise des risques pour ses systèmes d'information.

Ce dispositif doit s'appuyer sur un processus régulier d'identification et de traitement des risques. Il doit permettre de s'assurer que les mesures de sécurité sont adaptées, que les actions engagées et les coûts engendrés sont proportionnés à la réduction du risque.

Pour ce faire, chaque entité :

- met en place une organisation en application de l'annexe A de la présente instruction ;
- conduit des actions de motivation, sensibilisation et de formation à la sécurité des SI en communiquant clairement sur les sanctions encourues ;
- établit un inventaire de ses SI et en évalue la sensibilité ;
- conduit une démarche d'homologation pour les SI sensibles selon les principes du Référentiel Général de Sécurité (RGS) et de la PSSI de l'État (PSSIE) ;
- conduit une analyse de risques de ses SI sensibles et veille à la définition des mesures de sécurité applicables ;
- organise la mise en application des dispositions de sécurité édictées par les maîtres d'ouvrage des SI Métiers et d'infrastructures ;
- conduit des actions régulières de contrôle du niveau de sécurité des SI de son périmètre et met en œuvre les actions correctives nécessaires, en application des principes détaillés en annexe B ;
- met en place les modalités lui permettant de faire face aux alertes, aux incidents de sécurité et aux situations d'urgence concernant la sécurité de ses SI ;
- établit un bilan annuel sur l'ensemble de ces points, ainsi qu'un plan d'actions, le cas échéant pluriannuel, en précisant les étapes successives pour être en conformité.

Au niveau du ministère, des procédures sont mises en place pour assurer la coordination et la cohérence de l'ensemble de ces dispositions et pour assister les entités.

L'ensemble des mesures doit être mise en œuvre, la demande de dérogation doit être exceptionnelle, motivée, argumentée et instruite. Elle n'est possible que dans deux cas : la mesure n'est pas adaptée au regard du périmètre étudié ou les coûts financiers et humains sont disproportionnés au regard des enjeux.

La décision de dérogation sera prise au bon niveau, national, sectoriel, local. Les AQSSI et RSSI devront faire état de la traçabilité des dérogations en cas de contrôle.

Chaque année, le FSSI transmet à l'ANSSI les écarts de la PGSSI à la PSSIE et les dérogations prises par le ministère.

Article 9. Gestion des alertes, des incidents et des situations d'urgence

Les services SDSIE et SPSSI définissent et mettent en place les dispositions nationales permettant de traiter les alertes, les incidents de sécurité et de gérer les situations d'urgence à l'échelle du ministère. Les principes et les exigences afférant aux trois thématiques sont détaillées dans une directive opérationnelle.

Un annuaire des acteurs des systèmes d'information (chaînes décisionnelle SSI, technique opérationnelle et métier) est maintenu à jour et diffusé par le service SPSSI.

Les dispositions nationales doivent être déclinées au sein de chaque entité du ministère par la formalisation de son organisation et de ses procédures. Elle met en place un dispositif de gestion de crise, tient à jour et diffuse un annuaire local d'astreinte.

Les alertes significatives sont signalées par l'ANSSI aux FSSI. Leur prise en compte au niveau du ministère est organisée sous la responsabilité du HFDS.

Les incidents de sécurité doivent être remontés à la chaîne fonctionnelle SSI du ministère. Ceux jugés significatifs sont remontés à l'ANSSI sous la responsabilité du HFDS.

En cas de situation de crise ministérielle et/ou interministérielle les actions des entités s'inscrivent dans une organisation de gestion de crise pré-définie.

Le fonctionnement de la chaîne fonctionnelle SSI est régulièrement vérifié dans le cadre d'exercices PIRANET.

Titre IV. Contrôle et suivi de mise en application

Article 10. Obligation

La conformité à la PGSSI et aux directives associées implique des contrôles réguliers à différents niveaux (cf. Annexe B). Chaque entité se dote d'un processus de contrôle, ce processus définit les responsabilités en la matière. Le contrôle interne est réalisé par l'entité elle-même, le contrôle externe par un service de contrôle habilité à le faire.

Chaque entité établit annuellement une mesure d'écart à la PGSSI, identifie les axes d'amélioration et élabore un plan d'action comportant les objectifs, le budget, les porteurs des actions et l'échéancier. Elle contribue à l'accroissement de la protection des systèmes d'information du ministère.

Article 11. Contrôle interne

Au niveau de l'entité, des contrôles internes de conformité et de mise en œuvre du plan d'action sont effectués, le cas échéant avec l'appui de prestations externes (cf. Annexe B).

Le contrôle interne s'adresse plus particulièrement aux RSSI et AQSSI mais aussi aux responsables des services support informatique, des centres d'hébergement et des réseaux ainsi qu'aux responsables de maîtrises d'ouvrage et d'œuvre applicatives (liste non exhaustive).

Il est recommandé de formaliser le processus et le plan de contrôle et de communiquer auprès des agents et de la hiérarchie. Ce contrôle n'est pas antinomique du contrôle hiérarchique et fonctionnel.

Article 12. Contrôle externe

Au regard de leur domaine de compétence, l'ANSSI, le HFDS, le FSSI, les corps d'inspection, procèdent aux contrôles externes. L'entité met en œuvre les mesures correctives et les portent à connaissance du service de contrôle concerné.

Le FSSI, pour le compte du HFDS et HFDS Adjoint, assure la bonne conduite des actions de contrôle visant à vérifier la conformité des dispositions prises par les entités avec les exigences de la présente instruction. Il produit à l'échelle du ministère une synthèse globale des mesures d'écarts et des plans d'action établis par les entités.

Il établit le bilan annuel de sécurité des systèmes d'information du ministère à partir du résultat des contrôles menés et des informations communiquées annuellement par les entités (cf. Annexe B).

Ce bilan comporte :

- un état d'avancement de l'organisation en sécurité et de l'application des règles édictées par la PGSSI ;
- des indicateurs permettant d'appréhender la maturité générale en termes de SSI ;
- un suivi des actions réalisées pour la mise en conformité à la PGSSI ;
- une synthèse de l'état d'avancement de la cartographie des SI et de son actualisation ;
- une revue des incidents significatifs constatés et des dispositions mise en œuvre pour les résoudre ;
- un récapitulatif des exercices menés précisant les enseignements associés et un descriptif synthétique des plans d'action qui en sont issus.

Le bilan annuel permet de connaître le niveau de sécurité global du ministère. Il est soumis au CSSI, validé par le haut fonctionnaire de défense et de sécurité (HFDS) et est tenu à disposition de l'ANSSI.

Ministère de l'Écologie, du Développement durable et de l'Énergie
Ministère du Logement, de l'Égalité des territoires et de la Ruralité

Secrétariat général

Tour Pascal A

92055 La Défense cedex

Tél. : 01 40 81 21 22

www.developpement-durable.gouv.fr – www.territoires.gouv.fr