PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

DISPOSITIFS RÉGLEMENTAIRES DE SÉCURITÉ pilotés par le SGDSN

Protection du secret de la défense nationale (PSDN)

La **PSDN** vise à protéger les informations et supports dont la divulgation à des personnes non autorisées est de nature à nuire à la sécurité et à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Susceptible d'intervenir dans tous les domaines de l'action gouvernementale (notamment politique, militaire, diplomatique, économique ou industriel), **la PSDN participe ainsi de la sauvegarde des intérêts fondamentaux de la Nation.**

En fonction de leur degré de sensibilité, **trois niveaux de classification** peuvent être utilisés : Très Secret-Défense, Secret-Défense et Confidentiel-Défense.

Chacun de ces niveaux accorde une **protection proportionnée au risque encouru** en cas de divulgation des informations et supports classifiés qu'ils couvrent.

Protection du potentiel scientifique et technique de la nation (PPST)

Le dispositif de la **PPST** s'adresse aux établissements publics ou privés en vue de **protéger les savoirs et savoir-faire stratégiques ainsi que les technologies sensibles qui concourent aux intérêts fondamentaux de la Nation.**

Le dispositif offre une protection juridique et administrative fondée sur le contrôle des accès à ces informations stratégiques ou sensibles.

La réglementation prévoit en particulier la délimitation de zones protégées appelées **« zones à régime restrictif » (ZRR)** abritant les activités de recherche ou de production stratégiques ou sensibles à protéger au sein de l'établissement.

L'adhésion au dispositif et son application reposent sur une concertation entre l'entité qui héberge le potentiel à protéger et le ministère compétent.

Sécurité des activités d'importance vitale (SAIV)

La **SAIV** constitue le cadre permettant d'associer les **opérateurs d'importance vitale (OIV),** publics ou privés, à la mise en œuvre de la stratégie de sécurité nationale en termes de **protection contre les actes de malveillance (terrorisme, sabotage) et les risques naturels, technologiques et sanitaires.**

Les opérateurs d'importance vitale sont désignés par le ministre coordonnateur du secteur qui les sélectionne parmi ceux qui exploitent ou utilisent des **installations indispensables à la vie de la Nation** et qui concourent à la production et à la distribution de biens ou de services indispensables à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense ou à la sécurité de la Nation.

Dispositif NIS – Opérateurs de services essentiels (OSE)

Le dispositif de sécurité des systèmes d'information des **OSE** découle de la directive européenne 2016/1148 (directive « NIS »).

Ce dispositif vise à renforcer, face aux menaces cyber, la **sécurité des systèmes d'information des opérateurs qui fournissent des services essentiels au fonctionnement de l'économie ou de la société.**

Les OSE sont désignés par arrêté du Premier ministre sur proposition des ministres compétents et le cas échéant de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Les OSE ainsi désignés sont tenus d'identifier leurs **systèmes d'information « essentiels » (SIE)** nécessaires à la fourniture de services essentiels et de les déclarer à l'ANSSI. Ils doivent appliquer à ces SIE des règles de sécurité fixées par arrêté du Premier ministre et déclarer à l'ANSSI les incidents de sécurité affectant ces systèmes.

		Protection du secret de la défense nationale (PSDN)	Protection du potentiel scientifique et technique de la nation (PPST)	Sécurité des activités et des systèmes d'information d'importance vitale (SAIV et SIIV)	Opérateurs de services essentiels (OSE)
OBJECTIF		Protéger les informations et supports dont la divulgation à des personnes non autorisées est de nature à nuire à la sécurité et à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale	Protéger les savoirs et savoir-faire scientifiques ou techniques dont la captation pourrait nuire aux intérêts fondamentaux de la nation que ce soit vis-à-vis de risques économiques, terroristes, de prolifération d'armements conventionnels ou de destruction massive	Protéger les installations et les systèmes d'information qui fournissent des biens et des services indispensables au fonctionnement et à la continuité d'activité de la nation contre tous types de risques	Protéger les systèmes d'information essentiels (SIE) des opérateurs fournissant des services essentiels (OSE) au fonctionnement de la société ou de l'économie
PÉRIMÈTRE	Eléments à protéger	Procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers, quels qu'en soient la forme, la nature ou le mode de transmission, qu'ils soient élaborés ou en cours d'élaboration, ayant fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès	Ensemble des biens matériels et immatériels propres à l'activité scientifique fondamentale ou appliquée et au développement technologique de la nation	Points d'importance vitale (sites physiques) et systèmes d'information d'importance vitale des opérateurs d'importance vitale (OIV)	Composants matériels et logiciels des systèmes d'information essentiels nécessaires à la fourniture des services essentiels au fonctionnement de la société ou de l'économie
	Modalités d'accès au dispositif	Besoin de connaître ou d'accéder à des informations et supports classifiés pour l'exercice d'une fonction ou l'accomplissement d'une mission attestée par l'autorité administrative compétente	Concertation entre l'entité, publique ou privée, hébergeant le potentiel à protéger et le ministère compétent	Désignation de l'opérateur d'importance vitale par le ministère coordonnateur	Désignation par l'État, par arrêté du Premier ministre, après consultation de l'opérateur et du ministère compétent
MESURES DE PROTECTION		• Accès strictement limité aux personnes habilitées à un niveau supérieur ou égal au niveau requis et disposant du besoin d'en connaître • Traçabilité des informations et supports classifiés tout au long du cycle de vie (enregistrement, conservation, reproduction, diffusion, acheminement, archivage, destruction) • Homologation de sécurité des systèmes d'information contenant des informations classifiées • Protection physique des lieux abritant des informations et supports classifiés avec, le cas échéant, institution de zones protégées ou réservées auxquelles l'accès est réglementé • Responsabilité pénale en cas de manquement à ces obligations	• Délimitation de zones à régime restrictif (ZRR) dont l'accès physique ou logique est réglementé • Autorisation d'accès délivrée par l'entité, après avis favorable du ministre compétent • Mise en œuvre d'une politique de protection des systèmes d'information • Concertation continue avec les services de l'État pour accompagner la mise en œuvre et adapter si nécessaire la protection	• Les opérateurs sont tenus de garantir la sécurité de leurs points d'importance vitale (protection physique et logique) • Homologation de sécurité du SIIV et mise en œuvre de produits et de services de détection qualifiés par l'ANSSI • Protection complétée par l'action des services de l'État coordonnés par le préfet de département • Obligation de réaliser un plan de continuité d'activité (PCA)	L'accès aux systèmes d'information essentiels doit être techniquement protégé par l'application des règles de sécurité relatives à l'identification, à l'authentification et aux droits d'accès
POINTS DE CONTACT	Administration	Ministère de rattachement (service du haut fonctionnaire de défense et de sécurité)	Ministère de rattachement (service du haut fonctionnaire de défense et de sécurité)	• Ministère coordonnateur du secteur d'activité de l'opérateur (service du haut fonctionnaire de défense et de sécurité) • Préfecture de département du point d'importance vitale	L'agence nationale de la sécurité des systèmes d'information (ANSSI) contrôle la mise en œuvre du dispositif et notamment le niveau de sécurité des SIE
	Entité	Officier de sécurité	• Une personne désignée responsable de la ZRR par l'entité • Officier de sécurité ou fonctionnaire de sécurité et défense	Délégué à la défense et à la sécurité	Une personne désignée par l'entité pour assurer le lien avec l'ANSSI
BASE JURIDIQUE	Principes	• Organisation de la protection du secret de la défense nationale : article R. 2311-1 à R. 2311-11 du code de la défense • Protection des zones protégées : articles 413-7 et R. 413-1 à R. 413-5 du code pénal • Atteintes au secret de la défense natio nale : articles 413-9 à 414-9 du code pénal	• Protection des zones protégées : articles 413-7 et R. 413-1 à R. 413-5 du code pénal • Réglementation de l'accès aux ZRR : article R. 413-5-1 du code pénal • Organisation de la protection : décret 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 et relatif à la protection du potentiel scientifique et technique de la nation	• Protection des missions d'importance vitale : articles L. 1332-1 et suivants et R.1332-1 et suivants du code de la défense • Arrêtés sectoriels pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense	• Directive (UE) 2016/1148 du 6 juillet 2016 relatif aux mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive « NIS ») • Loi 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'UE dans le domaine de la sécurité • Décret 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et système d'information des OSE et des fournisseurs de service numérique
	Déclinaisons opérationnelles	Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale approuvée par arrêté du 30 novembre 2011	• Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation • Circulaire interministérielle n° 3415 du 7 novembre 2012 de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation	Instruction générale interministérielle n° 6600 du 7 janvier 2014 relative à la sécurité des activités d'importance vitale	Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018

POUR ALLER PLUS LOIN

À propos du SGDSN

Service du Premier ministre travaillant en liaison étroite avec le Président de la République, le secrétariat général de la défense et de la sécurité nationale (SGDSN) assiste le chef du Gouvernement dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. À ce titre il prépare la réglementation interministérielle, en assure la diffusion et en suit l'application.

www.sgdsn.gouv.fr

À propos de l'ANSSI

Rattachée au SGDSN, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. L'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

www.ssi.gouv.fr

PSDN

Protection du secret de la défense nationale

http://www.sgdsn.gouv.fr/missions/proteger-le-secret-de-la-defense-et-de-la-securite-nationale/

PPST

Protection du potentiel scientifique et technique de la nation

http://www.sgdsn.gouv.fr/missions/protection-du-potentiel-scientifique-et-technique-de-la-nation/

https://www.ssi.gouv.fr/guide/protection-du-potentiel-scientifique-et-technique-de-la-nation/

Foire aux questions

http://www.sgdsn.gouv.fr/missions/protection-du-potentiel-scientifique-et-technique-de-la-nation/le-dispositif-de-protection-du-potentiel-scientifique-et-technique-de-la-nation-faq/

SAIV

Sécurité des activités d'importance vitale

www.sgdsn.gouv.fr/communication/la-securite-des-activites-dimportance-vitale

www.ssi.gouv.fr/administration/protection-des-oiv/protection-des-oiv-en-france/

Foire aux questions

www.ssi.gouv.fr/administration/protection-des-oiv/foire-aux-questions/

OSE

Sécurité des systèmes d'information des opérateurs de services essentiels

www.ssi.gouv.fr/entreprise/reglementation/directive-nis/

Foire aux questions

www.ssi.gouv.fr/entreprise/reglementation/directive-nis/faq-operateurs-de-services-essentiels-ose/

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
sgdsn.gouv.fr

Maquette : Pôle Graphisme, Fabrication, Déplacements, Images – DSAF/DPSG – Juin 2020.