POUR ALLER PLUS LOIN

PROTECTION DU SECRET DE LA DÉFENSE NATIONALE

www.sgdsn.gouv.fr/missions/proteger-le-secret-de-la-defense-nationale

SÉCURITÉ DES ACTIVITÉS D'IMPORTANCE VITALE

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

PROTECTION DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION

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

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Les mesures d'hygiène informatique

Non exhaustives, les 42 mesures d'hygiène informatique représentent le socle minimum à respecter pour protéger les informations de son entité.

www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

L'HOMOLOGATION DE SÉCURITÉ

La démarche d'homologation est un processus d'information et de responsabilisation qui aboutit à une décision du responsable de l'organisation quant à :

- ▷ l'attestation de sa connaissance du système d'information et des mesures de sécurité (techniques organisationnelles ou juridiques) mises en œuvre
- ▷ l'acceptation des risques qui demeurent, qu'on appelle « risques résiduels »

www.ssi.gouv.fr/uploads/2014/06/guide_homologation_de_securite_en_9_etapes.pdf

A 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.

www.sgdsn.gouv.fr

A PROPOS DE L'ANSSI

Rattaché 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

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

51, boulevard de La Tour-Maubourg
75700 Paris SP 07
01 71 75 80 11
sgdsn.gouv.fr

Maquette : Pôle graphique, fabrication, déplacements, image – DSAF/DPL – Mai 2018.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

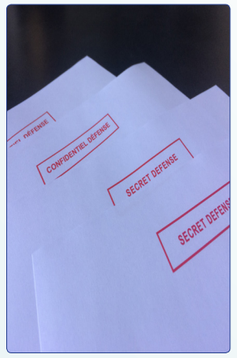
PREMIER MINISTRE

DISPOSITIFS RÉGLEMENTAIRES DE SÉCURITÉ DU SGDSN

En application des articles R. *1132-1 à R. *1132-3 du code de la défense, le secrétaire général de la défense et de la sécurité nationale assiste le Premier ministre 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 dans les domaines suivants :

- ▷ la protection du secret de la défense nationale ;
- ▷ la sécurité des activités d'importance vitale ;
- ▷ la protection du potentiel scientifique et technique de la nation.

PROTECTION DU SECRET DE LA DÉFENSE NATIONALE



Le secret de la défense nationale contribue à la sécurité de notre pays en protégeant des informations dont la diffusion nuirait à ses intérêts fondamentaux. La sensibilité de ces informations implique une protection particulière, permettant d'en maîtriser et d'en limiter la diffusion.

Peuvent ainsi être protégés au titre du secret de la défense nationale les informations et supports classifiés (documents, matériels, informations, réseaux informatiques, etc.) **dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.** 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.

SÉCURITÉ DES ACTIVITÉS D'IMPORTANCE VITALE

Le dispositif de sécurité des activités d'importance vitale (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.

PROTECTION DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION

Le dispositif de protection du potentiel scientifique et technique de la nation (PPST) s'adresse aux établissements publics ou privés. Il a pour but de protéger leurs **savoirs et savoir-faire stratégiques ainsi que les technologies sensibles** qui concourent aux intérêts fondamentaux de la Nation.

Le dispositif PPST offre une **protection juridique et administrative** fondée sur le contrôle des accès aux informations stratégiques ou sensibles détenues.

La réglementation prévoit **l'identification de zones protégées appelées « zones à régime restrictif » (ZRR) abritant les activités de recherche ou de production stratégiques de l'établissement.**

SGDSN
SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

			PROTECTION DU SECRET DE LA DÉFENSE NATIONALE PSDN	SÉCURITÉ DES ACTIVITÉS D'IMPORTANCE VITALE SAIV	PROTECTION DU POTENTIEL SCIENTIFIQUE ET TECHNIQUE DE LA NATION - PPST
CARACTÉRISTIQUES PRINCIPALES DU DISPOSITIF	**Objectif**		Protection des informations et supports relevant du secret de la défense nationale	Protection des installations qui fournissent des biens et des services indispensables au fonctionnement de la nation	Protection physique et informatique des savoirs, savoir-faire et technologies sensibles des établissements publics et privés, reconnus comme des intérêts souverains
	Périmètre		Informations et supports classifiés et systèmes d'information associés	Points d'importance vitale et systèmes d'information d'importance vitale	Zone protégée qualifiée de zone à régime restrictif (ZRR) et systèmes d'information associés
	Base juridique	**Principes**	Protection du secret de la défense nationale : articles 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 nationale : articles 413-9 à 414-9 du code pénal	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	Protection des zones protégées : articles 413-7 et R.413-1 à R.413-5 du code pénal Protection des intêrets fondamentaux de la nation : article 410-1 du code pénal
		Déclinaisons opérationnelles	Instruction générale interministérielle n°1300 relative à la protection du secret de la défense nationale, portée par l'arrêté du 30 novembre 2011	Instruction générale interministérielle relative à la sécurité des activités d'importance vitale n°6600/SGDSN/PSE/PSN du 7 janvier 2014	Circulaire interministérielle de mise en œuvre du dispositif de protection du potentiel scientifique et technique de la nation n°3415/SGDSN/AIST/PST du 7 novembre 2012
	Préalables nécessaires		Habilitation au secret de la défense nationale	Après consultation de l'opérateur, désignation par l'Etat (arrêté du ministre coordonateur du secteur d'activités)	Adhésion sur volontariat de l'établissement hébergeant le potentiel protégé
	Types de menaces pris en compte		Divulgation ou captation d'information intéressant tous les domaines d'activité relevant de la défense et de la sécurité nationale (politique, militaire, scientifique, économique, etc.) susceptible de nuire aux intérêts fondamentaux de la nation	Approche « tous risques » : actes de malveillance (terrorisme, sabotage, etc.), menaces cyber, risques naturels, technologiques, sanitaires	Pillage des conaissances stratégiques, notamment captation des savoirs qui peuvent être détournés à des finalités économiques, d'arsenal militaire conventionnel, de prolifération des armes de destruction massive et de terrorisme
	Risques encourus		Compromission du secret de la défense nationale	Arrêt de l'activité d'importance vitale Altération du système d'information d'importance vitale (SIIV)	Captation de savoirs et savoir-faire
	Nature de la protection		Juridique, physique, logique	Physique et logique	Juridique, administrative et logique
FONCTIONNEMENT DU DISPOSITIF	**Site ou bâtiment ou local à protéger**		Zone protégée voire zone réservée	Point d'importance vitale	Zone à régime restrictif (ZRR), catégorie de zone protégée
	Biens matériels ou immatériels à protéger		Procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers relevant du secret de la défense nationale	Composants névralgiques du point d'importance vitale Composants matériels et logiciels du système d'information d'importance vitale	Savoirs, savoir-faire et technologies sensibles et innovantes
	Mesures de protection des systèmes d'information		L'homologation de sécurité des systèmes amenés à traiter des informations relevant du secret de la défense nationale	Les règles de sécurité mentionnées dans les arrêtés sectoriels qui exigent, notamment, l'homologation de sécurité du SIIV et la déclaration des incidents de sécurité affectant le SIIV	Les ZRR doivent, au minimum, se doter d'une PSSI et désigner un RSSI
	Conditions d'accès aux éléments protégés		Procédure d'habilitation obligatoire motivée par le besoin d'en connaître pour accéder aux informations et supports classifiés. L'accès en zone protégée ou zone réservée est soumis à l'autorisation du responsable de site	Demande d'accès facultative : L'OIV a la possibilité de demander à l'autorité administrative de vérifier que les caractéristiques de la personne souhaitant accéder physiquement à son PIV ne sont pas incompatibles avec la sécurité du site concerné	Demande d'accès obligatoire : 1°) Le demandeur formalise sa demande au moyen d'un formulaire type et le transmet au chef de la ZRR qui peut compléter le formulaire ; 2°) Le chef de la ZRR transmet pour avis au ministre qui analysera la demande à l'aide d'une enquête administrative et une évaluation scientifique
	Avis de l'autorité administrative avant d'autoriser l'accès		Contraignant (décision d'habilitation ou de refus d'habilitation)	Non contraignant	Seul l'avis négatif du ministère est contraignant
	Contrôle de la mise en œuvre du dispositif		Le SGDSN veille au respect des dispositions applicables au niveau Très Secret-Défense. Pour les niveaux Confidentiel-Défense et Secret-Défense, chaque ministère s'assure, par délégation, de la mise en œuvre des mesures de sécurité par tout organisme public (administration, etc.) et privé (entreprise, etc.)	Les commissions zonales de défense et de sécurité contrôlent la mise en œuvre du dispositif de protection des PIV (à l'exception des PIV militaires) L'agence nationale de la sécurité des systèmes d'information (ANSSI) contrôle le niveau de sécurité des SIIV	L'administration apporte ses conseils aux responsables de la zone à régime restrictif afin d'élever son niveau de sécurité
	Points de contact		Administration : service du haut fonctionnaire de défense et de sécurité (HFDS)	Administration : service du haut fonctionnaire de défense et de sécurité (HFDS)	Administration : service du haut fonctionnaire de défense et de sécurité (HFDS)
			Etablissement : officier de sécurité	Etablissement : délégué pour la défense et la sécurité	Etablissement : chef de la zone à régime restrictif