SECURITE DES
ACTIVITES D'IMPORTANCE VITALE



GUIDE D'AIDE
A L'ELABORATION ET L'EXAMEN
D'UN PLAN PARTICULIER DE PROTECTION


VIGIPIRATE

2 juillet 2018

SGDSN

Ce guide a pour objet de constituer une aide à l'élaboration et à l'examen du *plan particulier de protection* (PPP). Il donne des indications et recommandations qui n'ont pas une valeur contraignante.

Le PPP doit se conformer au plan-type fixé par arrêté du Premier ministre. Si, lors de la rédaction du PPP, l'opérateur constate qu'un chapitre n'est pas applicable pour son *point d'importance vitale* (PIV), il peut indiquer la mention « néant » ou « non applicable ».

Pour faciliter la lecture, le PPP doit être paginé et le sommaire doit figurer au début du document.

Rappel de la procédure d'approbation du PPP

La décision d'approbation du préfet de département se fonde sur une évaluation qualitative du PPP soumis par l'opérateur. Cette évaluation prend en compte :

- *l'avis de la CZDS s'il a été sollicité ;*
- *la conformité du plan particulier de protection par rapport au plan-type ;*
- *la cohérence du dispositif proposé au regard de la politique générale de protection définie par le PSO ;*
- *la prise en compte des prescriptions de la DNS qui s'appliquent au PIV, notamment les scénarios de menace et les objectifs de sécurité ;*
- *l'adéquation du dispositif proposé aux infrastructures et aux modalités d'exploitation du PIV.*

Instruction générale interministérielle relative à la sécurité des activités d'importance vitale n° 6600/SGDSN/PSE/PSN du 7 janvier 2014

Suivi des modifications

Date	Version n°	Auteur / service	Commentaires

Préambule

Le préambule vise à rappeler les enjeux du dispositif SAIV et l'objectif attendu du PPP. S'il ne contient aucune information classifiée, le préambule peut être extrait du PPP et déclassifié de manière à présenter la démarche du PPP auprès de personnels non-habilités (membres du comité exécutif, instances représentatives du personnel, *etc.*).

Le préambule peut également indiquer le circuit de validation du document, sa version et la dernière mise à jour.

Les documents ressources dans la rédaction ou l'examen du PPP

Plusieurs documents peuvent faciliter la rédaction, la compréhension et l'instruction du PPP :

- l'instruction générale interministérielle relative à la sécurité des activités d'importance vitale n° 6600/SGDSN/PSE/PSN du 7 janvier 2014 ;
- le plan de sécurité d'opérateur (pour la compréhension de l'activité de l'opérateur, les scénarios retenus, les objectifs de sécurité, le choix du PIV, *etc.*) ;
- la directive nationale de sécurité du secteur (pour les scénarios notamment) ;
- le plan VIGIPIRATE (pour les mesures applicables) ;
- les éventuels comptes rendus de visites de la commission zonale de défense et de sécurité.

1. Présentation du point d'importance vitale

1.1. Désignation du PIV

Critères de désignation du PIV

Les critères peuvent figurer dans le PSO de l'opérateur.

- Nom de la société et adresse complète.
- N° de triplet attribué par le SGDSN et figurant dans l'arrêté de désignation du PIV.
- Nature des activités.
- Secteur(s) et *directive(s) nationale(s) de sécurité* (DNS) de rattachement.
- Lien avec l'opérateur d'importance vitale (filiale, *etc.*).
- Critères retenus pour la désignation du site comme PIV.
- Classement éventuel du site au titre d'autres réglementations et plans applicables (installation classée pour la protection de l'environnement, Seveso, installations portuaires relevant du code ISPS, site abritant des matières nucléaires, IGH, ERP, *etc.*).
- Surface totale du PIV.

1.2. Localisation du PIV

- Plan d'accès lisible et pratique pour des interventions externes (routes d'accès, différentes entrées, *etc.*).
- Plan de masse du site.
- Site situé en zone police ou gendarmerie.
- Description de l'environnement (urbain ou rural, zone résidentielle ou industrielle, proximité d'axes routiers et/ou ferroviaires).
- Zonage spécifique au titre d'autres réglementations (existence d'une zone protégée, d'une zone à régime restrictif, d'une zone de défense hautement sensible, d'une zone nucléaire à accès réglementé, *etc.*).

1.3. Organisation générale du PIV

- Site ouvert ou fermé au public.
- Effectifs employés sur le site (salariés, prestataires, *etc.*).
- Présence sur le site 24/7.
- Organisation hiérarchique (avec un organigramme).
- Rôle et responsabilités du délégué à la défense et à la sécurité du site.

2. Analyse de risque

2.1. Cartographie des risques

> ***Analyse de risque du PPP et du PSO***
> Si l'analyse de risque spécifique au PIV est déjà menée dans le PSO de l'opérateur, ce dernier peut la copier à cet emplacement ou renvoyer au document.

L'analyse de risque doit permettre à l'opérateur d'identifier les scénarios les plus pertinents pour son site au regard de sa situation, son environnement, ses retours d'expérience, ses vulnérabilités. Il définit ainsi les priorités de sa politique de sécurité en s'appropriant la DNS et son PSO (notamment en reprenant les scénarios de menace qui y sont présentés). Il complète ces scénarios par ceux qu'il estime pertinents au regard de son activité, de sa situation.

NB. L'analyse de risque doit notamment tenir compte des nouvelles orientations de la DNS en intégrant les risques de cybersécurité et les risques naturels, technologiques, pandémiques, *etc*.

2.2. Vulnérabilités spécifiques du site

Vulnérabilités propres à l'activité et l'environnement du site (exemples : site ouvert au public, proximité de grands axes de circulations, de sites industriels, zones de fragilités, bâtiments mitoyens).

2.3. Interdépendances

Mise en évidence des interdépendances (exemple : nécessité de disposer d'une alimentation électrique permanente pour assurer le fonctionnement des systèmes de sécurité, recours à des prestataires essentiels, à des matières premières non substituables).

2.4. Points névralgiques

Identification des points névralgiques du PIV par leur importance, leur sensibilité. L'arrêt ou la destruction du point névralgique peut conduire à un arrêt des activités du site et/ou à un problème de sécurité. Il s'agit, par définition, d'un élément difficilement substituable.

Donner la justification du choix des points névralgiques.

Cartographie des points névralgiques

Le fait de matérialiser les points névralgiques sur une carte permet de se rendre compte du périmètre concerné et également du respect du principe de défense en profondeur.

Ces points névralgiques peuvent également correspondre aux parties que l'opérateur souhaite soumettre à une enquête administrative préalable (*cf.* article R. 1332-22-1 du code de la défense).

3. Dispositifs de sûreté en place ou prévus

3.1. Moyens humains

3.1.1. Service de sécurité/sûreté

- Nom de la société.
- Missions des agents (exemples : contrôle et surveillance des entrées/sorties, de la circulation interne, de la sécurité technique, *etc.*).
- Effectifs employés.
- Présence sur le site.
- Rythme des rondes.
- Qualité des agents (internes ou prestataires).
- Qualifications et formations particulières (emploi de chiens de défense, de chiens pour la détection d'explosifs, port d'armes, *etc.*).

3.1.2. PC de sécurité et sûreté (PCS)

- Description du PC : localisation (sur le site ou distant), dispositifs de secours, site de secours.
- Nombre d'agents présents (jour/nuit/week-end).
- Outils de communication et moyens de supervision à disposition.
- Autres moyens matériels.
- Rôle du PCS en en cas de crise (armement spécifique).

3.2. Dispositifs de protection physique

3.2.1. Protection des points névralgiques et respect du principe de « défense en profondeur »

Stratégie de protection des points névralgiques dans le respect du principe de défense en profondeur et de l'équation de protection.
Orientations principales de la stratégie de protection (détection, dissuasion, protection, dissimulation, *etc.*).

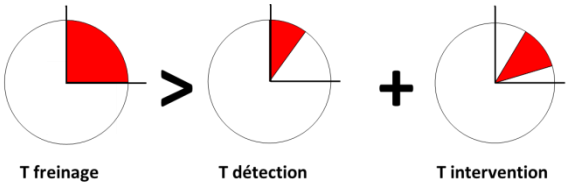
Le principe de défense en profondeur, avec la sectorisation générale du PIV en nombre de « couches » successives, doit être décrit de façon à expliciter l'articulation des dispositifs de protection, de la périphérie aux points névralgiques. Si ça s'avère pertinent, les différents dispositifs de protection peuvent figurer sur un ou plusieurs plans et être joints au PPP.

La défense en profondeur

La défense en profondeur consiste en la superposition de plusieurs lignes de défense, composées d'un ensemble de mesures de sécurité, chaque ligne devant contribuer à affaiblir l'attaque et à permettre aux suivantes de se renforcer en vue soit d'empêcher la destruction ou la prise de contrôle des composants névralgiques du PIV, soit d'en limiter les effets.

L'équation de protection

Le temps de résistance mécanique des dispositifs installés doit être supérieur au temps de détection de l'attaque (et de transmission de l'information) ajouté au temps d'intervention.



3.2.2. Clôtures, murs, portes, portails d'accès, obstacles retardateurs

- Clôture périmétrique (hauteur, résistance, *etc.*).
- Dispositif masquant la vue depuis l'extérieur (éléments naturels, *etc.*).
- Sécurisation des ouvrants (fenêtres, portes, *etc.*).
- Obstacles retardateurs (concertina, *etc.*).
- Sas d'entrée.
- Parking.
- Panneautage signalant une zone protégée ou un site sensible.
- Fonctions principales des dispositifs (freiner, dissuader, dissimuler, tromper, *etc.*).

3.2.3. Vidéoprotection

- Politique de vidéoprotection (aux entrées, à l'intérieur des bâtiments, pour les points névralgiques identifiés, donnant sur la voie publique, *etc.*)
- Spécificités techniques (enregistrement, qualité, détecteur de mouvement, caméras discrètes, infrarouge, *etc.*).
- Fonctions principales du dispositif de vidéoprotection (détecter, surveiller, lever de doute, dissuader, *etc.*).

Vidéoprotection de la voie publique

La vidéoprotection de la voie publique aux abords immédiats d'un site privé, peut être mise en œuvre par les autorités publiques aux fins de prévention d'actes de terrorisme. Cette mise en œuvre répond à des règles strictes (*cf.* code L. 223-1 du code de la sécurité intérieure).

3.2.4. Contrôle d'accès

- Badges (caractéristiques de la politique de gestion des badges, accès restrictifs par lieux/plages horaires, passage unique, technologie utilisée pour les badges, *etc.*).
- Biométrie (existence de contrôle biométrique, localisation, *etc.*).

- Clés (politique de gestion des clés, clés non copiables, *etc*.).
- Contrôle des véhicules.
- Fonctions principales du dispositif de contrôle d'accès (détecter, recenser, freiner, sectoriser, *etc.*).

3.2.5. Eclairage

- Efficacité des installations choisies : surface éclairée, déclenchement automatique.
- Fonctions principales du dispositif d'éclairage (dissuader, détecter, intervenir, *etc.*).

3.2.6. Protection des approches terrestres

- Ralentisseur, chicanes, barrières anti-véhicules bélier, *etc.*

3.2.7. Détection d'intrusion

- Contacteurs de porte, détecteurs bris de vitre, détecteurs volumétriques, détecteurs thermiques, gestion des alarmes, *etc.*

3.2.8. Protection des systèmes de sécurité

- Exemples de protections techniques : gaines spéciales, autonomie des systèmes, vérification de l'inviolabilité des badges, *etc.*

3.2.9. Systèmes de secours

- Moyens de production autonomes prévus permettant la continuité des systèmes de sécurité (description des moyens, autonomie).

3.3. Audits et contrôle

Vérification des dispositifs de sécurité, du respect des règles et procédures de sécurité (catégorie de l'audit/contrôle, périodicité, prise en compte des conclusions).
Prise en compte de tout élément utile tiré d'autres évaluations de sûreté (exemple : réglementation ISPS, évaluation de sûreté bâtimentaire réalisée par la DGSI, audit interne de l'opérateur).

3.4. Gestion des colis et du courrier

Procédure spécifique en matière de sûreté pour la gestion des colis et courrier entrants.

3.5. Gestion et stockage de l'information classifiée

- Conservation des documents classifiés selon les dispositions de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale du 30 novembre 2011 (coffre, local protégé, *etc*.).
- Mise en place d'une zone protégée.
- Définition des responsabilités.

> ***La zone protégée***
> L'objet de la zone protégée est d'assurer, aux lieux intéressant la défense nationale, une protection juridique contre les intrusions, complémentaire d'une protection physique (*cf. article 413-7 du code pénal*).

4. Sécurité des systèmes d'information

- Existence d'une *politique de sécurité des systèmes d'information* (PSSI). PSSI locale ou « groupe ».
- Autres documents d'application.
- Liste des principaux systèmes d'information du site, décrits de la façon synthétique suivante :
    - SI métier, SI bureautique, SI de sécurité/sûreté, SI industriel.
    - Indication de la criticité du système pour l'entreprise / pour les impacts sur les populations / *etc*.
    - Où est hébergé le système (à distance, localement) ?
    - Responsabilités :
        - Qui gère/administre le système ?
        - Le cas échéant, qui est en charge de la cybersécurité du système (éventuellement, distinguer l'aspect « gouvernance » et l'aspect « opérationnel ») ?
        - Y a-t-il un ou plusieurs prestataires « clés » dont la mise en œuvre du SI dépend fortement ?
- Description des dispositifs de sauvegarde des données existants.
- Dispositifs de secours permettant la continuité des systèmes métiers (description des moyens, autonomie).

> ***L'analyse de risque SSI***
> L'analyse de risque menée dans le cadre d'un PPP n'a pas vocation à aborder le sujet des systèmes d'information autrement que de façon synthétique, sans rentrer dans le détail technique. La DNS inclut des scénarios cyber qui sont ensuite repris dans le PSO ou le PPP.

5. Lien avec le plan VIGIPIRATE

Les OIV font apparaître dans leurs PSO et PPP les mesures qu'ils sont susceptibles de mettre en œuvre pour atteindre les objectifs de sécurité de leur domaine d'action, qui figurent dans la ou les directives nationales de sécurité qui leur sont applicables.

Le principe est que l'activation nationale de n'importe laquelle des mesures VIGIPIRATE puisse donner lieu immédiatement à une action concrète au sein du PIV, décrite dans le PPP. D'une manière générale, la déclinaison peut rester succincte mais il faut que l'opérateur ait anticipé sa réaction.
La déclinaison des mesures permet de s'assurer qu'il les a bien intégrées en amont et ainsi qu'il a prévu une application graduée de ces mesures.

NB. Toutes les mesures ne nécessitent pas une déclinaison concrète par l'opérateur. En effet, certaines mesures peuvent être suffisamment explicites pour ne pas à avoir à être déclinées (exemple : « ALR 20-01 Elaborer et mettre à jour un plan de continuité d'activité »).
Ou bien, une déclinaison serait redondante avec les mesures décrites par ailleurs dans le PPP (exemple : « BAT 10-02 Surveiller les abords des installations et bâtiments »).

Exemples de déclinaison de mesures du plan VIGIPIRATE :

Numéro de mesure	Mesures	Type de mesure	Prise en compte par l'opérateur : Oui/Non/Non applicable	Précisions sur les dispositions prises par l'opérateur
BAT 31-01	Renforcer la surveillance interne et limiter les flux (dont interdiction de zone)	additionnelle	*Oui*	*En cas d'activation de cette mesure, un seul des deux accès du PIV est maintenu et le contrôle visuel des bagages est systématisé. Un agent privé de sécurité vient renforcer l'accueil et participe aux contrôles.*
ALR 11-04	Rappeler les conduites à tenir en réponse à la menace d'actions terroristes (fusillade, colis abandonné, alerte à la bombe)	additionnelle	*Oui*	*En cas d'activation de cette mesure et en complément des mesures de sensibilisation décrites en 7.1, une session de sensibilisation du personnel peut être organisée par notre personnel de sûreté et un message de sensibilisation est diffusé sur nos panneaux d'affichage.*

6. Procédure d'alerte et de gestion de crise

6.1. Astreinte

- Rôles et fonctions du personnel d'astreinte.
- Fonctionnement (H24 ? délai d'intervention sur site ?)

NB. Les numéros peuvent figurer en annexe.

Missions de l'astreinte

Selon les organisations, une astreinte peut avoir été constituée pour répondre à des événements spécifiques (ex. : maintenance, incident sanitaire, etc.)
Néanmoins, l'opérateur doit s'interroger si ce dispositif est également efficace face à tout type de scénario susceptible d'interrompre ses activités (ex. : acte de malveillance, arrêt des activités, panne des SI, etc.).

6.2. Schéma d'alerte

Chaîne de remontée de l'alerte vers :

- les autorités de décision interne ;
- les autorités administratives (services préfectoraux, forces de sécurité intérieure, service du haut fonctionnaire de défense et de sécurité du ministère coordonnateur) ;
- les populations, les abonnés prioritaires si nécessaire.

Description de la procédure de « levée de doute ».

6.3. Outils d'alerte et de gestion de crise (hors salle de crise)

- Moyens de communications (téléphones filaires, mobiles, radios, haut-parleurs, interphones, internet ou intranet).

- Fiche de réaction/d'intervention spécifique à un risque encouru (pour le service de sécurité/sûreté, pour les membres de la cellule de crise).
- Consignes en cas d'alerte (consignes générales et dispositifs spécifiques selon les catégories de personnels ou d'emplois).
- Malette de crise à disposition pour le personnel d'astreinte, en salle de crise.
- Véhicule de fonction.

6.4. Organisation de crise

- Rôle et fonctionnement de la cellule de crise du PIV.
- Composition des membres de la cellule de crise (par fonction).

6.5. Salle de crise

- Localisation.
- Outils à disposition (manuel de gestion de crise, plans, *etc.*).
- Moyens de communication (dont moyens sécurisés pour les services de l'Etat).
- Existence d'un site de repli.
- Modification des consignes en cas d'alerte.

6.6. Exercices et entrainements

- Réalisation d'exercices (sur table, mise en situation). Périodicité.
- Agents concernés (cellule de crise, personnel de sûreté, ensemble du personnel, *etc.*).
- Scénarios (sécurité, sûreté, continuité d'activité, *etc.*).

6.7. Continuité d'activité

- PCA groupe, PCA de site.
- PCA abordant :
  - les scénarios d'indisponibilité du personnel, indisponibilité du site, indisponibilité du réseau informatique, indisponibilité des prestataires essentiels.
  - l'identification des missions prioritaires ;
  - les solutions de secours.
- Test du PCA (périmètre et périodicité des tests).

Continuité des activités

La continuité d'activité est un des objectifs de la révision des DNS (approche « tous risques ») et il convient donc d'y apporter une attention toute particulière. Par exemple, un PCA ne doit pas couvrir uniquement les questions de pandémie mais aussi aborder les problématiques d'indisponibilité du réseau SI, indisponibilité du bâtiment, indisponibilité des prestataires.

NB. Cette partie peut être facultative pour les opérateurs désignés au titre de l'article L. 1332-2 du code de la défense (opérateurs qui « peuvent présenter un danger grave pour la population »).

6.8. Retour d'expérience

Politique de retour d'expérience après une crise réelle, un exercice, un incident.

7. Gestion du personnel

7.1. Sensibilisation et formation

Sensibilisation

Une sensibilisation sur les questions de sûreté peut être facilement mise en œuvre à moindre coût (exemple : diffusion de l'affiche « comment réagir face à une attaque terroriste », guides de bonnes pratiques, etc.). Ces documents sont disponibles sur le site www.risques.gouv.fr

7.1.1. Sensibilisation

Sensibilisation des agents, de l'ensemble du personnel, du public, des visiteurs occasionnels.

7.1.2. Formation

- Formation des agents à la sûreté (catégorie ciblée).
- Formation à la gestion de crise (catégorie ciblée).
- Maintien des acquis (périodicité).
- Existence d'un plan de formation.

7.2. Postes sensibles et criblages

7.2.1. Postes sensibles

- Identification de postes sensibles (personnes « clés » du PIV).
- Politique pour l'attribution de postes « sensibles ».

7.2.2. Criblage

Organisation du criblage.

Criblage

Bien que le criblage ne soit pas une obligation, il représente une sécurité supplémentaire pour les PIV. Notamment pour des personnels susceptibles d'accéder seuls à des points névralgiques. (Ex. personnel de maintenance, société de gardiennage).

7.3. Services prestataires, sous-traitants

Gestion des personnels prestataires et sous-traitants (accès restreints, accompagnés sur le site, dans les points névralgiques uniquement). Information sur les règles de sécurité/sûreté.

7.4. Visiteurs

Gestion des visiteurs (accompagnés, port du badge apparent).

Annexes

A. Annuaires

Fonction	Nom	Prénom	Courriel	Numéro de téléphone fixe	Numéro de téléphone mobile	Autre fonction exercée
Poste de sécurité (joignable 24/7)						
DDS du PIV						
DDS du PIV suppléant						
DDS de l'OIV						
Directeur ou responsable du site						

Personnes à contacter

- Des adresses électroniques et des numéros de téléphone génériques limitent le risque d'avoir des annuaires obsolètes.
- En cas de changement important, l'annexe seule peut être envoyée à la préfecture pour mise à jour du PPP.