Guide de rédaction des plans particuliers de protection (PPP)

A destination des centres DGA, organismes sous tutelle DGA et industries de défense

2nde édition de février 2024– DGA/SSDI

Généralités

Le secrétariat général de la défense et de la sécurité nationale (SGDSN) a arrêté en juillet 2018 un plan-type[1] interministériel pour les plans particuliers de protection (PPP).

Afin de correspondre au mieux aux besoins et à l'approche de protection des installations relevant du ministère des Armées, la Direction de la protection des installations, moyens et activités de la défense (DPID) a adapté ce plan type[2] selon les principes suivants :

- Les dispositifs de sûreté sont décrits selon une approche fonctionnelle ;
- Une annexe récapitulant les moyens de protection mis en place pour chaque composant névralgique a été rajoutée ;
- Une annexe sur la lutte contre les drones malveillants et une autre portant sur les dispositions relatives aux risques nucléaire, radiologique, biologique et chimique (NRBC) sont désormais prévues.

Afin d'aider les opérateurs dans la rédaction de leurs PPP, le service de la sécurité de défense et des systèmes d'information (SSDI) de la direction générale de l'armement (DGA) a réalisé un guide qui se compose de trois parties :

- Le plan type du plan particulier de protection (annexe 1) qui est identique à celui fixé par la DPID et auquel l'opérateur doit se conformer ;
- Des fiches d'aide (annexe 2) qui précisent pour chaque chapitre les attendus et apportent des exemples et illustrations ;
- Un guide de rédaction de l'annexe NRBC (annexe 3).

Les modèles de rédaction des paragraphes apparaissent en vert dans le document afin d'être rapidement identifiables pour le lecteur.

Si lors de la rédaction du PPP, l'opérateur constate qu'une partie n'est pas applicable pour son point d'importance vitale (PIV), il conserve l'intitulé et mentionne « néant » ou « non applicable » en justifiant.

Le PPP finalisé doit être classifié au niveau *Secret* et porter la mention de protection *Spécial France*. Il doit être transmis par voie électronique (Intraced) ou par voie postale (clef USB, CD-ROM) à DGA/SSDI uniquement.

Pour rappel, les PPP des opérateurs relevant de la directive nationale de sécurité (DNS) « Industries de défense » sont approuvés par DGA/SSDI. Les PPP des opérateurs relevant de la DNS « Activités militaires de l'état » sont également approuvés par DGA/SSDI après avoir été au préalable validés par la DPID. Dans ce cas-là, DGA/SSDI saisit elle-même la DPID et lui communique directement le document. Enfin, concernant les PPP relevant de deux ou de plusieurs DNS, le document doit être envoyé à DGA/SSDI qui se charge ensuite de le transmettre pour avis au(x) ministère(s) concerné(s).

[1] Arrêté du 2 juillet 2018 portant approbation du plan type des plans particuliers de protection des points d'importance vitale.
[2] Note n°DEP-00119/ARM/DPID/DPP du 10 septembre 2019.

Le respect des préconisations contenues dans ce guide ne conduit pas nécessairement à une approbation automatique du PPP par DGA/SSDI qui peut être amenée à avoir des observations complémentaires.

Ce guide intègre les premières remarques formulées par les opérateurs ayant débuté la rédaction de leurs PPP. Il a vocation à être mis à jour pour prendre en compte les retours d'expérience. Un guide de rédaction de l'annexe sur la lutte anti-drones viendra compléter ce document prochainement.

Annexe 1 – Plan type du plan particulier de protection

Préambule

1. **Présentation du point d'importance vitale**
   - 1.1. Désignation du PIV
   - 1.2. Localisation du PIV
   - 1.3. Organisation générale du PIV
2. **Analyse de risque**
   - 2.1. Cartographie des risques
   - 2.2. Vulnérabilités spécifiques du site
   - 2.3. Interdépendances
   - 2.4. Composants névralgiques
3. **Dispositifs de sûreté en place ou prévus**
   - 3.1. Description générale de la défense en profondeur
   - 3.2. Organisation de la fonction défense-sécurité
   - 3.3. Protection mécanique
   - 3.4. Gestion et contrôle des accès et des flux
   - 3.5. Surveillance, détection, vidéo protection
   - 3.6. Levée de doute et intervention
   - 3.7. Systèmes de secours
   - 3.8. Audits et contrôle interne
   - 3.9. Gestion et stockage de l'information classifiée
4. **Sécurité des systèmes d'information**
5. **Lien avec le plan VIGIPIRATE**
6. **Procédure d'alerte et de gestion de crise**
   - 6.1. Astreinte
   - 6.2. Schéma d'alerte et de coordination avec les acteurs externes
   - 6.3. Outils d'alerte et de gestion de crise
   - 6.4. Organisation de crise
   - 6.5. Salle de crise
   - 6.6. Exercices et entrainements
   - 6.7. Continuité d'activité
   - 6.8. Retour d'expérience
7. **Gestion du personnel**
   - 7.1. Sensibilisation et formation
   - 7.2. Postes sensibles et enquêtes administratives
   - 7.3. Services prestataires, sous-traitants
   - 7.4. Visiteurs

Annexe 1 – Annuaire

Annexe 2 – Description synthétique des dispositifs de sûreté par composant névralgique

Annexe 3 – Lutte contre les drones malveillants

Annexe 4 – NRBC

Annexe 2 - Fiches d'aide à l'élaboration des plans particuliers de protection (PPP)

Fiche d'aide sur les attendus génériques d'un plan particulier de protection	
Sur la forme	
1	**Respect du plan type d'un PPP** (tel que défini par le présent guide)
2	**Le document doit être autoporteur** (ne pas faire de nombreuses références et renvois à d'autres documents) **sans toutefois être trop dense** (ne pas intégrer des notes ou politiques internes volumineuses)
3	**Présence d'un glossaire** définissant les acronymes utilisés dans le PPP
4	**Présence de plusieurs schémas, figures et plans** utiles à la compréhension du document
5	**Utilisation des termes adéquats** (composant névralgique et non point névralgique ou installations critiques, enquête administrative et non criblage)
Sur le fond	
1	**Cohérence d'ensemble avec la dernière version du PSO approuvé** (notamment au niveau de l'analyse de risques)
2	**Présence d'une analyse de risques avec les vulnérabilités spécifiques du site**
3	**Présentation du respect de l'équation de protection**
4	**Prise en compte du dernier compte-rendu d'inspection/contrôle/audit**
5	**Etre le plus à jour possible** à la date du dépôt du PPP
6	**Présence de deux annexes spécifiques :** lutte contre les drones malveillants & NRBC
Préambule	
1	**Rappel des enjeux** (du dispositif SAIV, de l'objectif attendu du PPP)
2	**Informations relatives à l'élaboration du document** (circuit de validation, version, mise à jour éventuelle)
3	**Liste des références** (IGI 6600/SGDSN/PSE/PSN du 7 janvier 2014, directive nationale de sécurité, dernière version du PSO de l'opérateur approuvé, plan VIGIPIRATE a minima)

Fiche n°1 – Présentation du point d'importance vitale	
1.1 - Désignation du PIV	
1	**Nom du PIV** - Appellation ; - Adresse complète (n°, voirie, code postal, ville, boîte postale éventuelle).
2	**N° de triplet attribué par le SGDSN** - Si le PIV a été créé avant l'approbation du PSO : numéro figurant dans l'arrêté d'approbation du PSO ; - Si le PIV a été créé après l'approbation du PSO : numéro transmis par l'administration.
3	**Rattachement** - Secteur(s) d'activité d'importance vitale de rattachement (activités militaires de l'état a minima) ; - Directive(s) nationale(s) de sécurité de rattachement (activités militaires de l'état ou industries de défense a minima) ; Attention : certains opérateurs peuvent relever de plusieurs secteurs d'activité d'importance vitale et de différentes directives nationales de sécurité. - Ministère coordinateur.
4	**Lien avec l'opérateur d'importance vitale** - Place dans l'organigramme (filiale etc.) avec schéma ; - Plan de sécurité opérateur de référence (référence d'approbation actualisée).
5	**Nature des activités** - Description des missions du PIV ; - Domaine(s) d'activités concerné(s).
6	**Critères retenus pour la désignation du site comme PIV** (nature des missions, caractère unique, matériels et installations spécifiques etc.).
7	**Classement éventuel du site au titre d'autres réglementations et plans applicables**, hors SAIV (ICPE, Seveso, INID, IPD, etc.) ; Si le site n'a aucune autre classification, indiquer « aucun classement selon d'autres règlementations ».
1.2 – Localisation du PIV	
1	**Coordonnées du PIV** - Adresse complète, coordonnées GPS éventuelles ; - Surface du PIV (en hectares) ; - Plan général du site avec échelle.

2	**Description de l'environnement** - Contexte politique et socio-économique ; - Zone d'implantation (zone industrielle, urbaine rurale, etc.) ; - Axes routiers et/ou ferroviaires, avec plans ; - Milieu naturel (bois, étang, cours d'eau, etc.) ; - Points particuliers situés à proximité (usine, centrale nucléaire, etc.).
3	**Zone de compétence police ou gendarmerie** - Brigade compétente (ville, nature –police ou gendarmerie-) ; - Distance (en km) de la brigade par rapport au site et temps d'intervention ; - Adresse et coordonnées de la police/gendarmerie compétente ; - Brigade éventuelle présente sur le site (gendarmerie de l'armement, de l'air, etc.).
4	**Zonage spécifique au titre d'autres réglementations** - Zone terrestre et/ou maritime (zone protégée, terrain militaire, zone de défense hautement sensible, port militaire, etc.) ; - Zone aérienne (zone d'interdiction de survol permanente ; zone d'interdiction de captation de données aériennes – ZICAD) ; Pour chacune des zones concernées : - Emplacement de la zone (bâtiment, pièce, site) ; - Référence de l'arrêté éventuel ; - Plan de localisation de la zone (avec échelle).
1.3 - Organisation générale du PIV	
1	**Organisation hiérarchique** - Organigramme visuel de l'organisation ; - Nom du responsable de l'établissement.
2	**Caractéristiques générales** - Répartition des effectifs (permanents, temporaires) ; - Horaires d'ouverture.
3	**Organismes éventuels présents sur le site** - Description des organismes ; - Effectifs.
4	**Organisation de la sûreté** - Rôle et responsabilités du délégué à la défense et à la sécurité locale – DDSL - (nom, coordonnées, missions) ; - Adjoints éventuels ; - Officier de sécurité ; - Officier de sécurité des systèmes d'information.

5	**Relations avec les acteurs extérieurs du site dans le cadre de la sûreté** - Préfecture ; - Services de renseignement ; - Forces de sécurité intérieure ; - Service départemental d'incendie et de secours (SDIS) ; - Autres partenaires éventuels (démineurs, SNCF, office français de la biodiversité, etc.).
6	**Modèle de rédaction du paragraphe sur les missions du DDSL** Le délégué à la défense et sécurité du site est responsable de la sûreté du site et officier de sécurité. En qualité de DDSL, ses fonctions et responsabilités sont les suivantes : • Élaborer, suivre et mettre à jour le plan particulier de protection (PPP) ; • Participer à l'élaboration du plan de protection externe (PPE) en lien avec les services de la Préfecture ; • Entretenir des liens réguliers avec la préfecture de [Insérer nom du département] ainsi que les forces de sécurité intérieure ([Insérer le(s) nom(s) de(s) brigade(s) concernée(s)]) ; • Etre le point de contact privilégié de la DGA (SSDI/BPR) (centres DGA uniquement) et de la DRSD (en particulier le poste RSD de [Insérer nom du poste] ; • Mettre en œuvre et piloter les dispositifs de sûreté du site ; • Sensibiliser le personnel du site en matière de sûreté ; • Organiser des exercices de sûreté en lien éventuellement avec les autorités extérieures ; • Participer à la gestion de crise.

Fiche n°2 - Analyse de risque

2.1 – Cartographie des risques

1

Exigences de l'analyse de risque

- Cohérence d'ensemble avec le PSO (scénarios identiques, etc.) ;

> Le site peut compléter ces scénarios par d'autres qu'il estime pertinent au regard de sa situation. Il peut également en exclure certains en fonction de son environnement. Cela doit être justifié dans le PPP.

- Réévaluation du risque brut à la lumière de l'environnement et des vulnérabilités du site ;
- Evaluation du risque net à la lumière du dispositif de protection ;
- Présence du tableau de criticité en synthèse.

2

Tableau synthétique

(1) Reprise des scénarios génériques de la DNS/PSO ;
(2) Description détaillée du scénario ;
(3) Vraisemblance PSO ;
(4) Impact PSO ;
(5) Niveau de risque PSO ;
(6) Vraisemblance (à la lumière des vulnérabilités du PIV et de son environnement) ;
(7) Impact PIV ;
(8) Niveau de risque PIV ;
(9) Mesures compensatoires/ de réduction de risques ;
(10) Niveau de risque résiduel ;

En cas de risque résiduel inacceptable, prévoir une 11ème colonne décrivant la programmation de mesures complémentaires.

Scénario	Description détaillée	V	I	Niveau de risque PSO	V	I	Niveau de risque PIV	Mesures compensatoires/ de réduction de risques	Risque résiduel
Vol d'information	Détournement d'un support contenant des ISC	2	5	10	2	3	6	- CADVIS ; - contrôle des accès ; - ZP etc.	5

3

Tableau de criticité de synthèse (voir celui utilisé dans le PSO)

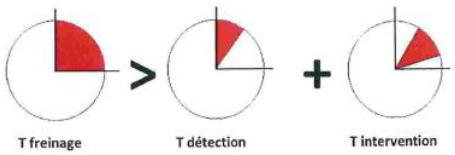
Forte				
Probable				
Moyenne				
Improbable				
Vraisemblance/Impact	Limité	Modéré	Critique	Catastrophique

2.2 - Vulnérabilités spécifiques du site	
1	**Attendus du paragraphe** - Description succincte des principales vulnérabilités du site non traitées ou partiellement non traitées ; - Perspectives à court, moyen et long termes (projet d'infrastructure, achat de nouveaux matériels, etc.).
2	**Vulnérabilités physiques/techniques** - Infrastructure (barrière de protection physique défaillante, exposition à un aléa, etc.) ; - Matériel (faiblesse d'un composant, maintenance insuffisante, etc.) ; - Réseau (mauvais câblage, voies de communication non protégées, etc.) ; - Logiciel (absence de sauvegarde, failles connues, etc.).
3	**Vulnérabilités humaines** - Personnel du site (absence de personnel, formation insuffisante, tâches non-maîtrisées, etc.) ; - Organismes partenaires (défaillance d'un fournisseur, absence de contrôle, etc.).
2.3 - Interdépendances	
1	**Exigences du paragraphe** - Description des principales interdépendances ; - Mesures de secours.
2	**Interdépendances énergétiques** - Electricité (nom du fournisseur, nombre de transformateurs, etc.) ; - Eau (nom du fournisseur, réseau d'eau potable, etc.) ; - Hydrocarbure (nom du fournisseur, gaz naturel, pétrole, énergies fossiles, etc.) ; - Mesures de secours (générateurs de secours, bassin de rétention d'eau, clause contractuelle prévoyant une intervention rapide du fournisseur etc.).
3	**Entités présentes sur le site (filiale, autre organisme, etc.)** - Gestion de la sécurité/sûreté ; - Transport ; - Mesures de secours (gestion des interfaces, communication etc.).
4	**Prestataires** - Maintenance (réseaux informatiques, systèmes de contrôle d'accès, etc.) ; - Approvisionnement (matériel, nourriture etc.) ; - Mesures de secours (dispositions contractuelles en cas de manquement etc.).
5	**Modèles de rédaction d'interdépendances** **Energie électrique** : les activités industrielles du site nécessitent d'être alimentées en permanence en électricité. Ces besoins sont assurés par l'opérateur [XXX] avec l'arrivée de deux lignes de 50 000 volts chacune au sein de deux postes de transformation (voir emplacement sur le plan). En cas de panne, le site dispose de deux groupes électrogènes

	permettant une autonomie totale de 72 heures. De plus, une clause spécifique du contrat oblige le fournisseur à prévoir une solution de secours en cas de coupure de plus de 48 heures. **Télécommunication :** pour la téléphonie, les liaisons radio et le réseau Internet, l'établissement est dépendant de l'opérateur [XXX]. Ces moyens de télécommunications sont indispensables au bon fonctionnement du site. La dépendance vis-à-vis du fournisseur est toutefois partiellement réduite grâce à une clause contractuelle incluant une garantie de rétablissement sous 24 heures en cas de coupure. **Fournisseurs** : le site dépend pour son bon fonctionnement de l'approvisionnement de plusieurs matières premières (aluminium notamment) et de matériaux de base. La liste des fournisseurs critiques est gérée par le service des achats du site et est mise à jour régulièrement. En raison du nombre de fournisseurs et des changements fréquents, la liste ne peut être intégrée dans le PPP. Elle peut toutefois facilement être transmise ou mise à la disposition de à l'administration sur demande. **Entité présente sur le site** : le site héberge en son sein l'entité [XXX]. Cette dernière est responsable de la sûreté de la partie nord du site. Elle met à disposition plusieurs agents de gardiennage chargés d'effectuer des rondes, de contrôler et de surveiller le poste d'accès secondaire. Ces dispositions ont été inscrites dans un contrat, qui prévoit également une procédure de remplacement en cas de manquement de personnel.
2.4 - Composants névralgiques	
1	**Utilisation du terme « composant névralgique et non « point névralgique »** Pour rappel, un composant névralgique est une installation ou un ouvrage, situé dans une zone sensible indispensable aux activités du site et/ou aux missions de la défense et dont la perte ou la dégradation serait jugée inacceptable .
2	**Hiérarchisation des composants névralgiques** - Composants névralgiques opérationnels (exemples : laboratoire, moyen d'essai, etc.) ; - Composants névralgiques de soutien (exemples : PCS, locaux techniques, etc.) ; - Composants névralgiques de servitudes (exemples : transformateur, château d'eau etc.) - Dans chacune de ces catégories, classer les composants névralgiques en fonction de leur sensibilité.
3	**Description générale du composant névralgique** - Emplacement du composant (n° du ou des bâtiment(s) avec plan de localisation) ; - Fonction (exemple : zone de stockage, laboratoire, salle serveur, etc.) ; - Justification du caractère névralgique (exemple : matériel entreposé).
4	**Dispositif de protection du composant névralgique** - Responsable éventuel du composant névralgique ; - Barrières de protection physique ; - Dispositif de contrôle d'accès éventuel ; - Autres mesures complémentaires éventuelles ; Ce paragraphe peut prendre la forme du tableau suivant (à mettre en annexe) :

Composant névralgique	Protection juridique	Protection mécanique	Contrôle des accès et des flux	Surveillance & détection	Responsable éventuel

	PCS	ZP	Clôture, barbelés	Mise en place d'un contrôle d'accès par badge	Présence de caméras, détecteurs de mouvement.	Service de sûreté
5	**Modèles de rédaction des composants névralgiques** **Transformateur** : les activités industrielles du site nécessitent d'être alimentées en permanence en électricité. En cas de détérioration ou destruction du transformateur, les activités vitales (cf. partie 1) du site ne pourraient plus être conduites. **PCS** : le PCS est indispensable pour la sécurité des biens, des personnes et des activités du site. En cas de détérioration ou de destruction de ce dernier, les alarmes et images de vidéo-surveillance ne seraient plus reportées et les contrôles d'accès ne pourraient plus être réalisés. Le site serait donc amené à fermer pour raison de sécurité et par conséquent, les activités vitales seraient mises à l'arrêt. **Château d'eau** : les moyens d'essais sont soumis à de très fortes températures et nécessitent d'être refroidis régulièrement. Cela est rendu possible grâce au château d'eau situé à l'intérieur du site (voir plan), qui dispose d'un réservoir de [XXX] litres et qui est alimenté par une station de pompage. La destruction de ce dernier conduirait à arrêter les essais qui est la mission principale du site. **Zone réservée** : la zone réservée permet de stocker de façon sécurisée les documents classifiés relatifs aux activités vitales du site (résultats d'essai notamment) et permet ainsi d'assurer la confidentialité des travaux menés. En cas de détérioration ou de destruction de cette dernière, les activités opérationnelles du site devraient être mises à l'arrêt car il n'y aurait plus de lieu de stockage pour les documents afférents.					

Fiche n°3 - Dispositifs de sûreté en place ou prévus	
3.1 - Description générale de la défense en profondeur	
1	**Attendu du paragraphe** - Le site doit démontrer qu'il respecte l'équation de protection grâce au principe de défense en profondeur ; - Ce paragraphe est une introduction générale qui résume, dans les grandes lignes, les dispositifs de sureté qui sont développés dans les paragraphes suivants. Rappel des concepts : - Défense en profondeur : superposition de plusieurs lignes de défense, composées d'un ensemble de mesures de sécurité ; - Equation de protection : 
2	**Démonstration de la stratégie de protection** - Eléments de freinage (clôture, contrôle d'accès etc.) et temps de freinage ; - Eléments de détection (ronde, levée de doutes etc.) et temps de détection ; - Eléments d'intervention (calcul du temps d'intervention en prenant en compte différents paramètres – heures ouvrées, heures non-ouvrées, site le plus éloigné des éléments d'intervention etc.) ; - Mesures programmées en cas d'équation de protection non respectée.
3	**Modèle de rédaction du paragraphe** La protection du PIV repose sur une combinaison de dispositifs (juridiques, organisationnels, techniques et humains), organisés en lignes successives. Cet enchaînement de différentes barrières (aussi appelé concept de défense en profondeur) permet de satisfaire l'équation de protection, qui se définit de la façon suivante : $T_{freinage} > T_{détection} + I_{intervention}$ Freinage Au niveau de **la zone périmétrique** (à savoir la ligne de séparation entre le site et l'extérieur), plusieurs moyens de freinage ont été mis en place. Une clôture métallique de deux mètres surmontée de barbelés et de concertinas encercle le site. L'ensemble du site est érigé en zone protégée et bénéficie donc à ce titre, d'une protection juridique. Les accès au site (véhicules et piétons) sont contrôlés par des dispositifs humains (contrôle visuel) et physique (portillons équipés de tourniquets). Au niveau de **la zone intérieure** (zone située à l'intérieur du site, constituée des espaces de circulation, des espaces verts et composants non sensibles), les bâtiments sont équipés de serrures de sécurité. Au niveau de **la zone sensible** (zone constituée des composants névralgiques), les locaux hébergeant les composants névralgiques sont équipés d'un système de contrôle d'accès par

	badge, permettant l'identification des personnels. Les locaux sont également dotés de fenêtres antieffraction et de portes en acier. Le temps de freinage jusqu'à la zone sensible est estimé à 20 minutes. Détection Au niveau de la zone périmétrique, la clôture est équipée d'un cordon anti-intrusion avec un report d'alarme au PCS et de plusieurs caméras de vidéo-surveillance. Des rondes sont également assurées par les agents de gardiennage. Le périmètre intérieur du site est placé sous vidéo-surveillance qui est veillé en permanence au niveau du PCS. Les ouvrants des composants névralgiques (portes et fenêtres) sont équipés de détecteurs d'ouverture et de chocs. L'intérieur de ces bâtiments dispose de détecteurs volumétriques et de caméras infrarouges avec report au PCS. Le temps de détection est immédiat puisque les alarmes sont automatiquement reportées au PCS. Le temps qu'un agent prenne en compte l'alarme et prévienne les forces de sécurité intérieure est estimé à 5 minutes. Intervention Le temps d'intervention de la brigade de gendarmerie est estimé à 5 minutes. Ainsi, l'équation de protection est vérifiée et se décline selon la formule suivante : $T_{freinage}$ 20 minutes > $T_{détection}$ 5 minutes + $T_{intervention}$ 5 minutes
3.2 - Commandement, organisation de la fonction défense-sécurité	
1	**Chaîne défense-sécurité** - Si la chaîne défense-sécurité a été décrite dans le 1. 3, faire un renvoi à cette partie. Si non, la chaîne DS peut être développée ici en développant les aspects suivants : - Directeur de site ; - Délégué à la défense sécurité et adjoints éventuels ; - Officier de sécurité et adjoints éventuels ; - Officier de sécurité des systèmes d'information ; - Autres acteurs éventuels (bureau de protection du secret, etc.) ; Pour chacun de ces acteurs, description de leurs responsabilités/missions ; En cas de site multi-formations, décrire les chaînes défense-sécurité des autres formations.
2	**Militaires/gendarmes** (si concerné) - Effectifs (heures ouvrées, non ouvrées) ; - Localisation et répartition sur le site ; - Missions génériques (contrôle des accès, rondes, filtrage, etc.) ; - Moyens disponibles (emploi de chiens de défense, port d'armes, véhicules, etc.) ; - Entrainements et formations (fréquence, nature de la formation, etc.) ; - Interface éventuelle avec les agents de gardiennage.

2	**Agents de gardiennage** - Effectifs (heure ouvrées, non ouvrées) ; - Localisation et répartition sur le site ; - Missions génériques (contrôle des accès, rondes, filtrage, etc.) ; - Qualité des agents (internes, prestataires) ; - Qualifications particulières (SSIAP, EPI, SST, etc.) - Moyens disponibles (emploi de chiens de défense, port d'armes, véhicules etc.) ; - Entrainements et formations (fréquence, nature de la formation, etc.) ; - Interface éventuelle avec les militaires.
3	**Poste central de sécurité** (aussi appelé poste central de protection –PCP-) - Effectifs du PCS (heures ouvrées, non ouvrées) ; - Localisation du PCS ; - Missions génériques ; - Moyens disponibles (système d'alerte, téléphones, réseaux informatiques, vidéosurveillance etc.) ; - Formation (nature des formations, fréquence etc.) ; - Rôle du PCS en cas de crise.
3.3 - Protection mécanique, freinage	
1	**Eléments extérieurs éventuels** - Parking (localisation, nature du parking –permanents/ visiteurs, procédure à suivre pour stationner sur le parking) ; - Dispositif masquant la vue depuis l'extérieur (élément naturel, bâtiment, etc.).
2	**Clôtures** - Clôture périmétrique (hauteur, résistance, état, autres caractéristiques, etc.) ; - Clôture administrative d'une zone particulière - zone protégée, terrain militaire, zone de défense hautement sensible - (disposition des panneaux, équipements de la clôture, etc.).
3	**Accès site** - Nombre d'accès ; - Nature (accès piétons, véhicules) ; - Dispositif de protection (barrière anti- véhicules bélier, ralentisseurs, chicanes, concertina etc.).
4	**Obstacles à l'intérieur du site** - Localisation ; - Caractéristiques.
5	**Sécurisation des ouvrants** - Caractéristiques des portes (serrure, porte blindée, etc.) ; - Caractéristiques des fenêtres (barreaux, grillagée, etc.).
3.4 - Gestion et contrôle des accès et des flux	

1	**Fonctions principales du dispositif de contrôle d'accès** Pour chaque dispositif de contrôle d'accès, lister ses principales fonctions : - Détecter (exemple : les tentatives d'intrusion) ; - Recenser (exemple : les entrées et sorties) ; - Freiner (présence d'obstacles – gabions, tourniquets etc.) ; - Sectoriser (entre différentes zones).
2	**Procédures** **1. Délivrance des contrôles d'accès** **-** Distinguer les autorisations d'accès pour le personnel affecté sur le site (et/ou se rendant régulièrement) et les visiteurs ; - Pour le personnel affecté sur le site : autorité prenant l'autorisation, enquête administrative réalisée ; - Pour les visiteurs : description de la procédure (formulaire à remplir, dépôt d'une pièce d'identité, inscription sur un registre, accompagnement sur le site, etc.). **2. Contrôle des véhicules** - Distinguer le cas des permanents et des personnels extérieurs ; - Description des procédures pour chacun de ces cas (badge d'accès, dépôt d'une pièce d'identité, horaires d'accès, etc.). **3. Procédure spécifique en matière de sûreté pour la gestion des colis et courrier entrants** - Zone située en dehors des composants névralgiques ; - Description de la procédure (arrivée des camions, modalités de réception, etc.).
3	**Moyens humains : poste d'accueil filtrage** - Responsable du poste d'accueil (chef de service, cadre de permanence, etc.) ; - Effectifs (heures ouvrées, heures non-ouvrées) ; - Localisation ; - Missions du poste (filtrage, suivi des personnes, bloquer certaines entrées, etc.) ; - Eventuel poste de préfiltrage.
4	**Moyens matériels** **1. Badges** - Description de la politique générale des badges (badge permanent vs. badge visiteur, logique de zones, etc.) ; Pour chacun des types de badges, décrire : - La procédure de délivrance et de restitution ; - Les personnes concernées ; - Eléments caractéristiques du badge (photo, nom, prénom, etc.) ; - Durée de validité ; **2. Clés** **-** Politique générale de gestion des clefs ; - Stockage des clefs de bureau et des locaux sensibles (boite à code, armoire forte, etc.) ;

	- Gestion des « passes » permettant d'accéder à plusieurs ou toutes les serrures (personnes y ayant accès). **3. Biométrie** - Localisation du lecteur biométrique ; - Gestion des données biométriques des utilisateurs.
3.5 - Surveillance et détection, vidéo protection	
1	**Eclairage** - Politique du système d'éclairage ; - Fonctions principales du dispositif (dissuader, détecter, intervenir, etc.) ; - Zones concernées par le dispositif (composants névralgiques, zones de travail, etc.) avec plans ; - Caractéristiques du système d'éclairage (déclenchement automatique, etc.).
2	**Détection** - Bâtiment, local, zone concerné(e) par un dispositif de détection ; Pour chaque dispositif, préciser : - Type de capteur (détecteur volumétrique, thermique, détecteur d'ouverture de porte, etc.) ; - Lieu d'activation (sur place, au PCS) ; - Système d'alarme (silencieuse, sonore) ; - Report de l'alarme ; - Maintenance générale du dispositif (tests, etc.).

3	**Surveillance**
	- Politique de surveillance générale ;
	- Politique de vidéo-protection :
	  - Fonction principales du dispositif de vidéo-protection ;
	  - Zones concernées par le dispositif de vidéo-protection avec plans ;
	  - Caractéristiques techniques (capacité d'enregistrement, détecteur de mouvement, caméra infrarouge, etc.) ;
	- Politique de surveillance humaine (fréquences des rondes) ;
	  - Effectifs (heures ouvrées, non ouvrées) ;
	  - Zones concernées par le dispositif de surveillance humaine ;
	  - Moyens à disposition (véhicules, etc.).

4	**Lutte anti-drones** Les dispositions relatives à la lutte anti-drones doivent être intégrées dans l'annexe réservé à cet effet.
3.6 - Levée de doute et intervention	

1	**Elément de levée de doute et/ou d'intervention** - Effectifs (heure ouvrées, non ouvrées, renforts éventuels) ; - Localisation sur le site ; - Missions génériques ; - Matériel à disposition (clefs, armes, équipe cynotechnique, etc.)
2	**Procédure de levée de doute et d'intervention** - Politique d'intervention ; - Déclenchement (ordre, radio, appel, etc.) ; - Plans d'intervention (fiches reflexes, conduire à tenir, etc.).
3.7 - Systèmes de secours	
1	**Moyens permettant la continuité des systèmes de sécurité** **-** Description (exemple : transformateur, groupe électrogène, etc.) ; - Localisation sur le site avec plan ; - Caractéristiques (autonomie, etc.) ; - Dispositif de protection éventuel ; - Dispositif d'astreinte.
3.8 - Audits et contrôle interne	
1	**Inspections/ audits** - Nom du service du ministère des Armées réalisant l'inspection/audit (DRSD, SSDI, etc.) ; - Périodicité des inspections et liste des dernières inspections ; - Eléments inspectés (ISC, dispositif de sécurité, etc.) ; - Prise en compte des recommandations (plan d'actions, programmation etc.).
2	**Contrôle interne** - Autorités réalisant le contrôle interne ; - Périodicité des évaluations ; - Eléments évalués ; - Prise en compte des recommandations (plan d'actions, programmation etc.).
3.9 - Gestion et stockage de l'information classifiée	
1	**Définition des responsabilités** **-** OS et éventuel adjoint ; - OSSI et éventuel adjoint ; - Bureau de protection du secret (BPS).
2	**Mesures de protection physique** (selon annexe 30 IGI 1300) - Classement du meuble ; - Classement du local ; - Classement du bâtiment et/ou de l'emprise.

3	**Mesures de protection juridique** **-** Mise en place d'une zone protégée ; - Mise en place d'une zone réservée.
4	**Mesures organisationnelles** **-** Rédaction d'une politique propre au PIV en matière de protection du secret ; - Nombre d'inventaires réalisés ; - Fréquence du changement de combinaisons des coffres.

<table>
<tr><th colspan="2">Fiche n° 4 – Sécurité des systèmes d'information</th></tr>
<tr><td>1</td><td>Attendus du paragraphe
- Décliner les mesures organisationnelles et de gestion de la sécurité des systèmes d'information ;
- Préciser la répartition des responsabilités entre la chaîne fonctionnelle de SSI du PIV et ses éventuels prestataires ;
- Identifier les systèmes d'information ;
- Identifier les modes opératoires de résilience SSI et les conditions d'un éventuel déclenchement de celles-ci ;
Cette partie doit être rédigée en cohérence avec les dispositions prévues à ce sujet par l'opérateur dans le PSO, notamment les scénarii cyber qui y sont présents.</td></tr>
<tr><td>2</td><td>Documentation des processus SSI
- Existence d'une politique de sécurité des systèmes d'information (PSSI) « groupe », ou d'une version locale déclinée à l'établissement ;
- Autres documents d'organisation de la voie fonctionnelle SSI tels que la note de nomination de l'Autorité qualifiée en SSI, les notes de désignation des Autorités d'homologation (mettre en cohérence avec le 1.3) ;
- Autres documents d'application tels que les processus d'homologation de sécurité des systèmes d'information, la procédure de gestion de crise et de déclarations d'incidents cyber aux autorités étatiques (ANSSI, autorité contractante et service enquêteur ministériel), PCA/PRA et PCI/PRI ; contrat cadre type pour des prestataires SSI.</td></tr>
<tr><td>3</td><td>Principaux systèmes d'information du site
- Lister les SI, éventuellement sous forme de tableau, en référençant les SI métier, SI bureautique, SI de sécurité/sûreté, SI industriels (de développement, d'ingénierie, de qualification, de production) ;
- Préciser en regard de chaque SI :
o Les niveaux de criticité du SI (pour l'entité, pour les impacts opérationnels métier, pour les impacts sur les programmes d'armement, sur les populations) et si les systèmes d'information ont fait l'objet d'une déclaration SIIV ;
o Le lieu d'hébergement (à distance, localement) ;
o Le SI est-il connecté avec d'autres systèmes qui ne sont pas à la maîtrise de l'opérateur ;
o Les rôles et responsabilités sur le SI (gestion opérationnelle ; administration technique et de sécurité ; RSSI ou responsable cyber-sécurité du système) ;
o S'il y a un ou plusieurs prestataires « clés » dont la mise en œuvre du SI dépend fortement ;
Cette partie peut prendre la forme du tableau suivant :
<table>
<tr><th>Référence du SI</th><th>Type de SI</th><th>Niveau de criticité</th><th>Lieu d'hébergement</th><th>Rôles et responsabilités sur le SI</th><th>Connexions éventuelles avec d'autres systèmes</th><th>Prestataires clefs pour la mise en œuvre du SI</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

	- Identifier les dispositifs de secours permettant la continuité des systèmes métiers (description des moyens, autonomie, en cohérence avec les procédures de PCA/PRA ou PCI/PRI) ; - Décrire les dispositifs de sauvegarde des données existants (en ligne ou hors ligne). Mettre en cohérence ce paragraphe avec le 2.2 (Vulnérabilités techniques et logiciel, absence de sauvegardes, failles connues, etc.).

<table>
<tr><th colspan="2">Fiche n°5 - Lien avec le plan Vigipirate</th></tr>
<tr><td>1</td><td>Attendus du paragraphe
- Décliner les mesures du plan Vigipirate afin de préparer un éventuel déclenchement de celles-ci. A cette fin :
- Classer les mesures par domaines d'actions (ex : installations dangereuses ; installations et bâtiments, etc.) ;
- Toutes les mesures du plan Vigipirate n'ont pas vocation à être déclinées :
o Certaines mesures sont suffisamment explicites pour ne pas être déclinées (exemple : élaborer et mettre à jour un plan de continuité d'activité) ;
o D'autres sont déjà décrites dans le PPP (exemple : surveiller les abords des installations et bâtiments) ;
- Cette partie doit être rédigée en cohérence avec les dispositions prévues à ce sujet par l'opérateur dans le PSO.</td></tr>
<tr><td>2</td><td>Tableau type
Les mesures du plan Vigipirate peuvent être déclinées selon le tableau suivant :
(1) Numéro de mesure ;
(2) Mesure ;
(3) Type de mesure ;
(4) Prise en compte par le site ;
(5) Précisions sur les dispositions prises par le site.

Exemple :
<table>
<tr><th>Numéro de mesure</th><th>Mesure</th><th>Type de mesure</th><th>Prise en compte par le site</th><th>Précisions sur les dispositions prises par le site</th></tr>
<tr><td>RSB 12-02</td><td>Limiter l'activité</td><td>Additionnelle</td><td>Oui</td><td>- Mise en œuvre du télétravail pour la personne équipée d'un VPN
- Interdire les missions non prioritaires à l'extérieur du site.</td></tr>
</table>
</td></tr>
</table>

Fiche n° 6 – Procédure d'alerte et de gestion de crise	
6.1 - Astreinte	
1	**Personnel d'astreinte de gestion de crise** - Désignation ; - Régime d'astreinte et planification ; - Liste des fonctions assurées en astreinte (médicale, de sécurité, etc.).
6.2 - Schéma d'alerte et coordination avec les acteurs externes	
1	**Logigramme** - Décrivant le schéma d'alerte général.
2	**Schéma d'alerte interne** - Procédure d'alerte des autorités de décision : o Personnes désignées à cet effet (PCS, gendarmes, etc.) ; - Autorités de décision : o Précisions sur les autorités de décision si elles n'ont pas été décrites au 6.1 ; - Procédure d'alerte du personnel du site : o Personnes désignées à cet effet (PCS, gendarmes etc.).
3	**Schéma d'alerte vers les autorités administratives** - Procédure d'alerte des autorités administratives : o Personnes désignées à cet effet (autorités de décision, etc.) ; - Liste des autorités administratives concernées (services préfectoraux, forces de sécurité intérieure, service du haut fonctionnaire de sécurité de défense, DGA/SSDI, DRSD etc.).
4	**Schéma d'alerte vers les populations** (si concerné) - Procédure d'alerte des populations : o Personnes désignées à cet effet.
6.3 - Outils d'alerte et de gestion de crise (hors salle de crise)	
1	**Moyens de communication** - En interne : o Moyens de diffusion (sirène, hauts parleurs, etc.) ; o Réseau radio ; o Réseau téléphonique (portables, fixes, etc.) ; o Réseau informatique. - Vers l'extérieur : o Réseau téléphonique (portables, fixes, etc.) ; o Réseau informatique (internet, réseaux classifiés – ISIS, Intraced- etc.).

<table>
<tr><td>2</td><td>Documents
- Instructions relative à la gestion d'un risque spécifique (incendie, problème de santé, acte terroriste, etc.) ;
- Fiches réflexes (levée de doute, sécurisation, blocage des entrées, observation d'un drone, etc.) ;
- Consignes générales en cas d'alerte.</td></tr>
<tr><td colspan="2">6.4 - Organisation de crise</td></tr>
<tr><td>1</td><td>Cellule de crise
- Critères de définition et d'identification d'une crise ;
-Fonctionnement de la cellule (déclenchement, par qui, comment, dispositions préparatoires, etc.).</td></tr>
<tr><td>2</td><td>Composition des membres de la cellule de crise
- Organigramme général ;
- Pour chaque fonction de la cellule de crise, précisez :
o Les missions et responsabilités (filtrer les appels, assurer la liaison avec le terrain, apporter une expertise sur un point particulier etc.) ;
o La personne assurant cette fonction (directeur de site, DDSL, OS, adjoint, etc.) ;
o Les relèves éventuelles ;
o Cela peut notamment prendre la forme du tableau suivant :
<table>
<tr><th>Fonction au sein de la cellule de crise</th><th>Missions et responsabilités</th><th>Personne assurant cette fonction</th><th>Relève éventuelle</th></tr>
<tr><td>Conseiller communication</td><td>Assurer la communication interne et externe, assurer les relations éventuelles avec les médias.</td><td>Responsable communication du site</td><td>Responsable RH</td></tr>
<tr><td>Animateur</td><td>Mettre en place la cellule de crise et la faire vivre, organiser des points de situation réguliers.</td><td>DDSL</td><td>/</td></tr>
</table></td></tr>
<tr><td colspan="2">6.5 - Salle de crise</td></tr>
<tr><td>1</td><td>Localisation de la salle de crise
- Localisation précise de la salle (zone, bâtiment, étage, salle) ;
- Délais d'installation (si la salle n'est pas permanente) et personnes réalisant cette tâche ;
- Présence d'une seconde salle éventuelle / site de repli ;
- Autres locaux pouvant éventuellement être affectés à certaines missions particulières (réception des journalistes, familles de victimes etc.).</td></tr>
<tr><td>2</td><td>Moyens à disposition de la salle de crise
- Moyens matériels (fournitures de bureau, chaises, etc.) ;
- Documents (instruction de gestion de crise, fiches réflexes, scénarios de gestion de crise, cartes, plan de communication, etc.) ;
- Moyens de communication (ordinateurs avec réseaux – ISIS, Intradef, Intraced, Internet etc.- , téléphones fixes ou portables, liaison radio etc.).</td></tr>
</table>

6.6 - Exercices et entrainements	
1	**Description générale des exercices** - Caractéristiques générales des exercices (mise en situation, périodicité) ; - Agents concernés (cellule de cerise, personnel de sûreté, ensemble du personnel, etc.) ; - Objet de l'exercice (sûreté – intrusion, acte terroriste-, sécurité – incendie etc.).
6.7 - Continuité d'activité	
1	**Analyse** - Identification des missions prioritaires ; - Scénarios retenus.
2	**Mise en œuvre** - Document formalisant le PCA ; - Evaluation du PCA ; - Formation du personnel gérant le PCA ; - Révision/ RETEX du PCA.
6.8 - Retour d'expérience	
1	**Retour d'expérience** - Existence d'une politique de retour d'expérience après une crise, incident ou exercice ; - Intégration en interne ou en externe du RETEX.
2	**Remontée des incidents** - Description de la politique de remontée des incidents : o Nature des incidents remontés ; o Canal utilisé (mail, appel téléphonique, FlashEvent, etc.) ; o Destinataire (DRSD, DPID, DGA/SSDI, etc.).

Fiche n°7 – Gestion du personnel	
7.1 – Sensibilisation et formation	
1	**Sensibilisation** - Politique générale de sensibilisation des personnels du site ; Pour chaque sensibilisation, décrire : - Son objet (protection du secret de la défense nationale, sûreté du site, etc.) ; - Le personnel visé (nouvel arrivant, personne manipulant des ISC, etc.) ; - Les personnes/services réalisant la sensibilisation (DDSL, OS, OSSI, DRSD, etc.) ; - Caractéristiques de la sensibilisation (périodicité, caractère obligatoire, etc.) ; - Déroulement de la sensibilisation (évaluation finale, test, signature d'une feuille d'émargement etc.).
2	**Formation** - Politique générale de formation du site ; - Formation des éléments d'intervention (périodicité, contenu de la formation, modalités, etc.) ; - Formation des éléments du PCS (périodicité, contenu de la formation, modalités, etc.) ; - Formation des acteurs de la gestion de crise périodicité, contenu de la formation, modalités, etc.).
7.2 – Postes sensibles et enquêtes administratives	
1	**Postes sensibles** - Critères retenus pour la désignation des postes sensibles (accès à des informations sensibles et/ou classifiées, savoir-faire unique, etc.) ; - Modalités de gestion des postes sensibles (inscription dans un catalogue des emplois, registre particulier, etc.) ; -Mesures particulières de sécurité applicables aux postes sensibles (sensibilisations plus fréquentes, enquête administrative plus poussée, contrôle intermédiaire, etc.).
2	**Typologie des enquêtes administratives** - Politique des enquêtes administratives au sein du PIV (personnes ciblées, degré de profondeur en fonction des zones, récurrence des contrôles, etc.) ; - Personnes faisant l'objet d'un contrôle primaire (visiteur, prestataire dans le cadre d'un contrat sensible par exemple) ; - Personnes faisant l'objet d'un contrôle élémentaire (personne occupant un emploi sensible selon l'IM 900, personne accédant en ZRR par exemple) ; - Personnes habilitées.
7.3 – Services prestataires, sous-traitants	
1	**Mesures de sécurité applicables** Pour chaque contrat mentionné au 2.2.4 (nettoyage, maintenance, etc.) décrire : - Le cadre contractuel (marché de défense et de sécurité, contrat sensible) ;

	- La gestion de la relation contractuelle de part et d'autre (POC côté site, POC côté prestataire/sous-traitant) ; - Les principales mesures de sécurité applicables (enquête administrative, accompagnement éventuel, rappel des règles, port d'un badge, etc.) pour : ○ Les personnes morales ; ○ Les personnes physiques.
7.4 – Visiteurs	
1	**Encadrement des visiteurs** - A l'entrée du site : procédure accès visiteurs (cf. 3.4.2) ; - Pendant la visite : description des mesures de sécurité (port d'un badge, accompagnement par un personnel, parcours de visite encadré, etc.) ; - A la sortie : procédure de sortie (cf. 3.4.2) ; - Pour le cas des visiteurs étrangers, description des procédures spécifiques éventuelles.

Fiche n°8 - Annexes

1 – Modèle d'annuaire

Fonction	Nom et prénom	Courriel	Numéro de téléphone (portable et ou fixe)
DDSL	XXX	XXX	XXX
DDSL adjoint	XXX	XXX	XXX

Les fonctions ne sont pas exhaustives.

2 – Modèle de tableau des dispositifs de sûreté des composants névralgiques

Cet aspect a été développé au §2.4 du présent guide.

Composant névralgique	Protection juridique	Protection mécanique	Contrôle des accès et des flux	Surveillance & détection	Responsable éventuel
PCS	ZP	Clôture, barbelés	Mise en place d'un contrôle d'accès par badge	Présence de deux caméras, détecteurs de mouvement.	Service de sûreté

Annexe 3 – Fiche d'aide à la rédaction de l'annexe NRBC

1. Documents d'aide à la rédaction de l'annexe NRBC

Afin de rédiger l'annexe NRBC du PPP, l'opérateur peut s'appuyer sur les documents suivants :

- Directive 2012/18/UE du Parlement européen et du Conseil du 4 juillet 2012 concernant la maîtrise des dangers liés aux accidents majeurs impliquant des substances dangereuses ;
- Plan de sécurité opérateur ;
- Instruction ministérielle n°003848/ARM/CAB/NP du 12 août 2021 relative à la résilience radiologique, biologique et chimique (RBC) ;
- Circulaire n°700/SGDSN/PSE/PSN du 2 octobre 2018 relative à la doctrine nationale d'emploi des moyens et de soins face à une action terroriste mettant en œuvre des matières chimiques ;
- Circulaire n°750/SGDSN/PSE/PPS du 18 février 2011 relative à la découverte de plis, colis, contenants et substances suspectés de renfermer des agents radiologiques, biologiques ou chimiques dangereux ;
- Circulaire n°800/SGDSN/PSE/PPS du 18 février 2011 relative à la doctrine nationale d'emploi des moyens de secours et de soins face à une action terroriste mettant en œuvre des matières radioactives.

2. Plan type de l'annexe NRBC

1 – Caractéristiques générales du site	
1	**Présentation du site** - Nom du site ; - Détention de matière NRBC : ☐ Oui ; ☐ Non ; Si non, indiquer [Néant]. - Si oui, préciser le type de matière détenue : ☐ Nucléaire ; ☐ Radiologique ; ☐ Biologique ; ☐ Chimique.
2 – Analyse de risque	

1

Cartographie des risques

- Le site reprend dans cette partie les scénarios développés au § 2.1 du PPP qui peuvent concerner directement ou indirectement le risque NRBC ;
- Doivent figurer a minima les trois scénarios de la DNS (S14). Si l'opérateur a choisi dans son PSO d'en développer davantage, le site reprend alors l'ensemble des scénarios qui ont été détaillés ;
- En fonction des caractéristiques du site (exemple : détention de matière NRBC), il est pertinent de rajouter d'autres scénarios (exemple : malveillance interne).
- Exemple d'analyse de risque NRBC :

Scénario	Description détaillée	V	I	Niveau de risque PSO	V	I	Niveau de risque PIV	Mesures compensatoires	Niveau de risque résiduel
Utilisation de moyens NRBC	Empoisonnement alimentaire par une substance hautement toxique dans une infrastructure collective.	3	3	9	2	3	6	- EARS pour l'ensemble des prestataires liés à la filière alimentation ; -Surveillance des approvisionnement.	3

2

Vulnérabilités du site en matière de risques NRBC

La liste ci-dessous n'est pas exhaustive. Elle a pour objectif d'aider les opérateurs à identifier leurs vulnérabilités potentielles en matière de risques NRBC en énumérant celles qui sont les plus fréquentes.

- Présence sur le site de matière NRBC (fabrication, stockage, etc.) ;
- Installations à risque (SEVESO, ICPE, etc.) situées à proximité immédiate du site ;
- Absence de procédure spécifique en matière de sûreté pour la gestion des colis et courriers entrants ;
- Inspection visuelle des véhicules insuffisante qui ne permet pas la détection d'une charge NRBC ;
- Infrastructure de restauration collective dont le personnel est externalisé ou qui se situe chez un organisme tiers ;
- Réseau public d'eau potable peu protégé ;
- Présence sur le site de nombreux dispositifs de ventilation et de climatisation.

3 – Organisation de la réponse face à un évènement de nature NRBC

3.1 – Chaine de commandement

1

Référent NRBC

Existence d'un (ou plusieurs) référent NRBC sur le site :

- ☐ Oui ;
- ☐ Non ;

Si oui, précisez ses missions.

2	**Schéma d'alerte des autorités de décision** - Procédure de remontée des alertes NRBC. Indiquer : o Vers quelle(s) personne(s) sont remontées les alertes (PCS, service de sûreté, etc.) ; o Par quel(s) moyen(s) sont-elles remontées (appel téléphonique, etc.) ; - Procédure d'alerte des autorités de décision. Indiquer : o Les personnes désignées à cet effet (DDSL, PCS, etc.) ; o Les autorités de décision (directeur de site, etc.) ; - Logigramme éventuel décrivant le schéma d'alerte général en cas de crise NRBC.
Procédures de mise en sécurité	
1	**Diffusion de l'alerte vers le personnel** - Distinguer les modalités de diffusion de l'alerte en heures ouvrées et en heures non ouvrées ; - Moyens utilisés pour diffuser l'alerte (sirènes, téléphones, espace Intranet, etc.) ; - Personnes désignées à cet effet (DDSL, PCS, gendarmes, etc.) ; - Directives éventuelles données lors de l'alerte (lieu de regroupement, mesures à prendre, consignes de secours, etc.).
2	**Fiches types** - Réalisation de fiches types : o Fiche de procédure d'évacuation (qui peut être similaire à celle d'une évacuation incendie) ; o Fiche de conduite à tenir en cas de découverte d'un colis suspecté de contenir des agents NRBC ; o Autres fiches éventuelles (confinement, gestion de crise NRBC, etc.) ; - Modalités de transmission des fiches (affichage sur le site, mails, etc.) ; Des modèles de fiches types sont disponibles au § 3 de cette annexe.
3	**Plan de recensement** - Comptage réalisé au(x) point(s) de rassemblement : o Indiquer le nombre et l'emplacement du ou des point(s) de rassemblement ; o La ou les personne(s) en charge du comptage ; - Elément servant de comparaison au comptage réalisé (extrait du SI qui gère les CA, la liste du registre des visiteurs, etc.).
Organisation de l'intervention	
1	**Modalités d'intervention interne** (si concerné) - Personnel concerné (astreinte spécialisée, personnels de la sûreté, gendarmes, etc.) ; - Modalités d'activation (moyen utilisé, personnel en charge de l'activation) ; - Délais d'intervention (en minutes) ; - Equipements (faire un renvoi au § 4). - Missions de l'unité d'intervention (levée de doute, secours, neutralisation de la charge NRBC, etc.).

2	**Modalités d'intervention externe** - Type d'unité(s) concernée(s) (SDIS, unités spécialisées : CMIC, CMIR, CMIB, cellule NRBC de la gendarmerie nationale, forces de sécurité intérieure, etc.) ; - Modalités d'activation (moyen utilisé, personnel en charge de l'activation) ; - Distance de l'unité d'intervention par rapport au site (en kms et minutes) ; - Modalités d'accueil sur le site (personne en charge de leur accueil, emplacement de l'accueil sur le site, documents éventuels transmis, point de situation, etc.) ; - Missions de l'unité d'intervention (levée de doute, secours, neutralisation de la charge NRBC, etc.).
4- Organisation matérielle et moyens spécifiques	
4.1 – Moyens de détection et d'identification	
1	**Existence de moyens de détection et d'identification** ☐ Oui ; ☐ Non ; Si non, indiquer [Néant]. Si l'achat de moyens de détection est programmé, préciser l'échéance.
2	**Caractéristiques des moyens de détection** - Nature (explosimètre, ictomètre, dosimètre, radiomètre, mallette de prélèvement, etc.) ; - Nombre ; - Contrôle périodique ; - Lieu de stockage ; - Modalités de mise en œuvre.
4.2 – Moyens de protection	
1	**Existence de moyens de protection** ☐ Oui ; ☐ Non ; Si non, indiquer [Néant]. Si l'achat de moyens de protection est programmé, préciser l'échéance.
2	**Caractéristiques des moyens de protection** - Nature (scaphandres, tenues imperméables ou semi-perméables, appareil respiratoire isolant – ARI-, masques, gants, bottes, etc.) ; - Volume ; - Contrôle périodique (mensuel, trimestriel, etc. Si des équipements ont des dates de péremption et sont gérés comme des produits consommables, le préciser) ; - Lieu de stockage (n° de bâtiment, pièce, etc.) ; - Modalités de mise en œuvre.
5 – Organisation de la formation	
5.1 – Formation et sensibilisation	

1	**Existence de formations et de sensibilisations en matière de risques NRBC** ☐ Oui ; ☐ Non ; Si non, indiquer [Néant]. Si la mise en œuvre de sensibilisation et/ou de formation est prévue, préciser l'échéance.
2	**Sensibilisation** - Objet de la sensibilisation (risque chimique, risque biologique, conduites à tenir, etc.) ; - Nature de la sensibilisation (présentation, mail, fiche réflexe, etc.) ; - Le personnel visé (nouvel arrivant, ensemble du personnel, personnel manipulant des produits spécifiques, etc.) ; - Les personnes/services réalisant la formation (DDSL, organisme extérieur, etc.) ; - Caractéristique de la sensibilisation (périodicité, caractère obligatoire, etc.).
3	**Formation** - Personnel formé (personnel du service sûreté, du service sécurité, éléments du PCS, etc.) ; - Nature et contenu de la formation (reconnaître un colis suspect, mettre en œuvre les mesures d'évacuation, etc.) ; - Caractéristique de la formation (périodicité, caractère obligatoire, etc.).
5.2 – Exercices et entrainements	
1	**Existence d'exercices et d'entrainements** ☐ Oui ; ☐ Non ; Si non, indiquer [Néant]. Si la mise en œuvre d'exercices est programmée, préciser l'échéance.
2	**Caractéristiques des exercices** - Nature des exercices (évacuation, mise à l'abri, déclenchement de l'élément d'intervention, intrusion malveillante avec colis piégé, etc.) ; - Agents concernés par l'exercice (personnel de sûreté, ensemble du personnel, etc.) ; - Périodicité.
6 – Audits et contrôle	
1	**Si concerné, préciser :** - Autorité réalisant l'audit/contrôle (contrôle interne, organismes étatiques, etc.) ; - Périodicité des évaluations ; - Eléments évalués ; - Prise en compte des recommandations (plan d'action, programmation, etc.).

3. Modèles de fiches types

Des fiches types « *Que faire en cas d'exposition à un gaz toxique* » et « *Réagir en cas d'attaque terroriste* » sont disponibles sur le site du Secrétariat général de la défense et de la sécurité nationale (SGDSN).

Fiche de conduite à tenir en cas d'évacuation – alerte NRBC
A L'AUDITION DU SIGNAL D'ALARME OU SOUS ORDRE D'UN RESPONSABLE, ÉVACUEZ. o Dès l'audition du signal sonore, gardez votre sang-froid ; o Dirigez-vous calmement et sans précipitation vers le point de rassemblement ; o Protégez votre nez et votre bouche par tous les moyens possibles (mouchoirs, foulards, tissus humides) ; o Si vous apercevez des gens en train de s'évanouir ou de suffoquer, aidez-les à sortir sans revenir sur vos pas ; o N'utilisez pas les ascenseurs ; o Une fois au point de rassemblement, retirez délicatement votre première couche de vêtements sans en toucher l'extérieur et cherchez à les isoler (si possible dans un sac plastique).

Fiche de conduite à tenir en cas de découverte de plis, colis contenants et substances suspectés de renfermer des agents radiologiques, biologiques ou chimique dangereux
CONSERVEZ VOTRE CALME ET VOTRE LUCIDITÉ. o Reposez immédiatement le pli, le colis ou le contenant suspect ; o Ne le manipulez plus et ne cherchez pas à le déplacer ou à essayer de l'ouvrir ; o Alertez immédiatement les forces de l'ordre et les services de secours ; o Fermez les ouvertures de la pièce afin d'éviter toute propagation ; o Arrêtez les systèmes de climatisation et de ventilation, ou en cas d'impossibilité, obstruez rapidement les bouches de ventilation ; o Eteignez les téléphones portables ; o En cas de perte de substances suspectes, isolez l'objet en le recouvrant par tout moyen approprié sans s'exposer inutilement ; o Enlevez les vêtements souillés sans toucher la partie exposée et laissez-les sur place ; o Toutes les personnes exposées et/ou impliquées doivent quitter le local du lieu de la découverte sans délai et se rendre dans un local confiné dédié. Ces personnes doivent éviter tout contact avec les autres personnels ; o Fermez la pièce à clef afin que personne ne puisse y pénétrer avant l'arrivée des équipes de secours et d'intervention.