DÉPARTEMENT DE VAUCLUSE

COMMUNE DE VILLARS





PLAN COMMUNAL DE SAUVEGARDE





élaboré par le Service Interministériel de Défense et de Protection Civiles – Préfecture de Vaucluse
Mise à jour Septembre 2026

Année 2026

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

SOMMAIRE

Tableau de mise à jour du Plan Communal de Sauvegarde 3
Textes de référence en matière de PCS 4
Arrêté municipal approuvant le PCS 5
Sigles et abréviations 6
Cartographie de la commune 7
PARTIE I : LES RISQUES DE LA COMMUNE 8
I.1. Risque inondation 9
I.2. Risque feux de forêts Nord 10
I.2. Risque feux de forêts Sud 11
I.3. Risque technologique et industriel 12
I.4. Risque transport de matières dangereuses et réseaux 12
I.5. Risque sanitaire 12
I.6. Risque lié au Retrait gonflement des Argiles 13
I.7. Risque sismique 14
I.8. Cavités et Aven 14
I.9. Risque Cyberattaques 15-20
I.10. Risque Paralysie des systèmes d'information 21-27
PARTIE II : DISPOSITIF OPERATIONNEL 28
Organiser la réponse communale 28-31
II.1.1 Le Poste de Commandement Communal (PCC) 32
II.1.2 Schéma d'alerte des membres du PCC 33
II.1.3 Montage opérationnel de la salle du PCC 34
II.2. Rôle des membres du PCC : fiches-actions 35-48
II.3. L'alerte des populations 49
ANNEXES OPÉRATIONNELLES 50
ANNEXE N° 1 : Points de rassemblement de la population 50
ANNEXE N° 2 : Annuaires 50-53
ANNEXE N° 3 : Enjeux sensibles sur la commune 54
ANNEXE N° 4 : Personnes vulnérables 54
ANNEXE N° 5 : Moyens d'hébergement et d'accueil 55
ANNEXE N° 6 : Restauration 55
ANNEXE N° 7 : Moyens de transport collectif 55
ANNEXE N° 8 : Moyens matériels publics communaux 55
ANNEXE N° 9: Moyens matériels privés 55
ANNEXE N° 10 : Moyens matériels des associations se trouvant sur le territoire communal 56
ANNEXE N° 11 : Procédures de vigilance 57
ANNEXE N° 12 : Préparation d'un exercice communal 58
ANNEXE N° 13 : La canicule 59
ANNEXE N° 14 : Modèle d'arrêté de réquisition 60
ANNEXE N° 15 : Main courante 61

Mise à jour Septembre 2026

Année 2026

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

Tableau de mise à jour du Plan Communal de Sauvegarde

Toute mise à jour du PCS devra être mentionnée dans le tableau ci-dessous. Ne pas oublier d'en informer l'ensemble des destinataires du Plan Communal de Sauvegarde :

- Monsieur le Préfet de Vaucluse (Pôle Défense et Protection Civiles).
- Monsieur le Sous-Préfet d'arrondissement.
- Monsieur le Directeur Départemental des Services d'Incendie et de Secours de Vaucluse.
- Monsieur le Colonel commandant le Groupement de Gendarmerie et/ou Monsieur le Directeur départemental de la Sécurité Publique.
- Monsieur le Directeur Départemental des Territoires.
- Monsieur le Commandant du Centre de Secours Principal d'APT
- Monsieur le Commandant de la brigade de Gendarmerie d'APT

Date de mise à jour	Page(s) modifiée(s)	Nature de la mise à jour
2016		Globalité
2023	Mise en concordance intégrale PCS type	Nouvelle municipalité
Septembre 2026	Mise en concordance intégrale PCS type	Nouvelle municipalité

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

Textes de référence en matière de PCS

Le PCS est régi par les dispositions de l'article L731-3 du Code de la sécurité intérieure (Titre III du Livre VII).

Il s'agit d'un document de compétence communale ou intercommunale contribuant à l'information préventive et à la protection des populations. Il détermine et fixe, en fonction des risques majeurs connus dans une commune donnée, l'organisation locale pour faire face à une crise et la gérer.

Ce document intègre et complète les plans ORSEC de protection générale des populations élaborés au niveau départemental par la préfecture.

Le PCS est obligatoire dans les communes :

- Dotées d'un Plan de Prévention des Risques Naturels (PPRN) approuvé.
- Comprises dans le périmètre d'un Plan Particulier d'Intervention (PPI).
- Comprises dans un des territoires à risque important d'inondation (TRI) prévus à l'article L 566-5 du Code de l'environnement ;
- Concernées par une zone de sismicité définie par voie réglementaire (cf article D 563-8-1 du Code de l'environnement) ;
- Concernées par une forêt classée au titre de l'article L 132-1 du Code forestier ou est réputée particulièrement exposée.

Dès lors qu'au moins une des communes membres d'un établissement public de coopération intercommunale à fiscalité propre est soumise à l'obligation d'élaborer un PCS la rédaction d'un Plan Intercommunal de Sauvegarde est obligatoire.
Le plan intercommunal de sauvegarde prépare la réponse aux situations de crise et organise, au minimum :
« 1° La mobilisation et l'emploi des capacités intercommunales au profit des communes ;
« 2° La mutualisation des capacités communales ;
« 3° La continuité et le rétablissement des compétences ou intérêts communautaires.

L'article R731-10 du Code de la sécurité intérieure précise que ce document doit être réalisé dans les deux ans à compter de la date d'approbation des PPRN et/ou PPI.

L'article L.2211-1 du Code Général des Collectivités Territoriales dispose que le maire est l'autorité de police compétente pour mettre en œuvre le Plan Communal de Sauvegarde et il prend toutes les mesures destinées à assurer la protection de ses administrés en cas d'événements affectant directement le territoire de la commune.

Par ailleurs, les communes non soumises à l'obligation d'avoir un PCS peuvent, si elles le souhaitent, en élaborer un.

Les communes membres d'un établissement public de coopération intercommunale à fiscalité propre peuvent confier à celui-ci l'élaboration d'un Plan Intercommunal de Sauvegarde.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

DÉPARTEMENT DE VAUCLUSE
Arrondissement d'Apt
Commune de VILLARS

ARRÊTÉ DU MAIRE portant mise à jour du Plan Communal de Sauvegarde « PCS »
2026ARD070

VU le code de la Sécurité Intérieure, et notamment ses articles L 132-1 relatif au pouvoir de police du maire et L 731-3 sur le plan communal de sauvegarde ;

VU le Code Général des Collectivités Territoriales, et notamment ses articles L2212-2 et L. 2212-4 ;

VU le code de l'environnement, et notamment son article L. 125-2 relatif à l'information préventive sur les risques majeurs ;

CONSIDERANT que la commune de VILLARS est susceptible d'être exposée à des risques de sécurité civile naturels et technologiques de tous types ;

CONSIDERANT qu'il appartient au maire de prévoir, d'organiser et de structurer l'action communale en cas de crise, afin de prendre d'urgence toutes mesures utiles en vue de sauvegarder la population, d'assurer la sécurité et la salubrité publiques et de limiter les conséquences des événements potentiellement graves et susceptibles de se produire sur le territoire de la commune,

ARRÊTE
Article 1 : Le Plan Communal de Sauvegarde « PCS » de la commune de VILLARS annexé au présent arrêté est approuvé et est applicable à compter du 6 Octobre 2026.

Article 2 : Le plan communal de sauvegarde fera l'objet des mises à jour nécessaires à sa bonne application. Conformément à l'article L. 731-3 III du Code de la sécurité intérieure, tous les 5 ans le Maire organisera un exercice associant les membres du Poste de Commandement Communal « PCC » ainsi que les services concourant à la sécurité civile pour éprouver le PCS.

Article 3 : Le plan communal de sauvegarde est consultable en mairie.

Article 5 : Une copie du présent arrêté ainsi que du plan annexé sera transmise à :

- Monsieur le Préfet de Vaucluse (Service Interministériel de Défense et de Protection Civiles).
- Monsieur le Sous-préfet d'arrondissement.
- Monsieur le Directeur Départemental des Services d'Incendie et de Secours de Vaucluse.
- Monsieur le Colonel commandant le groupement de Gendarmerie et/ou Monsieur le Directeur départemental de la Sécurité Publique.
- Monsieur le Directeur Départemental des Territoires.
- Monsieur le Commandant du Centre de Secours Principal d'Apt
- Monsieur le Commandant de la brigade de Gendarmerie d'Apt

Fait à VILLARS, le 6 octobre 2026

Le Maire,
Thomas SAMPIETRO

MAIRIE DE VILLARS VAUCLUSE

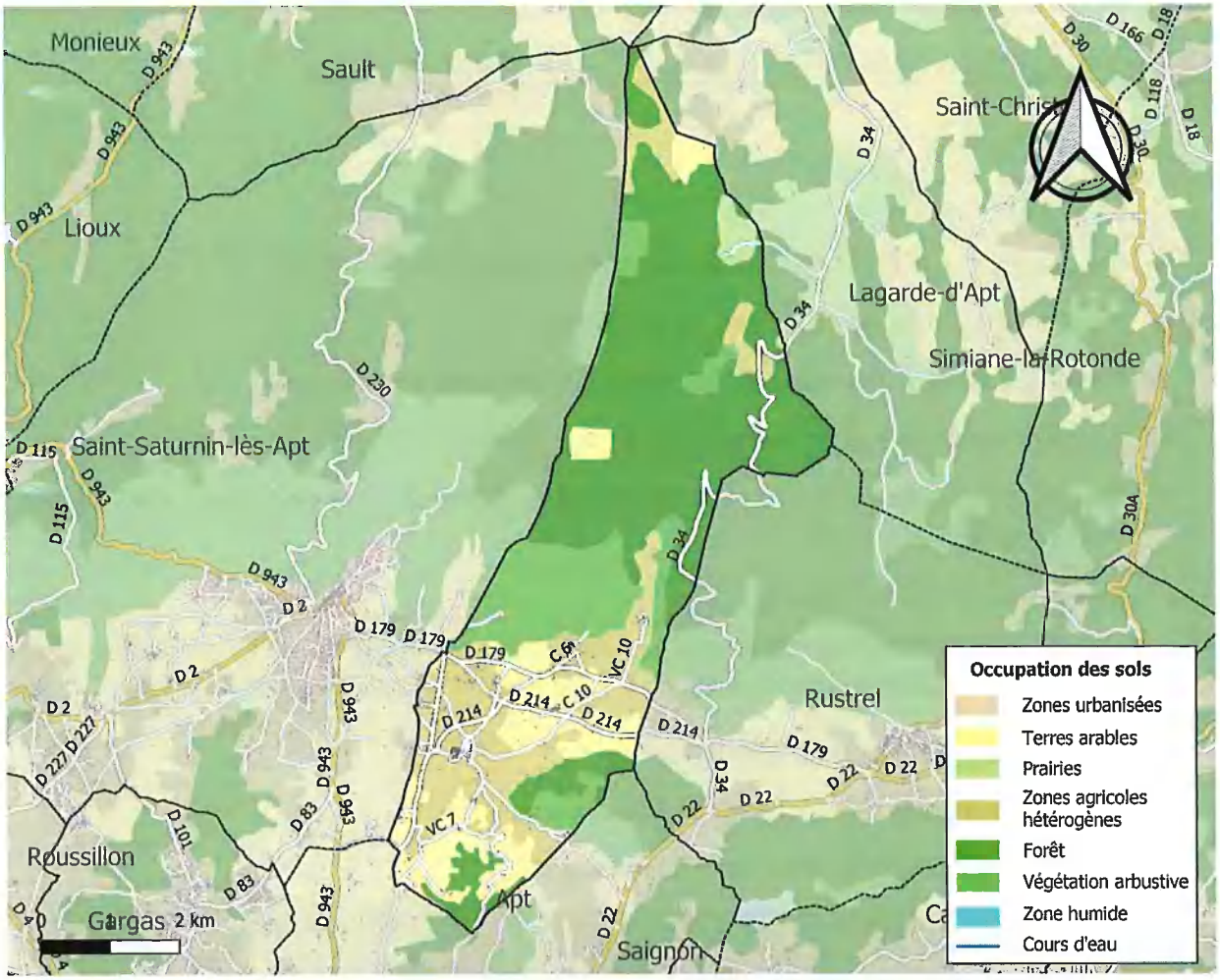
Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

Sigles et abréviations

COD	Centre Opérationnel de Départemental
CODIS	Centre Opérationnel Départemental d'Incendie et de Secours
COZ	Centre Opérationnel Zonal
CORG	Centre Opérationnel et Renseignement de la Gendarmerie
COS	Commandant des Opérations de Secours
CRICR	Centre Régional d'Information et de Coordination Routière
CRS	Compagnie Républicaine de Sécurité
CSP	Centre de Secours Principal
CUMP	Cellule d'Urgence Médico-psychologique
DDCS	Direction Départementale de la Cohésion Sociales
DDPP	Direction Départementale de la Protection des Populations
DDT	Direction Départementale des Territoires
DMD	Délégation Militaire Départementale
DDSP	Direction Départementale de la Sécurité Publique
Dpt	Département
DREAL	Direction Régionale de l'Environnement, de l'Aménagement et du Logement
DSC	Direction de la Sécurité Civile
DSI	Directeur des Secours Incendie
DSM	Directeur des Secours Médicaux
DT ARS	Délégation Territoriale de l'Agence Régionale de Santé
EMDA	Ensemble Mobile de Diffusion de l'Alerte
Gend	Gendarmerie
ICPE	Installation Classée pour la Protection de l'Environnement
Min Int	Ministère de l'Intérieur
PACA	Provence-Alpes-Côte d'Azur
PC	Poste de Commandement
PCA	Poste de Commandement avancé
PCC	Poste de Commandement Communal
PCF	Poste de Commandement Fixe
PDPC	Pôle Défense et Protection Civiles
PK	Point Kilométrique
PMA	Poste Médical Avancé
POI	Plan d'organisation interne
PPI	Plan Particulier d'Intervention
ORSEC	Organisation de la Réponse de SEcurité Civile
RAC	Responsable des Actions Communales
RCC	Centre de Coordination et de Sauvegarde
SAMU	Service d'Aide Médicale d'Urgence
SATER	Recherche et Sauvetage Aéro-TERrestre
SDIS	Service Départemental d'Incendie et de Secours
SNRS	Service de la Navigation Rhône-Saône
SRPJ	Service Régional de Police Judiciaire
TGV	Train Grande Vitesse
TMD	Transport de Matières Dangereuses
TMR	Transports de Matières Radioactives
UDA-PSY	Unité Départementale d'Aide PSYchologique

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

Cartographie(s) de la commune de VILLARS



Accusé de réception en préfecture Sauvegarde
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

PARTIE I : LES RISQUES DE LA COMMUNE

Identification des risques sur la Commune

Liste des aléas

Les risques naturels

- Inondations : plan PPRi de Calavon/Coulon en annexe cartographie
- Feux de forêts : risque en annexe cartographie
- Retrait gonflement des sols argileux : zone en annexe cartographique
- Séismes : commune classée en niveau 3 (modéré)
- Cavités, Souterrains : 1 aven la Pourachière et 2 cavités en cours de fermeture la Loubatière et cavité Naturelle Fo.

Les risques technologiques

Absent ou faible, seuls les transports de matières dangereuses qui traversent la commune peuvent nous concerner et à haut risque de pollution du champ captant et de la nappe phréatique.

Identification des vulnérabilités

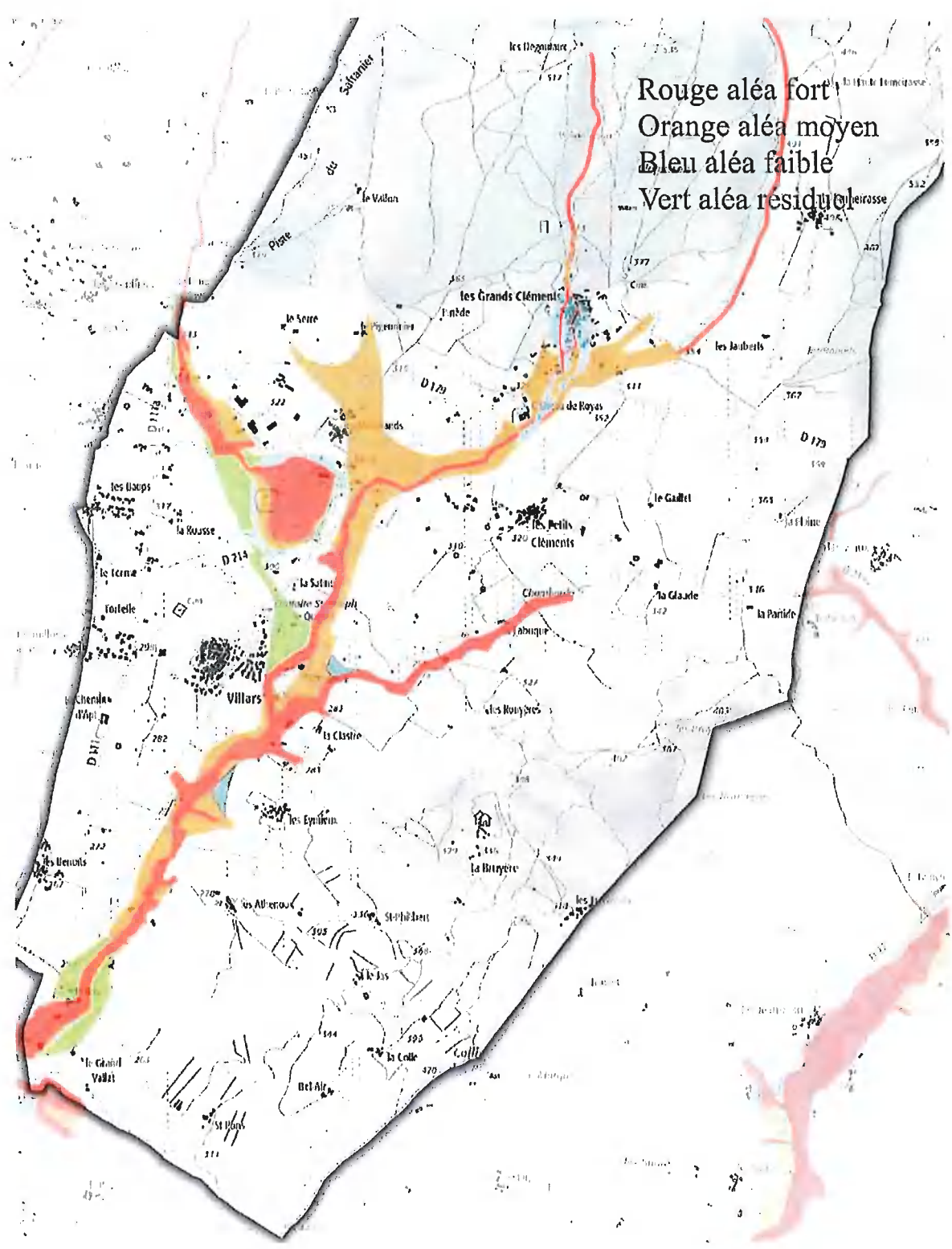
- Nombre d'habitants de la commune : 798 personnes (2026)
- Nombre de hameaux répartis sur la commune : 10

Désignation établissement	Nom Responsable	Tél	Effectif max	Catégorie ERP
École De Villars	Hugues LEROYER	04 90 75 40 55	112	ERP type R 5è cat
La Colline des Ocres	Patrick LEGENDRE NOUVIAIRE	04 90 75 44 58 / 06 14 84 25 42	138	ERP type L 5ème cat
Aire de Services les Hautes Garrigues	SARL SCIERIE LA BERNADETTE	07 72 30 79 51	24 cc	NA

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

I.1. Risque inondation

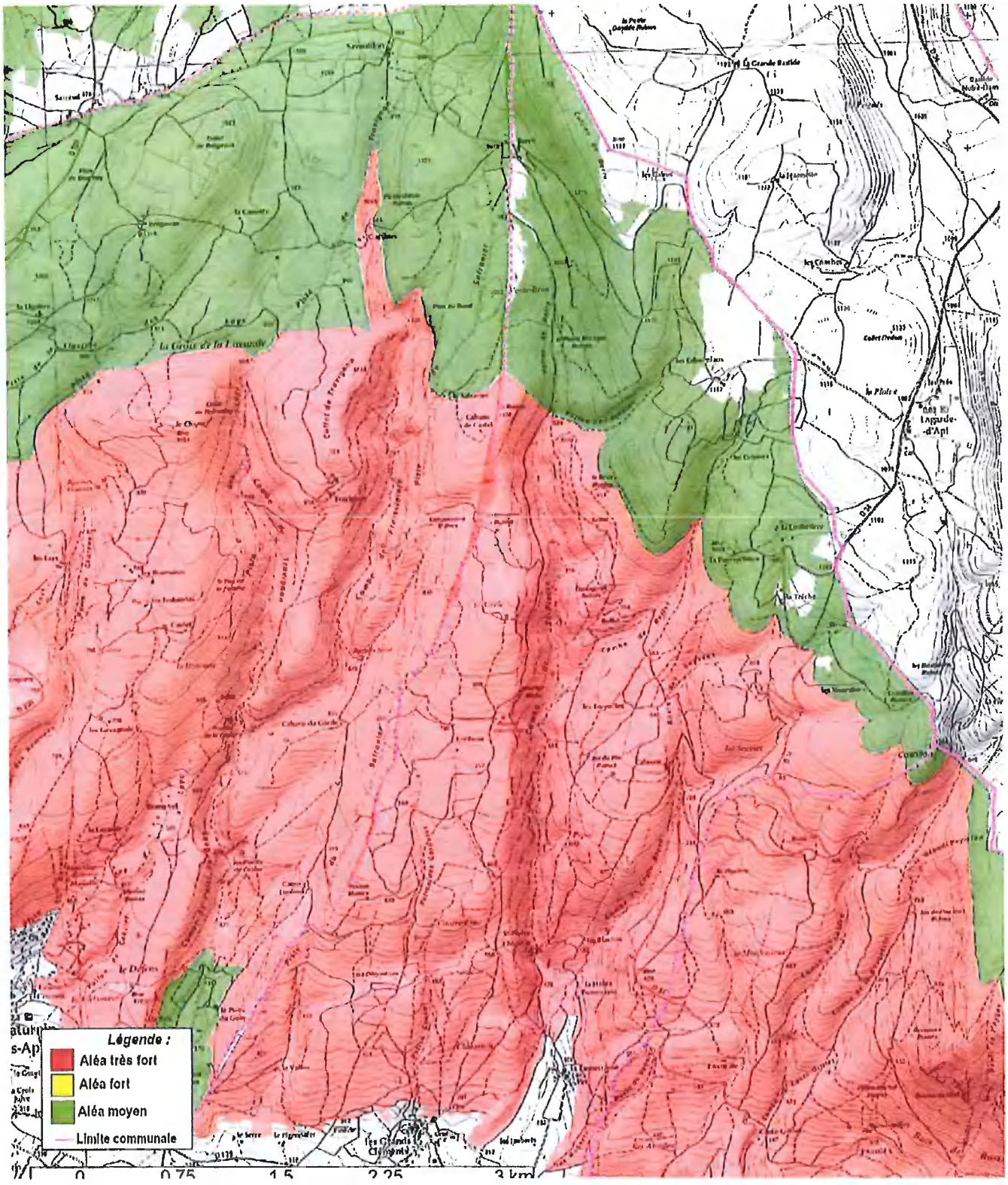
La Commune de VILLARS est concernée par le risque inondation sur le cours du CALAVON ; risque identifié par le PPRi CALAVON-COULON approuvé par arrêté préfectoral du 20/06/2024.



Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

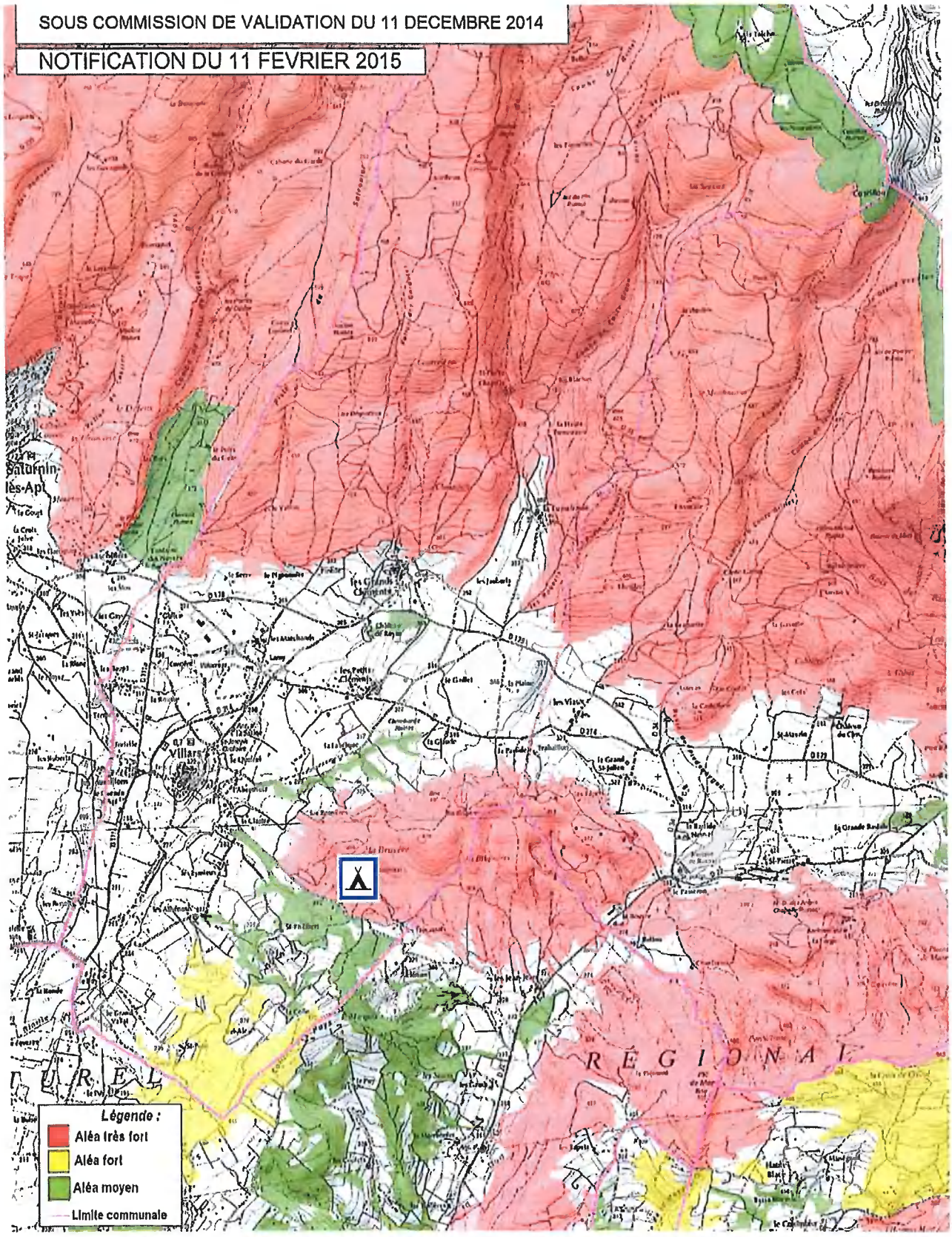
I.2. Risque feux de forêts

Feux de forêt Nord



Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

Feu de forêt Sud



Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

I.3. Risque technologique et industriel

La commune n'est pas située dans le périmètre d'un PPRt.

I.4. Risque transport de matières dangereuses et réseaux « TMD »

Le risque de Transport de Matières Dangereuses est relatif à l'ensemble des marchandises qui circulent par voie routière, ferrée, fluviale et souterraine. Il résulte globalement de la survenue d'un accident, et ne dispose par conséquent d'aucun moyen d'anticipation. Les communes interviennent dans le cadre de missions d'assistance des services de secours et des services de l'Etat pour la gestion de la situation.
Il peut entraîner des conséquences graves pour la population, les biens et/ou l'environnement.

Les produits dangereux sont nombreux ; ils peuvent être inflammables, toxiques, explosifs, corrosifs ou radioactifs.

Les principaux dangers liés aux TMD sont :

- L'explosion occasionnée par un choc avec étincelles, par le mélange de produits… avec des risques de traumatismes directs ou par l'onde de choc,
- L'incendie à la suite d'un choc, d'un échauffement, d'une fuite… avec des risques de brûlure et d'asphyxie,
- La dispersion dans l'air (nuage toxique), l'eau et le sol de produits dangereux avec risques d'intoxication par inhalation, par ingestion ou par contact.

Ces manifestations peuvent être associées.

Les accidents de T.M.D sur la commune de VILLARS sont liés à plusieurs types de voies :

☒ Voies départementales : RD 34/ RD 111/ RD 111a / RD 179 / RD 214

☒ Voies communales

Il s'agit uniquement d'un flux de transit.

Principales actions à réaliser

☐ Mobiliser une équipe à mettre à la disposition des services associés

☐ Empêcher l'accès à la zone de l'accident

☐ Ouvrir un centre d'accueil si besoin

☐ Informer la population située à proximité de l'accident en fonction du contexte

☐ Informer les ERP (établissement scolaire, ...)

☐ Veiller à ce que les personnes évacuées ne réintègrent pas leur domicile sans l'accord des autorités

☐ Rétablir la circulation et l'accès à la zone touchée lorsque tout danger est écarté

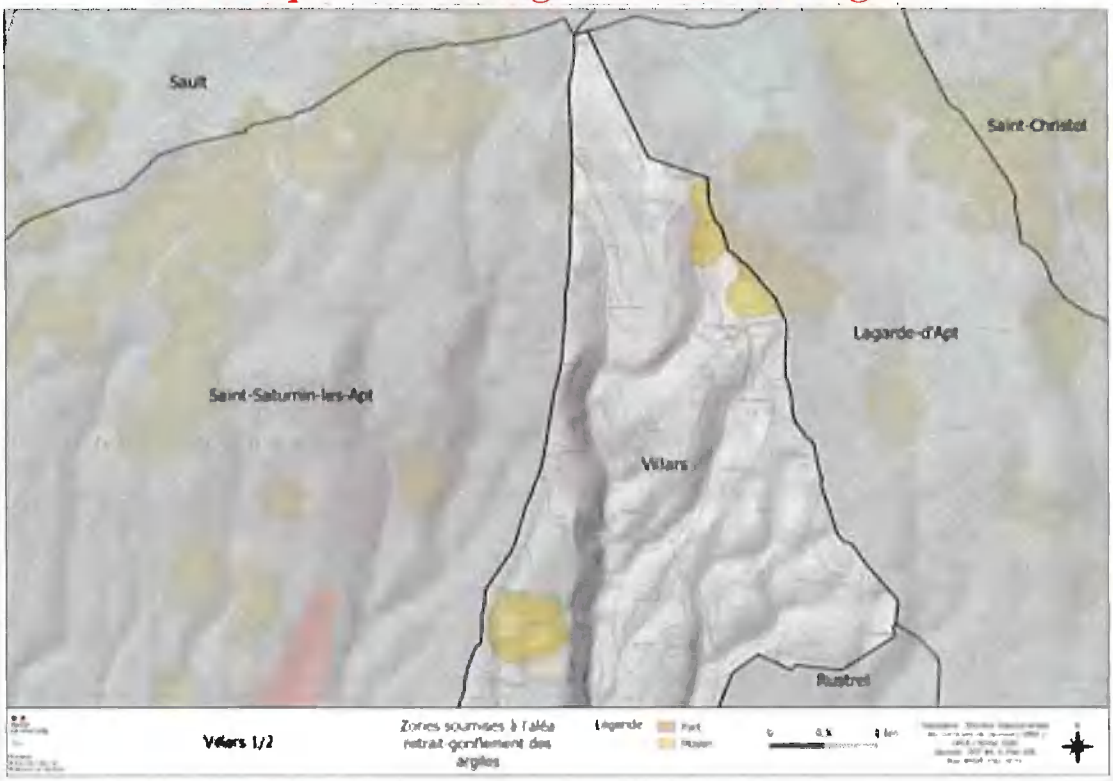
☐ Dresser le bilan des dégâts occasionnés au patrimoine communal

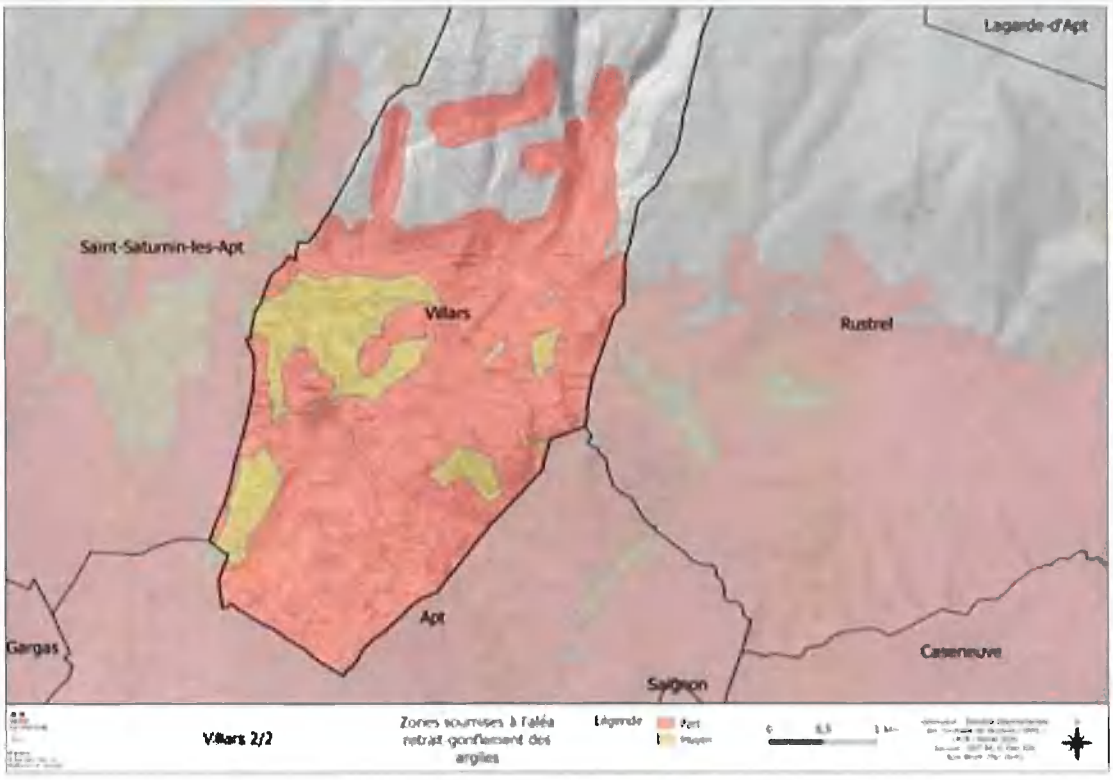
Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

I.5. Risque sanitaire

Toute épidémie/pandémie, Canicule (voir annexe 13 page 59) : suivi des personnes vulnérables (voir annexe 4 page 54)

I.6. Risque lié Retrait gonflement des Argiles

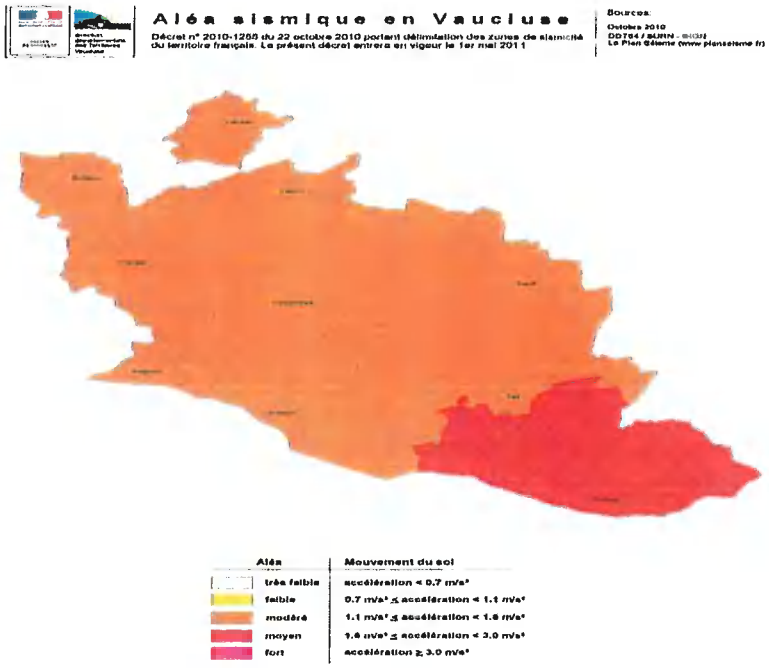




Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

I.7. Risque sismique

La commune de VILLARS est classée en zone sismicité Aléa modéré par le décret n°2010-1254 et 2010-1255 du 22 octobre 2010 relatif à la prévention du risque sismique qui détermine 5 types de zone de sismicité. Tous les IMMEUBLES et les TERRAINS de la commune sont situés dans la zone de sismicité.



I.8. Cavités et Aven



Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

I.9. Risque Cyberattaques

Fiche thématique « Cyberattaques »

1. ÉTAT DES LIEUX

Désireuses de bénéficier des nombreux atouts que proposent les outils numériques et les services en ligne, **les communes et intercommunalités s'appuient de plus en plus sur l'informatique pour mener leurs missions quotidiennes**. Par ailleurs, il est courant que les **données** traitées par ces dernières soient hébergées sur des serveurs informatiques internes ou chez des prestataires (dont des hébergeurs *Cloud* - Informatique en nuage en français).

Or, des groupes ou personnes malintentionnés profitent de cette dépendance croissante au numérique pour s'infiltrer sur ces systèmes informatiques et **mener des actions malveillantes.**

Leurs motivations sont diverses :

- **Gagner de l'argent,** au travers de cyberattaques qui bloquent les systèmes d'information et/ou exfiltrent des données pour ensuite demander une rançon à la victime, voire revendre l'information volée sur le *darkweb*. Les outils numériques peuvent également devenir le canal privilégié de certaines escroqueries (ex : usurpation d'identité, faux ordre de virement). Ces actions sont principalement portées par des groupes cybercriminels.
- **Espionner,** dans le but de récupérer des informations stratégiques ou d'un intérêt particulier pour l'attaquant (ou ses « clients »). Cette action peut être menée par des groupes cybercriminels ou des groupes d'attaquants sponsorisés par des États. À une échelle plus locale, l'espionnage informatique peut servir des intérêts individuels en soustrayant des informations politiques, administratives, financières ou personnelles pour en tirer un bénéfice personnel ou nuire à un adversaire.
- **Déstabiliser,** en rendant inopérantes certains activités-clés d'une entité, voire d'un pays. Cette action peut être menée par des groupes cybercriminels ou des groupes d'attaquants sponsorisés par des États.
- **Revendiquer** une cause politique ou sociétale, en prenant le contrôle de sites web, panneaux d'affichage, etc. pour faire passer des messages (ou les rendre indisponibles – cas du « déni de service »). Cette action est principalement menée par des groupes d'activistes.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI), autorité nationale en matière de cybersécurité et cyberdéfense, constate aujourd'hui que le **nombre de cyberattaques demeure élevé,** touchant sans distinction les entreprises de toute taille et tout secteur, les collectivités territoriales et les établissements de santé.

Cette tendance s'explique de plusieurs façons :

- **Les usages numériques non maîtrisés et les faiblesses dans la sécurisation des données** continuent d'offrir de trop nombreuses opportunités aux attaquants. Si cela est vrai pour les services hébergés et administrés en interne, le recours au *Cloud* (informatique en nuage en français) et l'externalisation de services auprès d'entreprises de services numériques, lorsqu'ils ne s'accompagnent pas de clauses de cybersécurité adaptées, représentent aussi une vulnérabilité importante. Les attaquants peuvent également rebondir s'ils existent des connexions entre différents systèmes (ex : celui d'un prestataire et d'un client).

Plan Communal de Sauvegarde
Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

- **Par manque de sensibilisation, les utilisateurs se font piéger par du « phishing »** (hameçonnage en français), mode opératoire très souvent utilisé par les cyberattaquants pour récupérer des données personnelles ou de connexion par la tromperie (faux courriels, faux sites web), leur permettant notamment d'accéder par la suite à des systèmes d'information en exploitant les mots de passe ainsi obtenus.

- **L'amélioration des capacités des cyberattaquants** (outils, processus) leur permet de mener plus facilement des attaques ciblées ou massifiées. Concernant **les attaques massifiées, elles répondent à des logiques de rentabilité** du côté des cybercriminels : un grand nombre d'entités sont visées, puis l'attaque sera menée là où il existe des failles de sécurité facilement exploitables, par manque d'hygiène informatique (logique de la « pêche au chalut »).

En particulier, il est important de noter qu'**il n'est pas nécessaire d'être une cible pour devenir une victime** : lorsqu'un acteur malveillant envoie un million de courriels malveillants ou rebondit à partir d'un carnet d'adresses déjà piraté, les agents d'une collectivité territoriale peuvent être touchés sans ciblage initial délibéré de la part de l'attaquant.

2. MESURES PREVENTIVES

Face à ces menaces, les communes et intercommunalités doivent donc prendre en compte le risque cyber au juste niveau et adopter les bonnes mesures pour se protéger.

L'objectif est d'atteindre un niveau d'hygiène informatique minimisant la probabilité et l'impact d'attaques « opportunistes », afin de rendre le risque résiduel (celui qui subsiste après l'application des mesures retenues) acceptable. Pour cela, il est notamment important de :

- **Identifier les activités et données clés de la commune, et leurs enjeux de sécurité**
  L'identification (liste, cartographie) des activités et données critiques de la commune et la manière dont elles sont opérées (systèmes internes, externes), puis leur priorisation en matière de confidentialité et disponibilité, sont essentielles pour pouvoir mener des actions de sécurisation des systèmes jugés les plus critiques (briques de sécurité, architecture sécurisée). Elles permettent aussi de savoir quels systèmes relancer en priorité en cas d'incident.

- **Sauvegarder les données les plus importantes et vérifier la capacité à les restaurer**
  Des sauvegardes régulières des données les plus indispensables ou utiles, notamment celles présentes sur les serveurs de fichiers, d'infrastructure et d'applications métier critiques, doivent être réalisées. Il s'agit de garder à l'esprit que ces sauvegardes peuvent aussi être affectées par une attaque par rançongiciel si elles ne sont pas protégées de manière spécifique.
  À titre d'illustration, la règle *de sauvegarde 3-2-1* est une méthode recommandée (par exemple par l'ANSSI dans son guide dédié à la sauvegarde des systèmes d'information). Elle consiste à avoir 3 copies des données (l'original et 2 copies de sauvegardes), sur 2 supports de stockages différents (par exemple 1 copie sur disque dur externe et 1 copie sur système de bande) dont 1 copie hors site et hors connexion (pour éviter que

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

l'attaquant ne détruise ce jeu de données). Enfin, la capacité à restaurer à partir de ces sauvegardes doit être régulièrement testée pour éviter tout blocage inattendu le jour où il est critique de récupérer ces données.

- **Maintenir à jour ses logiciels et systèmes**
  Les vulnérabilités non corrigées des systèmes d'exploitation ou des logiciels présents sur le système d'information peuvent être utilisées pour infecter le système ou favoriser la propagation de l'infection. L'expérience montre que très souvent les failles exploitées par les attaquants donnaient déjà lieu à des correctifs publiés par les éditeurs, correctifs qu'il aurait suffi d'installer pour se protéger au bon niveau.

- **Sensibiliser les agents**
  Le plus souvent, l'attaque par rançongiciel commence par l'ouverture d'une pièce jointe piégée ou la consultation d'une page web malveillante, voire la saisie d'identifiants en pensant accéder à un portail légitime. Ainsi la formation des utilisateurs aux bonnes pratiques de sécurité numérique est une étape fondamentale pour lutter contre cette menace, même si elle ne constitue pas un rempart absolu.

➔ ***D'autres mesures peuvent également être mises en place en s'appuyant sur le diagnostic*** www.monaidecyber.ssi.gouv.fr

3. GERER UNE CRISE D'ORIGINE CYBER

Malgré les efforts de sécurisation déjà mené, le risque qu'une cyberattaque impacte le fonctionnement d'une commune ou intercommunalité existe. Il ne peut être totalement exclu. Dès lors, il s'avère nécessaire d'assurer un certain niveau de résilience, en établissant un plan de réponse aux cyberattaques associé au dispositif de gestion de crise, dans le but d'assurer la continuité des activités puis un retour à un état nominal.

• SPECIFICITES DE LA CRISE CYBER

Une crise « d'origine cyber » se définit par **la déstabilisation immédiate et majeure du fonctionnement courant d'une organisation** (arrêt des activités, impossibilité de délivrer des services, impact sur l'image et la confiance, etc.) **en raison d'une ou de plusieurs actions malveillantes sur ses services et ses outils numériques** (cyberattaques de type rançongiciel, déni de service, etc.).

C'est donc un événement à fort impact, qui ne saurait être traité par les processus habituels et dans le cadre du fonctionnement normal d'une commune.

En comparaison à d'autres scénarios de crise, les crises cyber ont **des caractéristiques propres** qu'il est important d'appréhender :

- L'existence d'une double temporalité des impacts, avec un arrêt immédiat de certaines activités et une remédiation pouvant s'étendre sur plusieurs semaines voire plusieurs mois.
- Une potentielle propagation de l'attaque à d'autres systèmes ou organisations, en raison de l'interconnexion des systèmes d'information.
- Une menace (l'attaquant) s'adaptant aux mesures d'endiguement et de remédiation.
- Une incertitude concernant le périmètre de la compromission et les raisons de l'attaque.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

• PREREQUIS

La gestion d'une crise cyber nécessite donc d'être anticipée, **en apportant un focus particulier sur les actions de préparation suivantes :**

- La mise en place de **processus d'alerte** et de mobilisation du dispositif de crise.
- La **connaissance et la maîtrise des systèmes d'information** et applications métiers.
- L'identification des **activités et données essentielles** et les moyens de les faire fonctionner en mode dégradé.
- L'identification de **réseaux de soutien** (prestataires, CSIRT régional, services de l'État) et de premières actions de confinement de la menace puis de remédiation.
- La mise en place **d'outils résilients,** permettant *a minima* le pilotage et la communication (outils de communication annexes, systèmes de repli, etc.).
- La préparation d'une **stratégie de communication.**

L'objectif est de gagner en fluidité et d'adopter des automatismes, qui permettront de réagir efficacement dans l'immédiat comme sur le temps long, et de redonner confiance aux équipes et à l'écosystème concernés directement ou indirectement par les conséquences de l'incident.

• GOUVERNANCE

La particularité du scénario de crise cyber **implique de mobiliser à la fois des profils métiers, cyber et informatiques.** Il convient donc de planifier une organisation de crise en amont de tout événement et de s'accorder sur le rôle de chaque partie, afin de faciliter la mobilisation.

Le volet « stratégique » (ou « décisionnel ») est logiquement activé, sous la direction du maire ou du directeur général des services, avec pour **mission d'orienter et d'arbitrer la gestion de la crise.**

En parallèle, la mobilisation du **volet « opérationnel » informatique,** sous l'autorité de la direction des systèmes d'information (DSI ou RSSI) doit permettre de **piloter les actions techniques** (en particulier l'investigation, la remédiation et la reconstruction des systèmes d'information et les relations avec les prestataires) et d'exposer au volet « stratégique » **les particularités de la crise cyber** (ex : temps d'investigation long, priorisation dans la reconstruction des systèmes).

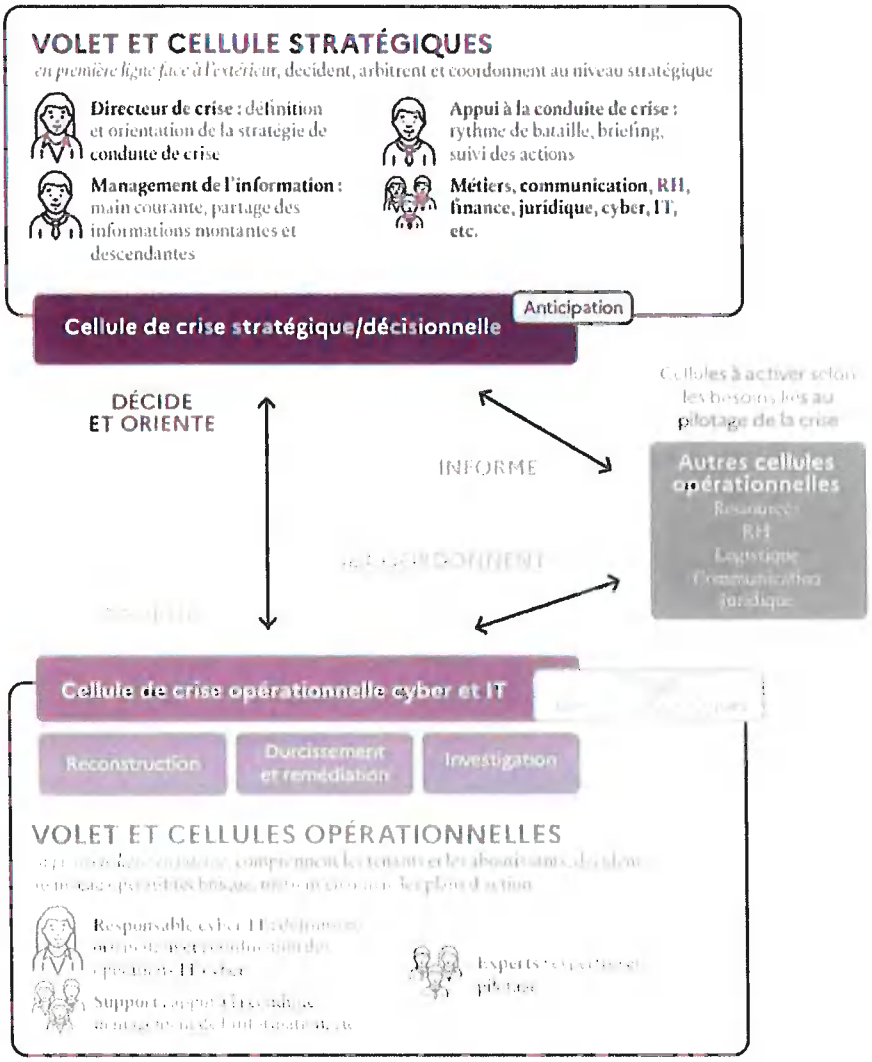
D'autres activités « opérationnelles » sont également à mener en parallèle et en cohérence, par exemple en lien avec les ressources humaines, la logistique et surtout la communication.

La coordination entre tous ces volets est bien évidemment primordiale pour permettre une compréhension mutuelle des enjeux de la crise et une conduite efficace.

Un modèle d'organisation du dispositif **est proposé ci-dessous :**

Plan de Sauvegarde

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026



Source : Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique, ANSSI

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

4. RESSOURCES COMPLEMENTAIRES

- La cybersécurité pour les TPE/PME en treize questions – ANSSI : https://cyber.gouv.fr/publications/la-cybersecurite-pour-les-tpepme-en-treize-questions
- Attaques par rançongiciel, comment les anticiper et réagir en cas d'incident – ANSSI : https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes
- Fiche réflexe Rançongiciel – Cybermalveillance : https://www.cybermalveillance.gouv.fr/medias/2019/11/230417_FicheReflexe_Rancongiciels.pdf
- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique – ANSSI : https://cyber.gouv.fr/publications/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique
- Anticiper et gérer sa communication de crise cyber – ANSSI : https://cyber.gouv.fr/publications/anticiper-et-gerer-sa-communication-de-crise-cyber

  Fiche sur « les mises à jour » – Cybermalveillance : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour

  Fiche sur « les sauvegardes » – Cybermalveillance : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes
- Fiche sur « les rançongiciels » – Cybermalveillance : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares
- Guide « Cybersécurité : toutes les communes et intercommunalités sont concernées » – AMF / ANSSI : https://cyber.gouv.fr/publications/cybersecurite-toutes-les-communes-et-intercommunalites-sont-concernees

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

I.10. Risque Paralysie des systèmes d'information

Fiche-réflexe « Paralysie des systèmes d'information »

Que faire en cas d'attaque par rançongiciel ?

INTRODUCTION

Dans un contexte de numérisation croissante des activités d'une commune, l'un des principaux risques identifiés est **la paralysie de tout ou partie des systèmes d'information** de la commune et/ou des systèmes du prestataire qui hébergerait l'une de ses applications.

Cette situation, empêchant alors la commune d'assurer ses services et activités essentielles, peut notamment être **induite par une cyberattaque, via le déploiement d'un rançongiciel.**

PERIMETRE D'APPLICATION

La fiche-réflexe « paralysie des systèmes d'information » est à utiliser **dans le contexte particulier d'une cyberattaque par rançongiciel** qui :

- ciblerait **directement** les systèmes d'information d'une commune, rendant inaccessible tout ou partie de ses fichiers et/ou applications ;
- ou impacterait les systèmes d'information **d'un prestataire** (informatique ou hébergeur), rendant indisponible au niveau de la commune le(s) service(s) rendu(s).

Une attaque par rançongiciel consiste à déployer un programme malveillant pour obtenir de la victime le paiement d'une rançon. L'attaquant met alors l'ordinateur ou le système d'information de la victime hors d'état de fonctionner, de manière supposée réversible.

Cela peut se matérialiser par :

- La présence d'un message de demande de rançon, qui peut prendre plusieurs formes (fichiers texte, fond d'écran, popup, etc.) ;
- L'impossibilité de lire le contenu de fichiers de travail ;
- Le changement des extensions des fichiers désormais illisibles ;
- Le comportement anormal de certaines applications ;
- Une exfiltration de données.

L'attaquant adresse alors un message à la victime dans lequel il lui propose, contre le paiement d'une rançon, de lui fournir le moyen de déchiffrer ses données.

Les événements accidentels, c'est-à-dire ne résultant pas d'une activité malveillante sur les SI, et les actions malveillantes n'entraînant pas l'interruption immédiate et majeure des services essentiels de l'organisation sont par conséquent exclus du périmètre de définition. Néanmoins, les recommandations de cette fiche **peuvent être utilisées comme bonnes pratiques pour faire face à ces situations.**

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

OBJECTIFS ET LIMITES DE LA PRESENTE FICHE

Ce document a pour objectif de recenser les principaux points d'attention (techniques ou non) utiles pour guider la conduite de la gestion de crise en cas d'attaque par rançongiciel.

Volontairement synthétique et généraliste, **son contenu ne peut en aucun cas remplacer la compétence des experts** requis pour aider à l'endiguement, l'analyse, la remédiation ou la restauration suite à une attaque. De la même manière, **les consignes des forces de sécurité intérieure ou de toutes autres autorités en charge (comme l'ANSSI) doivent primer** lorsqu'elles s'inscrivent dans le cadre législatif et réglementaire idoine.

Plusieurs actions préventives, permettant de réduire la probabilité d'une cyberattaque, sont détaillées dans la fiche thématique « Cyberattaques » également fournie.

1. ANALYSE DE LA SITUATION

- ☐ Remonter tout incident ou dysfonctionnement à la chaîne fonctionnelle. *[Décrire le processus défini et les contacts associés]*

- ☐ Qualifier la situation au travers d'une première analyse rapide et estimer ainsi :

  - Le caractère malveillant du dysfonctionnement (*versus* la simple panne) ;

  > Attention, la caractérisation d'une cyberattaque peut être plus ou moins longue (plusieurs heures) en fonction des informations remontées. Par ailleurs, l'identification de l'origine de l'attaque est longue (plusieurs jours voire semaines) et complexe (besoins de logs, expertise), et ne constitue pas un prérequis aux premières actions de gestion de crise.

  - La criticité de la situation, notamment en matière d'impact sur l'activité.

- ☐ En cas d'incident majeur, donner l'alerte auprès de l'autorité qualifiée à déclencher le dispositif de gestion de crise (PCS) et les actions induites par son déclenchement, dont l'information de l'autorité préfectorale. *[Décrire le processus défini et les contacts associés]*

➔ *Il est recommandé de se référer aux autres fiches réflexes de votre PCS (voir notamment le guide d'élaboration d'un PCS mis à disposition par la préfecture des Bouches-du-Rhône).*

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

2. ACTIONS A MENER EN CAS D'ATTAQUE PAR RANÇONGICIEL

• PREREQUIS

Pour être efficace, la gestion d'une crise d'origine cyber repose sur des compétences particulières (ex : maîtrise des systèmes d'information, expertise interne ou externalisée) et un dispositif spécifique (ex : chaîne d'alerte dédiée, outils résilients, gouvernance).

Des actions préparatoires sont ainsi nécessaires pour mettre en place une organisation de crise adaptée.

Voir les sous-sections « Prérequis » et « Gouvernance » de la fiche thématique « Cyberattaques ».

• MESURES D'URGENCE

☐ **Débrancher les ordinateurs ou les serveurs du réseau sans les éteindre.**

Débrancher le câble Ethernet de chaque ordinateur et de chaque serveur infecté, et désactiver leur connexion Wi-Fi pour isoler ces machines. En cas de doute, faire de même pour l'ensemble des machines.



Attention : si cela paraît contre-intuitif, le fait d'éteindre un appareil infecté ou suspect peut aggraver la situation au redémarrage, et/ou supprimer des indices et preuves pour l'investigation. Il faut donc laisser ces équipements allumés après les avoir isolés du réseau.

☐ **Ne pas allumer les machines qui seraient éteintes avant l'attaque** (afin d'éviter de les infecter).

☐ **Alerter les services ou le prestataire informatique.** *[Coordonnées à insérer]*

☐ **Solliciter de l'aide pour la résolution technique de l'incident** *[Coordonnées à insérer. Exemples : CERT-FR ; CSIRT régional « Urgence cyber, Région Sud » ; Expert Cybermalveillance ; prestataire informatique ; assurance cyber].*

☐ **Vérifier que les sauvegardes sont bien isolées.** Si ce n'est pas le cas, les débrancher du réseau (voir ci-dessus).

☐ **Décider de couper (ou non) la connexion à Internet pour éviter la propagation de l'attaque** (via la box ou l'équipement de cœur de réseau).

Isoler d'Internet le système d'information a généralement des impacts majeurs sur son fonctionnement et les services métiers. Il est préférable d'avoir préparé cette procédure en amont, en ayant pris en compte les situations en heures ouvrées et non ouvrées (qui valide, qui procède à l'opération technique).

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

- **Ne pas payer la rançon.**

Même si le montant de la rançon paraît parfois accessible, rien n'assure après paiement que les fichiers seront déchiffrés ou que l'ordinateur sera de nouveau utilisable. De plus, cela peut contribuer à alimenter un système et démarrer un cercle vicieux : après avoir payé, la commune risque d'être identifiée comme « bon payeur » par les cybercriminels.
Dans certains cas, une solution de déchiffrement existe (voir le site No More Ransom).

• RESOLUTION TECHNIQUE DE L'INCIDENT

La résolution technique d'un incident cyber peut requérir plusieurs semaines à plusieurs mois de travail de la part des équipes internes et/ou du prestataire :

- Dans un premier temps, il est en effet nécessaire d'identifier les raisons du succès de la cyberattaque (notamment le vecteur d'intrusion) pour définir le périmètre de compromission du système d'information, et par conséquent, le niveau de maîtrise dont dispose l'attaquant.
- La compréhension de ces deux éléments doit permettre dans un premier temps de limiter les actions de l'attaquant (endiguement) puis dans un second temps, de l'évincer des systèmes.
- En fonction du périmètre de compromission, des actions de reconstruction, potentiellement sur plusieurs semaines ou mois, pourront alors être envisagées.

- **Procéder à l'investigation**, de préférence avec l'aide du prestataire choisi, afin d'identifier la source de l'infection et prendre les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

- **Faire une analyse antivirale et comportementale du matériel** à l'aide d'une solution de type EDR (*Endpoint Detection and Response*).

- **Conserver les preuves (après avoir pris consigne auprès des forces de sécurité intérieure),** notamment pour pouvoir porter plainte (ex : le message piégé, les fichiers de journalisation (logs) de votre pare-feu, des copies des postes ou serveurs touchés). *Voir la section « enjeux juridiques ».*

➔ ***Si l'on sait garantir l'éradication des éléments malveillants*, réinstaller les systèmes impactés** en effectuant une restauration complète des systèmes infectés, en reformatant les postes ou serveurs touchés, en lançant une réinstallation complète de ces équipements puis des données depuis une sauvegarde vérifiée comme saine.

➔ **Reconnecter le ou les matériels à Internet et/ou aux connexions extérieures existantes,** en s'assurant de la non-persistance des attaquants.

Une reconnexion à Internet ou aux réseaux des partenaires alors que la source de l'infection n'a pas été identifiée et corrigée peut permettre aux attaquants de continuer leurs actions malveillantes.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

3. AIDE-MEMOIRE : ACTIONS A MENER EN PARALLELE

• COMMUNICATION DE CRISE

En fonction de l'impact de l'attaque, il est possible que les outils de communication nominaux (ordinateurs, téléphones, site web) soient indisponibles. Il est nécessaire d'anticiper ce point en envisageant des outils résilients.

☐ **Définir le plan de communication,** en fonction des publics ciblés (contenu du message, moyens de communication, temporalité).

☐ **Alerter et informer les différents publics :**

- *En interne : vers les agents, afin de leur indiquer les consignes et les modalités de continuité de service.*
- *En externe (liste non-exhaustive) :*
  - *Vers les administrés, pour les informer des consignes à suivre et des modalités de la continuité de service.*
  - *Vers l'intercommunalité, en particulier pour éviter une propagation (latéralisation) de l'attaque.*
  - *Vers les autorités (préfecture dans le cadre du déclenchement du PCS, CNIL, etc.).*
  - *Vers vos prestataires et partenaires (trésorerie, fournisseurs, etc.), pour éviter une propagation (latéralisation) et les prévenir des difficultés à venir.*
  - *Vers la presse.*
  - *Sur votre site web.*
  - *Sur les réseaux sociaux.*

☐ **Mettre en place une veille sur les réseaux sociaux,** pour faciliter le suivi des impacts de la communication et anticiper les actions.

☐ **Veiller à informer chaque public concerné de la sortie de crise.**

• CONTINUITE D'ACTIVITE

☐ **Lister l'ensemble des services et activités impactés et se poser la question des impacts induits sur la collectivité (en fonction du contexte socio-politique).**

☐ **Mettre en place les solutions de travail provisoires.**

Il est particulièrement risqué de remettre en production le système d'information impacté tant que les investigations et la remédiation n'ont pas abouti.
Il est donc préférable d'avoir prévu des systèmes alternatifs et provisoires afin de fournir quelques services essentiels, notamment pour la gestion de crise (téléphones avec partages de connexion, postes informatiques isolés avec imprimantes directement connectées, fax, messagerie externalisée provisoire, etc.).

Plan Communal de Sauvegarde
Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

❑ **Identifier les services et activités à relancer / reconstruire en priorité.**

Le plan de continuité d'activité (PCA) et/ou le plan de reprise d'activité (PRA) sont deux documents permettant d'identifier les activités essentielles d'une commune et les moyens d'assurer leur continuité (de manière dégradée ou nominale).
Une priorisation des actions techniques est faite en fonction des besoins de continuité d'activité et des obligations légales que doit respecter la commune (ex : fourniture de l'état civil – voir section « enjeux juridiques »). Elle est validée par le maire. Des communications aux utilisateurs et aux parties prenantes externes sont réalisées quand les services rouvrent.

❑ **S'assurer en particulier qu'il est possible de verser** la paie des agents et/ou les prestations sociales aux administrés.

En cas d'indisponibilité des éléments financiers, il peut être envisagé de se baser sur le versement effectué le mois précédent. Il est recommandé de contacter la DDFIP pour traiter ce sujet.

• METTRE EN PLACE UNE LOGISTIQUE ADAPTEE AUX ENJEUX ET A LA DUREE DE LA CRISE

➔ *Il est recommandé de se référer aux autres fiches réflexes de votre PCS*
(voir notamment le guide d'élaboration d'un PCS mis à disposition par la préfecture des Bouches-du-Rhône).

• RESSOURCES HUMAINES

Redéployer les agents sur certaines activités.

La perte des services numériques augmente le temps de travail (ex : rédaction à la main, archives). Pour gagner en efficacité sur ce qui est important et prioritaire, il peut être nécessaire de redéployer du personnel (notamment des agents dont l'activité serait à l'arrêt suite à l'attaque).

❑ **Préserver les agents en assurant des roulements et des créneaux de repos** (en particulier pour les équipes informatiques).

En complément, de la restauration, des moyens de transport peuvent être mis à disposition des équipes impliquées (notamment en dehors des jours/heures ouvrés habituels). Un réaménagement temporaire d'une partie des locaux peut être effectué si nécessaire.

• ENJEUX JURIDIQUES

❑ **Identifier si certaines obligations auprès des administrés, des partenaires ou des fournisseurs ne peuvent pas être respectées.**

Le cas échéant, adapter le plan de continuité/reprise d'activité pour garantir des actions prioritaires. Dans un contexte d'élections, il est également important de pouvoir assurer le déroulement du processus électoral.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

- ☐ **Porter plainte** auprès du commissariat de police ou de la brigade de gendarmerie dont dépend la commune (au plus tôt et en parallèle de la résolution technique de l'incident).

- ☐ **En cas d'atteinte aux exigences en matière de protection des données personnelles, déclarer son incident auprès de la CNIL** *[Notifier une violation de données personnelles | CNIL].*

- ☐ **Renforcer la vigilance vis-à-vis des fraudes d'opportunité.**

Des personnes malintentionnées, informées de la cyberattaque visant la commune, peuvent profiter de la situation pour commettre des fraudes (ex : fraude au faux virement). Il est conseillé de mettre en place des processus de vérification et de validation, en particulier pour les paiements.

• SORTIE DE CRISE

- ☐ **Vérifier que les conditions nécessaires à la sortie de crise sont atteintes.**

Les conséquences d'une attaque sur l'activité d'une commune peuvent être visibles pendant plusieurs mois, voire après une année (ex : maintien de processus dégradés, réinstallation du matériel).

- ☐ **Veiller à informer tous les publics concernés de la sortie de crise.**

- ☐ **Effectuer un retour d'expérience sur la crise** (et adapter la fiche-réflexe en conséquent).

Le préfet de département a validé le 13 avril 2023 un dispositif départemental opérationnel post-événementiel (DDOPE). Ce document recense les principes d'actions à mettre en œuvre, tant par les services de l'État et les collectivités territoriales que par les acteurs associatifs et le secteur privé pour œuvrer à la résilience, après la survenue d'un événement d'ampleur ayant gravement impacté un territoire et sa population. Il présente les dispositifs connexes facilitant la gestion post-événementielle et le retour à la normale (plan de continuité d'activité, retour d'expérience).

Ce document est communicable sur demande à l'adresse pref-siracedpc@bouches-du-rhone.gouv.fr

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

PARTIE II : DISPOSITIF OPERATIONNEL

Organiser la réponse communale

Modalités de déclenchement du plan communal de sauvegarde

Le plan communal de sauvegarde est **activé par le Maire ou par son représentant désigné, sans formalisme particulier**.

- De la propre initiative du Maire, dès lors que les renseignements reçus par tout moyen ne laissent aucun doute sur la nature de l'événement. Il en informe alors automatiquement l'autorité préfectorale.
- À la demande de l'autorité préfectorale (le Préfet ou son représentant).

Dès lors que l'alerte est reçue par le Maire ou par son représentant, celui-ci doit, dans un premier temps, constituer la cellule de crise municipale.

Organisation du dispositif communal

Le Maire ou l'Élu représentant

Pendant la crise, le maire ou son représentant fait partie intégrante du dispositif de secours. En cas de sinistre dit limité et présent uniquement sur le territoire de la commune, il est désigné « Directeur des Opérations de Secours » (DOS). Dans cette mission il doit :

- Diriger et coordonner les actions des intervenants
- Assurer et coordonner la communication
- Informer les niveaux administratifs supérieurs
- Anticiper les conséquences de l'événement
- Mobiliser les moyens publics et privés sur le territoire

Il est aidé dans sa tâche par le Commandant des Opérations de Secours (COS), le sapeur-pompier le plus gradé, qui le conseille. Il va exercer son rôle depuis le Poste de Commandement Communal (PCC). Le maire peut faire appel au Préfet en cas d'alerte qui dépasse sa compétence.

D'un point de vue opérationnel, sa mission est de prendre du recul pour avoir une vision globale. Ce recul ne doit pas nuire à son autorité et à son pouvoir de décision. Ainsi, il doit être en mesure de valider ou de modifier la stratégie de réponse proposée. Son rôle sera également dans le contact à la population pour l'informer de la crise, la rassurer mais également prévenir au cas par cas des mauvaises nouvelles (décès, destruction, etc.). En cas de crise où le(a) préfet(e) se saisit de la direction des secours, il/elle n'est pas exclu(e) de la chaîne : il/elle va avoir un rôle d'agent de liaison avec le(a) Préfet(e), en apportant son expertise sur le territoire, mais également avec les autres maires impactés et pourra se retrouver en première ligne avec les médias.

Coordination des moyens et des actions

Le Maire ou son représentant doit être épaulé par un chef de poste de commandement communal. Structure de coordination entre le DOS et les équipes de terrain par laquelle transitent toutes les informations montantes et descendantes.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

Selon l'événement et la cinétique de la situation, le(a) chef de PCC doit être en mesure de prioriser les interventions et aussi d'avertir du risque de dépassement des moyens communaux et de la nécessité de faire appel aux échelons supérieurs.

Les équipes de terrain

Elles sont chargées de mener à bien les différentes missions de sauvegarde définies par le responsable du PCC selon les directives du DOS. Elles sont aussi en charge de faire remonter des informations complémentaires sur l'évolution de la situation sur le terrain.

Répartition des tâches de l'équipe municipale

Cf. fiches action en annexe.

Organisation de l'alerte

Liste des contacts pour la préfecture

NOM	Prénom	Tel portable / bureau	Rôle	Mail
SAMPIETRO	Thomas	06 59 35 28 67	Maire	thomas.sampietro@mairievillars84.fr
BALAZUN	Corinne	06 42 15 70 37	1ère adjointe	corinne.balazun@mairievillars84.fr
MUSSO	Tristan	06 13 53 02 75	4ème adjoint	tristan.musso@mairievillars84.fr
SAUTEL	Benoit	06 71 40 92 30	Conseiller municipal	benoit.sautel@mairievillars84.fr
SILVA	Emeline	04 90 75 40 01	Secrétaire de Mairie	secretairegenerale@villars84400.fr

Qui alerter ?

Le Maire ou son représentant prend la décision de diffuser l'alerte après évaluation de la situation. L'alerte peut concerner selon la situation :

- Toute la population : tempête, canicule, grand froid, neige, phénomène pluvieux
- Une partie de la population : mouvements de terrains, incendie, accident TMD

Les moyens d'alerter

L'**alerte** : c'est la diffusion en phase d'urgence par les autorités, d'un signal destiné à avertir la population d'un danger, imminent ou en train de produire ses effets, susceptible de porter atteinte à leur intégrité physique et nécessitant d'adopter un comportement réflexe de sauvegarde.

L'information : consiste à diffuser des consignes de comportement de sauvegarde, par anticipation ou concomitamment à un danger grave, puis à notifier la fin de la situation de péril avant de communiquer les conseils pouvant favoriser le retour à la normale (procédure de catastrophe naturelle, actions préventives adoptées...).

La fonction « information » est complémentaire de la fonction « alerte ».

Sources des alertes : APIC/vigicrue flash, Météo France, préfecture de Vaucluse, Smartemis.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

L'alerte à l'ensemble de la population

Moyens	Lieu	Opérateur	Observation
Site internet	Mairie de Villars	Secrétaire	
Application mobile	NA	Personnes ressources	Appli Panneau Pocket
FR-Alert	NA	Préfecture	Notifications
Affichage Public	Commune	Secrétaire et ouvriers	Anticipation pour lecture

L'alerte ciblée par personnes ressources (hameaux)

Nom / Prénom	Hameau	GSM
BALAZUN Corinne	Les Grands Cléments	06 42 15 70 37
DE KERVILER Christine	Les Petits Cléments	06 88 49 23 28
BONAMY Déborah	Les Baups	06 74 91 50 22
JEAN Marlène	Les Joumillons / Le Logis Neuf	07 77 39 65 37
MUSSO Tristan	Les Marchands	06 13 53 02 75
CELIE Thomas	Les Trécassats	06 05 97 79 37
NICOLE Romain	La Fumeirasse	06 20 28 00 51
SAUTEL Benoit	Les Athenoux	06 71 40 92 30
VANEL Magali	Les Benoits	06 02 39 77 99
LEROYER Hugues	Les Eymieux	06 71 75 22 97

Soutien aux populations : mise en place de centres d'accueil et de regroupement

L'ouverture et la mise en œuvre du centre d'accueil et de regroupement des populations est géré par le responsable du soutien aux populations (cf. fiche action en annexe).

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

Nom structure	Superficie (m²)	Capacité d'accueil	Ouverture	Équipement
Salle des fêtes	135	135	Clefs mairie ou Maire	Tables, chaises, point chaud, point froid, WC, points d'eau, DAE
Cantine scolaire	75	75	Clefs mairie ou Maire	Tables, chaises, point chaud, point froid, WC, points d'eau
École	354	112	Clefs mairie ou Directeur ou Maire	WC, points d'eau, dortoir
Chapelle St Roch	91	21	Clefs mairie ou Maire	WC, points d'eau, tables
Auberge du Villarsois	117	100	Clefs mairie ou Maire	Tables, chaises, point chaud, point froid, WC, points d'eau

Recensement des moyens matériels et humains mobilisables

Recensement des moyens humains

Les employés municipaux titulaires et/ou vacataires et/ou intérimaires peuvent être sollicités pour venir participer au plan de sauvegarde communal, ce en fonction des compétences dans le cadre d'emploi dans la commune.

De même, l'ensemble des conseillers et adjoints municipaux peuvent être sollicités dans le cadre de leur compétence.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

II.1. Le Poste de Commandement Communal (PCC)

II.1.1. Organigramme du PCC

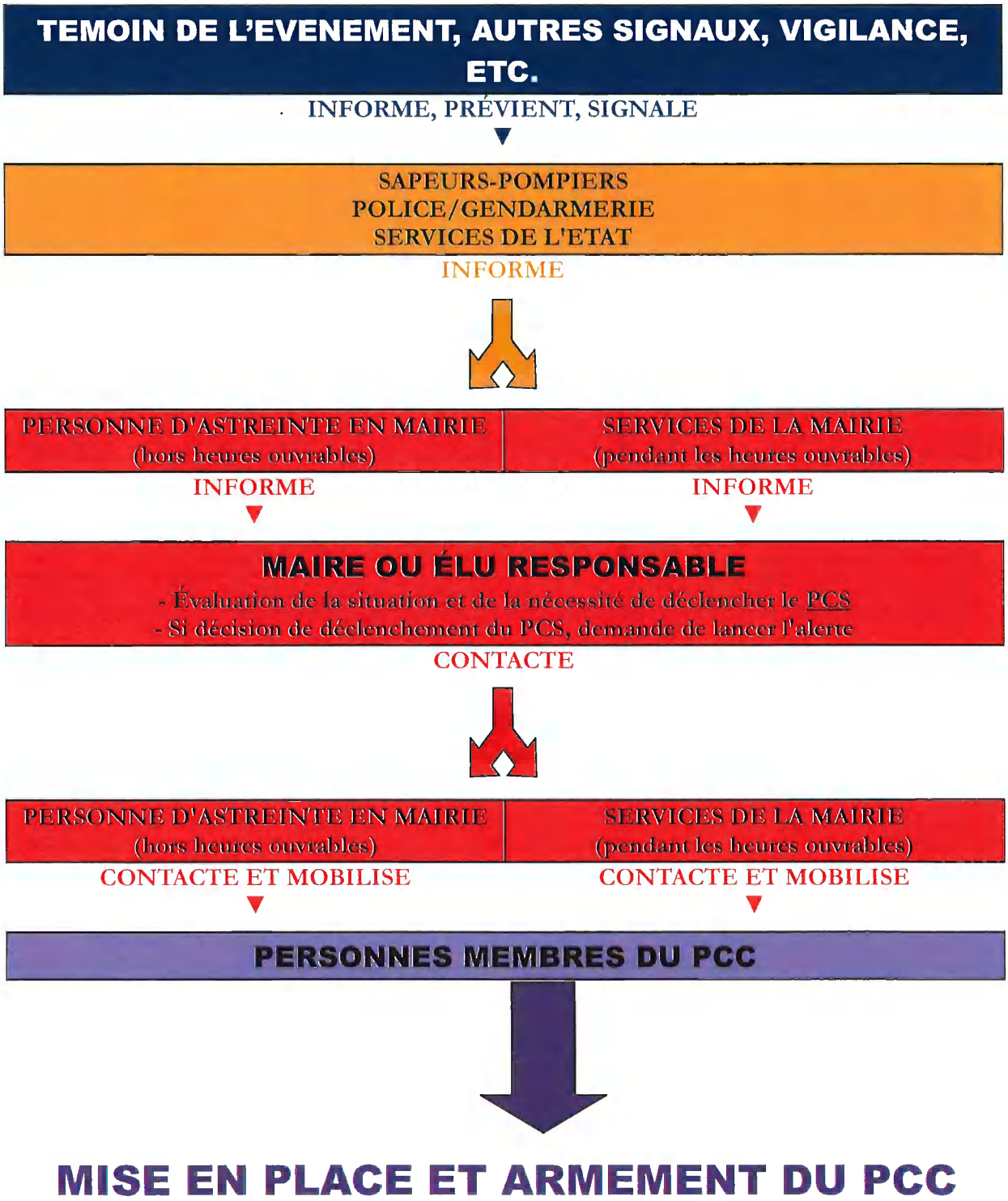
MAIRE = DOS	
SAMPIETRO Thomas	Tél : 06 59 35 28 67
Suppléant : SAUTEL Benoit	Tél : 06 71 40 92 30
ELU = RAC	
BALAZUN Corinne	Tél : 06 42 15 70 37
Suppléante : JEAN Marlène	Tél : 07 77 39 65 37

▼ ▼ ▼

Cellule SECRÉTARIAT / COMMUNICATION	Cellule TERRAIN	Cellule LOGISTIQUE
Responsable : DE KERVILER Christine Tél : 06 88 49 23 28 **Suppléante :** JULIEN Sarah Tél : 06 17 39 05 23	**Responsable :** LEROYER Hugues Tél : 06 71 75 22 97 **Suppléant :** REMICHE Nicolas Tél : 06 77 21 84 91	**Responsable :** MUSSO Tristan Tél : 06 13 53 02 75 **Suppléant :** NICOLE Romain Tél : 06 20 28 00 51
Personnel : VANEL Magali Tél : 06 02 39 77 99 MENSE Marilyne Tél : 06 86 65 12 28	**Personnel :** CELIE Thomas Tél : 06 05 97 79 37 BONAMY Déborah Tel : 06 74 91 50 22	**Personnel :** FERRIER Lionel Tél : 06 26 54 55 10

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

II.1.2. Schéma d'alerte des membres du PCC



Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

II.1.3. Montage opérationnel de la salle du PCC

SALLE DU PCC

SALLE DU CONSEIL MUNICIPAL

Adresse exacte : 8 place de la Mairie 84400 VILLARS

Accès GPS : 43.923115, 5.405043

Équipements de la salle du PCC		
Type d'équipement	**Présence**	**Détails**
Lignes téléphoniques fixes	OUI	Nombre 3
Téléphones mobiles	OUI	Nombre 2 à 5 Voir coordonnées PCC
Accès Internet	OUI	WIFI
Ordinateur	OUI	Nombre 4
Imprimante	OUI	Nombre 2
Scanner	OUI	Nombre 2
Photocopieur	OUI	Nombre 2
Rétroprojecteur	OUI	Nombre 1
Radio	NON	Nombre
Défibrillateur	OUI	Nombre 1
Fournitures de bureau (tableau blanc, papeterie, etc.)	OUI	- 6 tables - 25 chaises - papeterie
Documents utiles (PCS, plans, cartographies, annuaires, liste et adresse des habitants de la commune etc.)	OUI	- Plans, PCS, - Annuaire, Main courante

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

II.2. Rôle des membres du PCC : fiches-actions

FICHE ACTION N° 1 : Le DOS

DOS = Directeur des Opérations de Secours (fonction assurée par le Maire)

RESPONSABLE

M. le Maire
SAMPIETRO Thomas
Tél : 06 59 35 28 67

SUPPLÉANT

SAUTEL Benoit
Tél : 06 71 40 92 30

En cas de déclenchement du PCS, le Maire devient le DOS.

Le DOS analyse la situation, détermine les actions prioritaires, et ordonne l'exécution selon les éléments connus du PCC.

ROLE DU DOS

- Chargé de décider des orientations stratégiques de sauvetage et de sauvegarde de la population.
- Choisit et valide si nécessaire les actions proposées par le COS.

DÉTAIL DES MISSIONS PRINCIPALES

- Déclenchement du PCS.
- Évaluation de la situation et des besoins au vu des remontées du terrain (par le COS et le responsable « Terrain » du PCC au fur et à mesure de l'événement).
- Si nécessaire, prise des ordres de réquisition, d'interdiction, d'autorisation exceptionnelles afin d'assurer la sûreté, la salubrité et la sécurité publiques.
- Mobilisation des moyens publics ou privés.
- Communication avec la population communale.
- Renseignement des autorités.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

FICHE ACTION N° 2 : Le RAC

RAC = Responsable des Actions Communales / Coordonnateur des Actions communales

RESPONSABLE	
BALAZUN Corinne Tél : 06 42 15 70 37	SUPPLÉANTE JEAN Marlène Tél : 07 77 39 65 37

Le RAC est l'interlocuteur privilégié du COS dans la mise en œuvre des actions de terrain communales qui s'inscrivent en amont ou en périphérie des opérations de secours.

Le RAC assure la direction et la coordination des actions des membres du PCC : responsable secrétariat/communication, responsable terrain, responsable logistique.

Le RAC a autorité sur les moyens municipaux.

ROLE DU RAC

- **Assure la liaison avec les autorités "opérationnelles" (le DOS et le COS)**
- **Anime le poste de commandement communal (PCC)**
- **Assure la direction et la coordination des actions des membres du PCC : responsable secrétariat/communication, responsable terrain, responsable logistique.**

DÉTAIL DES MISSIONS PRINCIPALES

- **S'assure de la mise en place du dispositif, veille à ce que les actions décidées par le DOS soient réalisées et transmet les ordres au terrain**
- **Est en lien permanent avec le DOS et se tient informé des décisions prises**
- **Après analyse et réflexion, il propose les options stratégiques au DOS aux fins de décisions. Si le DOS n'est pas joignable, il lui appartient de prendre les décisions qui sont dictées par l'urgence**
- **Assure la direction et la coordination des actions des membres du PCC : responsable secrétariat/communication, responsable terrain, responsable logistique.**
- **Fait régulièrement des points de situation avec les responsables des cellules opérationnelles puis rend compte au DOS.**

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

FICHE ACTION N° 3 : Cellule Secrétariat/Communication

RESPONSABLE

DE KERVILER Christine
Tél : 06 88 49 23 28

SUPPLÉANT

JULIEN Sarah
Tél : 06 17 39 05 23

PERSONNELS

VANEL Magali
Tél : 06 02 39 77 99

MENSE Marilyne
Tél : 06 86 65 12 28

RÔLE

- Chargé de la synthèse et du regroupement de toutes les informations.
- Appui pour répondre aux besoins du PCC.
- Réception, transmission et diffusion d'information en interne au sein du PCC et en externe (grand public notamment).

DÉTAIL DES MISSIONS PRINCIPALES

- Appel des membres du PCC pour intégrer le PCC.
- Organisation de la salle du PCC.
- Accueil téléphonique du PCC.
- Tenue de la main courante.
- Rédaction et transmission des documents émanant du PCC.
- Appui aux autres cellules du PCC.
- Réception et diffusion des informations en interne et en externe.
- Tenue du calendrier des événements du PCC.
- Gestion de la logistique du PCC (approvisionnement en matériel, papeterie etc.).
- Diffuser l'alerte à la population ou aide à la diffusion.
- Assurer la communication avec la population, rédaction des communiqués de presse et relation avec les médias sous la responsabilité du maire et en lien avec lui.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

FICHE ACTION N° 4 : Cellule Terrain

RESPONSABLE

LEROYER Hugues
Tél : 06 71 75 22 97

SUPPLÉANT

REMICHE Nicolas
Tél : 06 77 21 84 91

PERSONNELS

CELIE Thomas
Tél : 06 05 97 79 37

BONAMY Déborah
Tél : 06 74 91 50 22

RÔLE

- Assurer les missions d'évaluation de la situation sur le terrain et de sécurisation des zones.
- Assurer la coordination entre les décisions d'actions de sauvegarde prises au PCC et les missions de secours réalisées sur le terrain par les services de secours.
- Assure au mieux les missions de secours à exécuter sur le terrain, en cas d'absence des services de secours.

DÉTAIL DES MISSIONS PRINCIPALES

- Suivi et surveillance de la situation sur le terrain.
- Évaluation des besoins sur place (évacuation, moyens particuliers humains ou matériels).
- Remontée d'informations vers le PCC sur la situation.
- Sécurisation des zones à risque (mise en place de périmètres de sécurité, panneaux indicateurs etc.).

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

FICHE ACTION N° 5 : Cellule Logistique

RESPONSABLE

MUSSO Tristan
Tél : 06 13 53 02 75

SUPPLÉANT

NICOLE Romain
Tél : 06 20 28 00 51

PERSONNEL

FERRIER Lionel
Tél : 06 26 54 55 10

RÔLE

- Gestion des moyens humains et matériels, publics ou privés.
- Assurer le ravitaillement des personnes sinistrées et des acteurs communaux intervenant dans la crise.
- Mise en œuvre des solutions d'hébergement des personnes sinistrées et/ou évacuées.
- Rassemble le matériel communal et/ou se procure le matériel nécessaire à la réalisation des tâches.

DÉTAIL DES MISSIONS PRINCIPALES

- Gestion, le cas échéant, des modalités d'utilisation du ou des système(s) d'alerte de la population.
- Mise à disposition des autorités et autres personnes intéressées (bénévoles par exemple), des moyens matériels et humains, publics ou privés recensés par la commune.
- Gestion des modalités d'utilisation de ces moyens.
- Gestion des transports (notamment transport collectif des personnes évacuées).
- Organisation des moyens de ravitaillement (notamment transport des marchandises, portage et préparation de repas).
- Gestion des rassemblements de personnes à évacuer (information des personnes concernées pour qu'elles puissent se préparer à leur départ, regroupement des personnes à des points de rassemblement prédéterminés).
- Mise à disposition et gestion des moyens d'hébergement, de ravitaillement...

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

FICHE ACTION N° 6 : Actions alerte
Camping soumis à risque feu de forêt

Coordonnées de la mairie	
Maire	*SAMPIETRO Thomas*
Téléphone	*06 59 35 28 67*
Astreinte	*SAUTEL Benoit*
Téléphone	*06 71 40 92 30*

Informations sur le camping	
Camping	*Camping « La Colline des Ocres »*
Adresse	*1649 Route des Trecassats 84400 Villars*
Exploitant	*LEGENDRE-NOUVIAIRE Patrick*
Téléphone	*04 90 75 44 58 / 06 14 84 25 42*
Courriel	*campinglesbardons@gmail.com*
Nombre d'emplacements	*23*
Capacité	*138*
Période d'ouverture	*Toute l'année*
Autres informations utiles	*23 chalets*

Informations sur le risque	
Nature du risque	*Feux de forêts*
Aléa	*Aléa très fort*
Nom du massif	*La Bruyére*

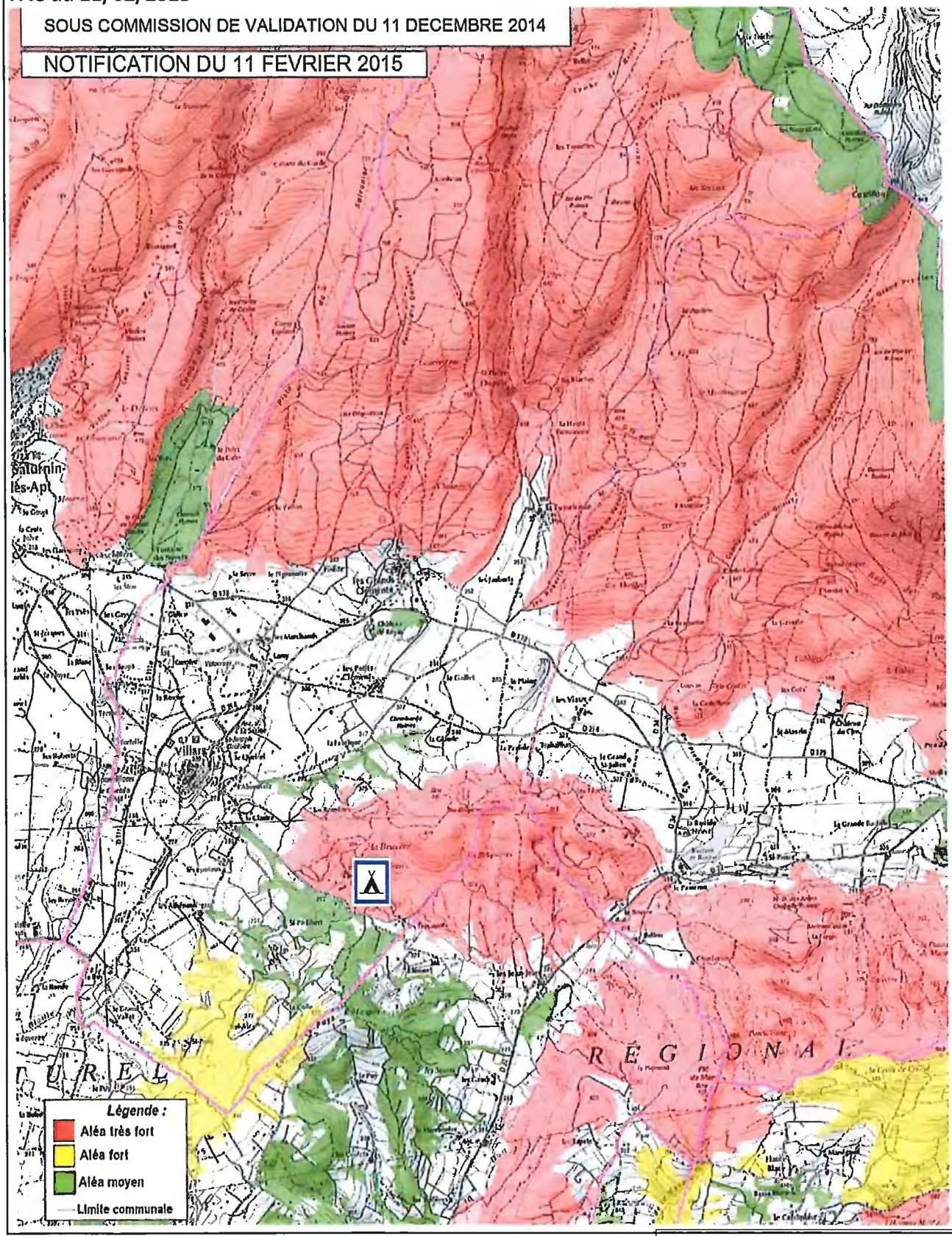
Détaillez comment le risque impacte le camping :
Camping situé dans un vallon à proximité de la voie communale des Trécassats.
Les boisements linéaires situés au Sud et au Nord du terrain peuvent constituer des mèches propageant l'incendie vers le versant de la Bruyère, ce qui pourrait générer un feu de très grande ampleur et difficilement traitable". Aucun matériel ou équipements sensibles stockés sur place.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

Cartes correspondantes (PPRIF, carte communale, PAC...) :

Carte de localisation du camping soumis à risque feu de forêt :

PAC du 11/02/2015



Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

Connaissances sur le risque :

Moyens à utiliser pour s'informer sur le niveau de risque :

Ci-dessous lien qui renvoie sur le site internet qui communique les informations journalières pour la fréquentation des massifs forestiers ou borne d'information téléphonique : 04 28 31 77 11.
www.risque-prevention-incendie.fr/vaucluse/

Procédure mise en œuvre au sein de la mairie (qui est en charge à la mairie du recueil de cette information, qui le remplace en cas d'absence, les suites données…) :

En semaine et le week-end, Mr le Maire reçoit l'information de la Préfecture ou du propriétaire et, donne l'alerte par téléphone et un élu municipal se rend immédiatement sur place (le lundi/mardi/jeudi/vendredi toute la journée et mercredi matin de 8h à 12h un agent communal se rend sur place) ; les suppléants les remplacent en cas d'absence.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

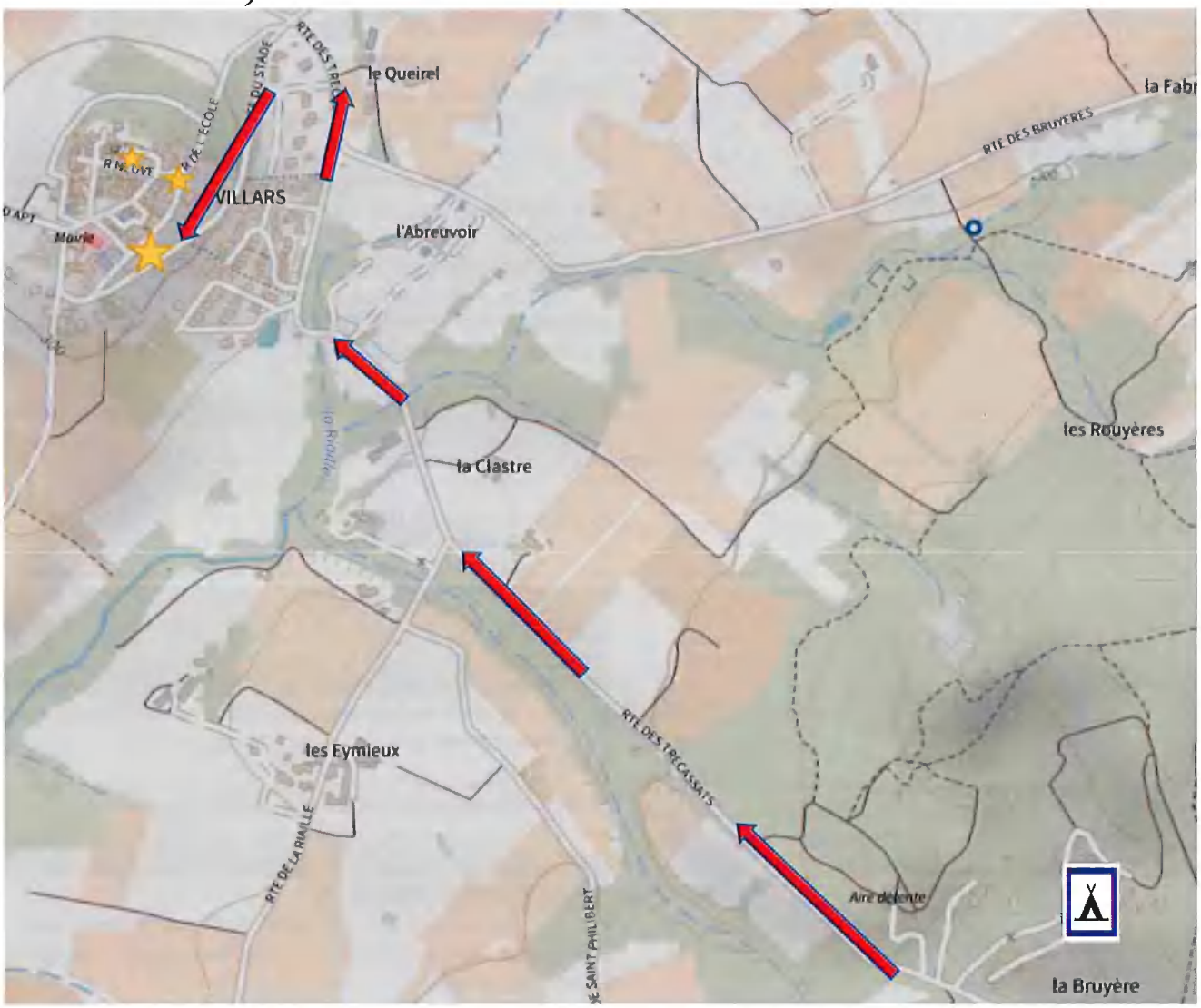
Niveaux de Vigilance		
Quand ?	**Phases**	**Quoi ?**
Niveau de vigilance sur les massifs forestiers		**Définir les différentes actions et les moyens à mettre en œuvre lors du passage des niveaux de vigilance.** **Les actions prédéfinies ci-dessous le sont à titre d'exemple et doivent être adaptées et complétées en fonction de ce qui sera mis en œuvre par la commune.**
Risque très sévère sur les massifs forestiers du sud du département (Accès aux massifs limité)	**VIGILANCE**	· Suivre le niveau de danger sur : (www.risque-prevention-incendie.fr/vaucluse/) ou borne téléphonique 04 28 31 77 11 • Informer par un appel téléphonique le camping de l'accès limité aux massifs · **Le gestionnaire du camping accuse réception de la vigilance faite par téléphone ou en présentiel** en cas de coupure des lignes téléphoniques : *- réponse à l'appel téléphonique ou en personne* • Le maire doit demander au gestionnaire de mettre en œuvre les mesures prévues dans la phase de pré-alerte du cahier de prescriptions de sécurité. • Suivre le niveau de danger : *- suivi de l'alerte par l'un des deux gestionnaires présent sur place serveur de suivi du SDIS : 18 ou 112*
Risque Extrême sur les massifs forestiers du département (Fermeture des massifs forestiers)	**VIGILANCE RENFORCEE**	· Suivre le niveau de danger sur : (www.risque-prevention-incendie.fr/vaucluse/) ou borne téléphonique 04 28 31 77 11 • Prendre contact avec le SDIS • Informer le camping de la fermeture des massifs forestiers : *- information par un appel téléphonique ou en personne* *Mr le Maire alerte par téléphone et/ou un élu municipal se rend immédiatement sur place (le lundi/mardi/jeudi/vendredi toute la journée et mercredi matin de 8h à 12h un agent communal se rend sur place).* • Le maire doit demander au gestionnaire de mettre en œuvre les mesures prévues dans la phase d'alerte du cahier de prescriptions de sécurité · Mobiliser les élus pour une sensibilisation accrue des campeurs · S'assurer de la disponibilité du lieu d'hébergement : Salle des Fêtes capacité d'accueil 135 personnes, chaises et tables **(voir fiche hébergement d'urgence p.47).** • Obtenir de l'exploitant le recensement des campeurs (notamment les personnes non véhiculées, personnes âgées, les PMR, groupe de mineurs…) • S'assurer de l'accessibilité des voies d'accès au camping : moyen humain de la cellule terrain du PCS.
Départ de feu	**ÉVACUATION**	• Être et rester en contact avec le SDIS • Le maire donne l'ordre d'évacuer et de mettre en œuvre les mesures prévues dans la phase d'évacuation du cahier de prescriptions · Évacuation des campeurs suivant les axes routiers préalablement définis pour rejoindre le lieu d'hébergements accompagnés d'un élu ou agent communal : route des Trécassats puis en agglomération route du Stade. · Organiser l'accueil des campeurs au sein du lieu d'hébergements (renvoi à la fiche « accueil des populations » page 46).

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

Itinéraire pour rejoindre le lieu d'hébergement sur la commune

Itinéraire via la route des Trécassats puis la route du Stade à emprunter pour rejoindre le lieu d'hébergement « Salle des Fêtes » 161 Route du Stade 84400 Villars et coordonnées GPS du lieu d'hébergement :

43.922839, 5.405856



Les campeurs évacuent accompagnés de l'élu ou agent communal rendu sur place.

Les autres lieux d'hébergement (annexe n°5 page 55) : départ après enregistrement des personnes, 8 place de la Mairie et accompagnement des groupes constitués par le PCC vers les autres sites : Chapelle St Roch et Auberge du Villarsois.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

FICHE ACTION N° 7 : Actions à mener

PRÉ-CRISE

- Installer une cellule de veille.
- Faire des points réguliers sur l'évolution de la situation (météo France, Vigicrues…).
- Mettre en pré-alerte la population : avertir et tenir la population informée de l'évolution de la situation.
- Rappeler à la population les consignes de sécurité selon le risque attendu.
- Anticiper les actions qui sont définies dans le PCS (pré-positionner les barrières de sécurité, pré-alerter les personnes ressources…).
- …

LA CRISE

- Déclencher la cellule de crise.
- Alerter la population (Voir fiche Alerte des populations p.49).
- Évacuation des populations si l'eau atteint une hauteur d'eau de___ et/ou un débit de____.
- Porter une attention particulière aux personnes vulnérables (annexe n°4 p.54) et enjeux sensibles (annexe n°3 p.54).
- Fermeture des axes routiers impactés par l'évènement (indiquer le nom de l'axe et l'endroit où il devra être coupé).
- Surveiller la formation d'embâcle.
- Ouverture du centre d'accueil des personnes.
- …

POST-CRISE

- Gérer les volontaires.
- Assurer le soutien des sinistrés.
- Coordonner les opérations de retour à la normale.
- Prévoir des bennes pour stocker les déchets.
- …

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

FICHE ACTION N° 8 : Organiser une évacuation

L'action se déroule sous l'autorité du maire (ou de son représentant).

- Définir les zones sinistrées et/ou à évacuer (cartographies page 7 et 13).

- Alerter la population de l'ordre d'évacuation (Voir fiche Alerte des populations p.49) et indiquer les zones refuges : lieu d'hébergement « Salle des Fêtes – Chapelle St Roch - Auberge du Villarsois » et coordonnées GPS du lieu d'hébergement : 43.922839, 5.405856.
- Estimation des moyens humains et matériels à engager : les cellules « logistique » et « terrain » devront se coordonner pour cette action.
- Fermeture des routes, bouclage de la zone en coordination avec la police municipale ou la gendarmerie.

- Évacuation de la population
  - La cellule terrain aura pour rôle de vérifier que toutes les personnes ont bien quitté leurs habitations et en particulier les personnes vulnérables recensées dans le PCS.

Elle fera remonter les informations concernant les personnes évacuées et des personnes refusant d'évacuer au PCC qui devra les transmettre aux services de pompier et/ou de gendarmerie.

Attention les personnes en charge d'alerter et d'aider à l'évacuation des personnes sur le terrain ne doivent pas s'aventurer en zone de danger (ne pas créer de sur-accident). Seuls les services de secours formés pour ce type d'intervention sont habilités à entreprendre des actions en zone où le risque est présent.

- Après l'évacuation surveiller la zone évacuée pour lutter contre les pillages et éviter que des personnes veuillent (re)gagner leur domicile.

<u>Déclencher une évacuation implique d'ouvrir un lieu d'hébergement pour les personnes évacuées (cf voir fiche action « Hébergement d'urgence » page 47)</u>

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

FICHE ACTION N° 9 : Hébergement d'urgence

- Prendre la liste des centres d'hébergement (annexe n°5 p 55), ouvrir le ou les centre(s) le(s) plus pertinent(s) en fonction de la crise et du nombre de personnes à reloger. Vérifier que les centres ne se situent pas en zone de risque si la crise devait prendre de l'ampleur.

- Diffuser l'information à la population qu'un d'hébergement est ouvert.

- Organiser l'accueil des populations
  - Aménager la salle (dans la mesure du possible) avec une zone consacrée au recensement des personnes et de diffusion de l'information, une zone de repos, une zone ravitaillement et une zone infirmerie/prise en charge des personnes.

  - Les personnes prises en charge devront être enregistrées sur un registre (Nom, prénom, âge…) pour assurer le suivi et connaître le nombre de personne prise en charge par la commune.

- La cellule logistique devra réfléchir comment se procurer la nourriture et le matériel nécessaire (annexe n°6, n°8 et 9 pages 55) pour accueillir la population (lits picots, lits pour enfants, couvertures, chaises…)

Pour équiper votre centre d'hébergement vous pouvez faire appel à des associations de sécurité civile (type : croix rouge, protection civile). Des conventions peuvent être passées avec ces associations pour lors de la crise.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

FICHE ACTION N° 10 : Remontée d'information et coordination avec le Centre Opérationnel Départemental

Dès que le maire décide de mettre en œuvre le PCS, il doit en informer immédiatement le Préfet et le COD (si activé) ainsi que le SDIS et la gendarmerie (CF annexe n°2 p.50)

Rôle du COD : le Centre Opérationnel Départemental est activé en situation de crise majeure dépassant les limites d'une commune, le Préfet ou son représentant prend alors la Direction des Opérations de Secours. Il est composé par l'ensemble des services de l'État et des acteurs de la sécurité civile. Il permet de :

- suivre et produire une analyse de la situation
- assurer une expertise
- coordonner l'action des services
- anticiper l'évolution de la situation
- organiser la communication autour de l'évènement

- Vous devrez rendre compte au Préfet et au COD : selon un format « je suis, je vois, je fais, je demande »
  - Par le standard de la préfecture : 04 88 17 84 84
  - Lorsque le COD est activé par le numéro de secrétariat COD :04 88 17 80 70 et/ou par messagerie : pref-cod-crise@vaucluse.gouv.fr

- Vous devrez tenir informé le préfet et le COD de l'évolution de la situation en faisant remonter les informations de manière régulière
  - *quelle est la situation initiale ?*
  - *quel est le bilan ?*
  - *quelles sont les actions en cours ?*
  - *quelles sont les situations envisageables à court et moyen terme ?*
  - *quelles sont les actions complémentaires à proposer ?*

- Il est important que ces échanges entre le Poste de Commandement Communal et le Centre Opérationnel Départemental soient réguliers. Ils permettront au niveau de la commune :
  - De faire remonter rapidement les difficultés rencontrées et les demandes auprès du COD et de ses services.
  - De faire rapidement remonter les éléments du terrain au COD, pour permettre aux acteurs présents d'avoir une vision précise de la situation.
  - D'être rapidement au courant des décisions/actions prises au niveau départemental.
  - D'avoir des points précis sur l'évolution globale de la situation.

Mission du Maire : Même dans le cas où le Préfet prend la direction des opérations de secours, le maire a toujours pour mission de mettre en œuvre, sur le territoire de sa commune, les mesures de sauvegardes qui s'imposent (art L 2212-2 du CGCT), parmi lesquelles :

- L'alerte des populations
- L'évacuation et l'hébergement de personnes déplacées
- Le soutien matériel et le ravitaillement des populations
- L'appui aux services de secours

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

II.3. L'alerte des populations

Il convient d'alerter le plus rapidement possible la population du danger qui menace la commune.

Qui fait l'alerte ? Selon le système d'alerte choisi, plusieurs personnes peuvent être amenées à faire l'alerte (dans le cas du porte-à-porte par exemple).	
Aux heures et jours ouvrables	M. SAMPIETRO Thomas, Maire Secrétariat de la mairie Lundi/Mardi/Jeudi/Vendredi de 9h à 12h
Hors heures et jours ouvrables	M. SAMPIETRO Thomas, Maire Mme BALAZUN Corinne, 1ère adjointe Mr LEROYER Hugues, 2ème adjoint Mme JEAN Marlène, 3ème adjointe Mr MUSSO Tristan, 4ème adjoint Mme DE KERVILER Christine, conseillère déléguée

Quand alerter ?
L'alerte doit être déclenchée lorsque le danger est avéré et imminent.
C'est le Maire qui prend la décision d'alerter ou non en fonction des éléments qu'il a à sa disposition pour évaluer la situation.

Qui alerter ? Préciser les cibles de diffusion avec hiérarchisation des cibles prioritaires en fonction du risque considéré (établir un annuaire des personnes à alerter en fonction du risque qui les concerne).
La population entière doit être alertée, si la menace concerne l'ensemble du territoire communal.
Des listes par risque des personnes à alerter peuvent être mises en place, ces listes sont pertinentes si le nombre de personne est peu élevé (sinon une alerte globale est plus pertinente). Elle permettra d'alerter en priorité les personnes les plus exposées. (Exemple :Ce type d'alerte peut être utilisé pour les habitations isolées en zone feux de forêts.)
Pouvoir identifier les personnes vulnérables en temps de crise est essentiel (pour pouvoir les indiquer aux services de secours, pour les aider lors d'évacuation ou les contacter lors de coupures de réseaux ou d'isolement prolongé). Pour cela les communes peuvent s'appuyer sur le registre nominatif des personnes âgées et des personnes handicapées (article L121-6-1 du code de l'action sociale et des familles). Ce registre n'est pas à intégrer dans le PCS par contre son emplacement et les noms et numéros de téléphone **portable** des personnes habilitées à le consulter doivent y figurer (Annexe n°4).

Comment alerter ? Indiquer les moyens d'alerte existant et pouvant être mis en œuvre dans votre commune en cas de crise.		
Diffusion d'un signal sonore	- *Cloches* - *Klaxon continu d'un véhicule*	Eglise non loin du PCC
Diffusion d'un message d'alerte	- *Téléphone* - *Porte-à-porte*	Téléphoner à l'ensemble de la population concernée. Faire du porte à porte par les membres du conseil municipal et tous volontaires.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

ANNEXES OPÉRATIONNELLES

ANNEXE N° 1 : Points de rassemblement de la population

Lieu de rassemblement	Adresse	Accès
Place de la Fontaine	Place de la Fontaine 84400 VILLARS	Route du Stade ou route d'Apt
Salle des Fêtes	161 Route du Stade 84400 VILLARS	Route du Stade

ANNEXE N° 2 : Annuaires

- **Numéros d'urgence**

Service d'urgence	Téléphone
Sapeurs-Pompiers	18 ou 112
SAMU	15 ou 112
Police/Gendarmerie	17
SOS Médecin	04 90 82 65 00
Sans-Abri	115
Centre antipoison de Marseille	04 91 75 25 25
Association de Sécurité Civile	06 25 11 28 48
Numéro d'astreinte de la commune	06 83 15 32 73
Etc.	

- **Annuaire des membres du Poste de Commandement Communal (PCC)**

*** Responsable du PCC (DOS et RAC)**

Prénom - NOM	Tél. domicile	Tél. portable	Fonction dans la commune
SAMPIETRO Thomas		06 59 35 28 67	DOS- Maire
SUPPLÉANT			
SAUTEL Benoit		06 71 40 92 30	Conseiller municipal

BALAZUN Corinne		06 42 15 70 37	RAC – 1ère adjointe
SUPPLÉANTE			
JEAN Marlène		07 77 39 65 37	3ème adjointe

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

*** Cellule Secrétariat/Communication**

Prénom - NOM	Tél. domicile	Tél. portable	Fonction dans la commune
RESPONSABLE			
DE KERVILER Christine		06 88 49 23 28	Conseillère déléguée
SUPPLÉANTE			
JULIEN Sarah		06 17 39 05 23	Conseillère municipale
PERSONNELS			
VANEL Magali		06 02 39 77 99	Conseillère municipale
MENSE Marilyne		06 86 65 12 28	Conseillère municipale

*** Cellule Terrain**

Prénom - NOM	Tél. domicile	Tél. portable	Fonction dans la commune
RESPONSABLE			
LEROYER Hugues		06 71 75 22 97	2ème Adjoint
SUPPLÉANT			
REMICHE Nicolas		06 77 21 84 91	Conseiller municipal
PERSONNELS			
CELIE Thomas		06 05 97 79 37	Conseiller municipal
BONAMY Déborah		06 74 91 50 22	Conseillère municipale

*** Cellule Logistique**

Prénom - NOM	Tél. domicile	Tél. portable	Fonction dans la commune
RESPONSABLE			
MUSSO Tristan		06 13 53 02 75	4ème adjoint
SUPPLÉANT			
NICOLE Romain		06 20 28 00 51	Conseiller municipal
PERSONNEL			
FERRIER Lionel		06 26 54 55 10	Conseiller municipal

- **Annuaire des services et employés municipaux**

Service municipal	Chef du service	Tél. domicile	Tél. portable
SILVA Emeline	Mr le Maire		04 90 75 40 01
BERTRAND Aurélie	Mr le Maire		04 90 75 40 01
BOURGUE Alex	Mr le Maire		06 89 26 05 94
NOCCIOLETTI Christophe	Mr le Maire		06 89 26 05 94

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

• Annuaire des collectivités locales, des services de l'État et des grands opérateurs

* Service de l'État

Service de l'État	Téléphone
Préfecture de Vaucluse	04 88 17 84 84
Direction Départementale des Territoires	04 90 80 85 02/03
Direction Départementale de la Protection des Populations	04 88 17 88 00
Direction Départementale de l'emploi du travail et des solidarités	04 88 17 84 84
Délégation Départementale de l'Agence Régionale de Santé	04 13 55 85 50
Unité Territoriale de la DREAL	04 88 17 89 02

* Collectivités locales

Collectivité	Téléphone
Conseil Régional PACA	04 91 57 50 57
Conseil Départemental de Vaucluse	04 90 16 15 00
Communauté de Communes Pays d'Apt Luberon	04 90 04 49 70
Mairie de Saint-Saturnin-lès-Apt	04 90 75 43 12
Mairie d'Apt	04 90 74 00 34
Mairie de Rustrel	04 90 04 91 09
Mairie de Lagarde d'Apt	04 90 75 00 93

* Grands opérateurs

Opérateurs	Téléphone
ENEDIS/GRDF	0811 01 02 12
Service des eaux SUEZ	09 77 40 11 36
Orange	1015/0800 083 083
Autres	

• Annuaire des professionnels de santé

* Hôpitaux et cliniques

NOM	Adresse	Téléphone	Télécopie
Hôpital d'Apt	225 avenue de Marseille 84405 APT	04 90 04 33 00	

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

* Médecins généralistes et spécialistes

Prénom - NOM	Adresse	Téléphone	Télécopie
Centre Médical Les Druides	172 Bd National 84400 APT	04 90 74 17 95	
Maison Médicale	225 avenue de Marseille 84405 APT	04 90 04 33 00	

* Infirmiers

Prénom - NOM	Adresse	Téléphone	Télécopie
Centre Médical Les Druides	172 Bd National 84400 APT	04 90 74 17 95	
DROUIN Thibaut Cabinet Infirmier	Maison médicale 54 Ch. St Roch 84490 Saint-Saturnin-lès-Apt	06 62 30 71 17	

* Pharmacies

Prénom - NOM	Adresse	Téléphone	Télécopie
Pharmacie du Chateau	465 Avenue des Cordiers 84400 GARGAS	04 90 04 89 04	
Pharmacie Collard Et Bellot	Av. Jean Geoffroy 84490 Saint-Saturnin-lès-Apt	04 90 75 41 79	
Pharmacie du Pays d'Apt	308 Avenue de la Libération 84400 APT	04 90 04 75 92	
Pharmacie des Ocres	657 Avenue Victor Hugo 84400 APT	04 90 74 20 57	
Pharmacie St Michel	21 Av. Jean Moulin, 84400 Apt	04 90 74 17 55	
Pharmacie Cathédrale	146 Rue des Marchands, 84400 Apt	04 90 74 02 53	
Pharmacie Angot	72 Rue des Marchands, 84400 Apt	04 90 74 01 39	

* Ambulances

Prénom - NOM	Adresse	Téléphone	Télécopie
Ambulances Mistral	Rue des Bourguignons 84400 APT	04 90 04 70 70	
Ambulances Cantarelli	375 Avenue Victor Hugo 84400 APT	04 90 04 75 37	

* Laboratoires d'analyses médicales

Prénom - NOM	Adresse	Téléphone	Télécopie
BIOAXIOME	39 quai Léon Sagy 84400 APT	04 90 74 17 57	
SYNLAB	82 avenue Victor Hugo 84400 APT	04 90 71 66 66	

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

ANNEXE N° 3 : Enjeux sensibles sur la commune

***Hôtel, restaurant, campings**

NOM et Type	Adresse	Capacités d'accueil	Téléphone
Camping La Colline des Ocres	1649 Route des Trecassats 84400 Villars	23 chalets	04 90 75 44 58 06 14 84 25 42
Restaurant La Fontaine	14 Place de la Fontaine 84400 Villars	Restauration 10 personnes	04 90 75 48 55
Bar les Amis	34 Place de la Fontaine 84400 Villars	Restauration 20 personnes 8 couchages	04 90 75 01 77
École de Villars	1a Rue de l'école 84400 Villars	112 personnes	04 90 75 40 55

***Entreprises, commerces**

NOM et Type	Adresse	Nombre de personnes (max)	Téléphone	Observations

***Autres (médiathèque, gymnase...)**

NOM et Type	Adresse	Effectif moyen	Téléphone	Observations

ANNEXE N° 4 : Personnes vulnérables

Le registre nominatif des personnes âgées et des personnes handicapées est classé en mairie, il est consultable par :

M. le Maire Thomas SAMPIETRO, numéro de téléphone 06 59 35 28 67

Prénom - NOM	Adresse	Téléphone	Observations
LEGIER Roger	3013 route de Rustrel 84400 VILLARS	06 75 26 31 54	Personne à contacter : BEDOC Martine 06 89 23 00 35
PEZIERE Serge	20 rue des Aires Les Grands Cléments 84400 VILLARS	04 90 75 55 54 06 80 32 68 70	Personne à contacter : PEZIERE Claire 04 90 75 99 18 06 79 73 51 87

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

ANNEXE N° 5 : Moyens d'hébergement et d'accueil

NOM	Adresse	Capacités d'accueil	Téléphone	Sanitaires	Cuisine
Salle des Fêtes	161 Route du Stade 84400 Villars	120 personnes assises		oui	oui
Chapelle St Roch	60 Rue du Collet 84400 Villars	21 personnes		oui	non
Auberge du Villarsois	Rue Neuve 84400 Villars	100 personnes		oui	oui

ANNEXE N° 6 : Restauration

NOM	Adresse	Téléphone
Restaurant La Fontaine	14 Place de la Fontaine 84400 Villars	04 90 75 48 55
Bar les Amis	34 Place de la Fontaine 84400 Villars	04 90 75 01 77
Boulangerie	13 Rue des Roux 84400 Villars	04 90 75 43 05
Hypermarché, supermarché, épicerie		
Etc.		

ANNEXE N° 7 : Moyens de transport collectif

Entreprise de transport	Adresse	Téléphone
Maison de la Région de Vaucluse	135 avenue Pierre SEMARD MIN Avignon Bât D4 84000 AVIGNON	04 90 14 40 60

ANNEXE N° 8 : Moyens matériels publics communaux

DÉSIGNATION	Quantité	Adresse
Petit matériel (balai, seau, brouette, etc.)	4 BALAIS, 3 PELLES	Mairie, Salle des fêtes et Hangar Communal
Clocher d'église	Sonner le tocsin	10a Place de la Mairie 84400 Villars
Thermique : une tronçonneuse, un élagueur, une souffleuse Sur batterie : une tronçonneuse, une souffleuse Un groupe électrogène		
Véhicules	1 véhicule utilitaire type plateau benne 1 véhicule utilitaire type porteur de déchets végétaux	
Etc.		Salle des Fêtes / Auberge du Villarsois

ANNEXE N° 9 : Moyens matériels privés

- **Entreprises de Bâtiments et Travaux Publics**

NOM	Adresse	Téléphone	Télécopie

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

- **Entreprises de manutention et de levage**

NOM	Adresse	Téléphone	Télécopie

- **Autres entreprises**

NOM	Type d'activité	Adresse	Téléphone	Matériel
ISNARD Laurent	Scierie la Bernadette	160b chemin de la Carrière 84400 VILLARS	07 72 30 79 51	Tracteur

ANNEXE N° 10 : Moyens matériels des associations se trouvant sur le territoire communal

NOM	Adresse	Téléphone	Télécopie

DÉSIGNATION	Quantité	Adresse
Petit matériel (balai, seau, brouette, etc.)		
Matériel d'hébergement		
Matériel d'alimentation		
Matériel de communication		
Véhicules		
Etc.		

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

ANNEXE N° 11 : Procédures de vigilance

➢ Vigilance météorologique

Depuis octobre 2001, la carte de vigilance vous informe si un danger météorologique peut toucher le département dans les 24 heures à venir.

Une couleur est attribuée : vert , jaune, orange ou rouge à chaque département métropolitain, selon les dangers potentiels associés aux conditions météorologiques prévues. Si la carte de vigilance comporte au moins une zone orange ou rouge, un bulletin régional de suivi de phénomène exceptionnel consultable par tous est émis par Météo France (évolution, intensité...).

En vigilance orange ou rouge, un pictogramme précise sur la carte le type de phénomène météorologique attendu : vent violent, vagues-submersion, pluie-inondation, inondation, orages, neige/verglas, avalanches, canicule, grand froid.

Selon le niveau de vigilance, le préfet exerce sa mission d'information et d'alerte auprès des maires et les avertit au moyen d'un appel téléphonique via le serveur d'alerte de la préfecture.

La carte de vigilance est élaborée 2 fois par jour par Météo-France, pour une diffusion à 6 heures et à 16 heures. Des actualisations intermédiaires sont effectuées chaque fois que la situation le requiert.

La carte de vigilance est consultable en permanence par tous sur le site internet de Météo France : www.vigilance.meteofrance.com

➢ Vigilance crues

La vigilance crues est destinée à informer de l'existence d'un risque de crue, plus ou moins important, traduit par une couleur, vert , jaune, orange ou rouge, affectée à un ou des tronçon(s) de cours d'eau surveillés par l'État, selon le niveau de vigilance nécessaire.

A l'échelle locale, la carte de vigilance crues détaille les stations d'observation qui servent à la surveillance. Par un clic sur une station, il est possible d'avoir accès à des données en temps réel (hauteur et débit).

Dès lors qu'au moins un tronçon sur le territoire concerné atteint un niveau de vigilance jaune, orange ou rouge, la carte est accompagnée d'un bulletin d'information.

Les informations relatives aux crues sont actualisées tous les jours à 10 h et à 16 h. Toutefois, en période de crues ou en cas de changement notable, les cartes et bulletins sont réactualisés plus fréquemment et à tout moment.

Ces éléments, sont disponibles 24h/24h sur le site internet :
www.vigicrues.gouv.fr

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

ANNEXE N° 12 : Préparation d'un exercice communal

La réalisation d'exercices de simulation représente le meilleur moyen de tester les procédures mises en place pour faire face à différents types de sinistres.

I. OBJECTIFS GENERAUX D'UN EXERCICE DE CRISE

Un exercice de crise nécessite avant toute chose une très forte implication des autorités concernées et de la direction de tous les services impliqués. Il doit être pensé dans une démarche de recherche d'efficacité et surtout ne pas céder à la complaisance.

Globalement un exercice de crise devra permettre d'atteindre tout ou partie des objectifs suivants :

- Mettre en œuvre et tester les différents éléments étudiés dans un plan,
- Exercer les responsables à la gestion de crise,
- Vérifier la disponibilité et la bonne utilisation des moyens techniques,
- Évaluer les moyens de communication.

II. PLANIFICATION ET DEROULEMENT D'UN EXERCICE

II.1. La phase de préparation :

Elle débute dès la prise de décision d'engager une simulation. Il s'agit alors de constituer une équipe de projet qui aura pour mission de mener l'exercice à son terme et de respecter les principaux objectifs assignés.

Éléments essentiels

- Définir clairement les objectifs poursuivis,
- Choisir et expliciter le scénario de l'exercice,
- Composer une équipe de projet impliquant les différents responsables intervenants,
- Définir précisément les points et critères d'évaluation de l'exercice.

II.2. La phase de réalisation

Cette étape est de loin la plus stratégique car elle va déterminer le niveau de réussite du projet. Tout doit être prêt le jour J afin de garantir le maximum d'efficacité à la simulation et d'éliminer tout élément qui pourrait fausser le déroulement du scénario et l'analyse post-exercice qui sera entreprise.

II.3. La phase d'évaluation

Cette étape boucle le cycle de l'exercice. Elle est divisée en deux temps :

- L'analyse : évalue les résultats et le niveau d'atteinte des objectifs de l'exercice,
- Le retour d'expérience : tire les principales conclusions de l'exercice et détermine les actions à entreprendre pour améliorer les processus opérationnels.

Principaux éléments d'évaluation

Selon la portée de l'exercice réalisé, l'évaluation devra prioritairement mesurer :

- Le niveau de mobilisation et l'organisation du dispositif de crise,
- La conduite générale de la crise au niveau de tous les acteurs impliqués,
- La maîtrise des communications,
- La résultante réelle face au sinistre considéré.

Retour d'expérience

Il devra expliciter précisément les orientations qui devront être prises, si nécessaire pour améliorer le dispositif pré-établi :

- La modification du plan de crise et/ou des plans d'intervention,
- L'achat de matériels complémentaires,
- Les perspectives et priorités d'apprentissage des acteurs.

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

ANNEXE N° 13 : la canicule

1. Canicule : critères d'alerte

Du 1er juin au 15 septembre, la procédure de vigilance et de mobilisation saisonnière intègre :

- l'expertise du Système d'Alerte Canicule Santé (SACS) intégrant le suivi des indicateurs bio-météorologiques (IBM) et l'analyse météorologique de Météo-France,
- le suivi et l'analyse des indicateurs sanitaires par l'Institut de veille sanitaire (INVS).

Ainsi, le dispositif de veille bio-météorologique est assuré par Météo-France et par l'Institut de veille sanitaire (INVS), en lien avec la direction générale de la santé (DGS), afin de détecter au mieux la survenue d'une éventuelle canicule.

En Vaucluse, des seuils de température de 36° le jour et 21° (IBM) la nuit atteints et perdurant pendant 72 heures (3 jours) sont le critère de base de prévision d'une canicule.

LES DIFFÉRENTS NIVEAUX DU PLAN CANICULE S'ARTICULENT AVEC LES QUATRE COULEURS DE VIGILANCE MÉTÉOROLOGIQUE.

2. Les 4 niveaux du plan « Canicule »

- niveau 1 : **VEILLE SAISONNIÈRE – Niveau de vigilance météorologique VERT** – du 1er juin au 15 septembre, avec activation du dispositif d'information et de communication assuré par le numéro vert national 0 800 06 66 66 (appel gratuit depuis un poste fixe) de 9h à 19h ;
- niveau 2 : **AVERTISSEMENT CHALEUR – Niveau de vigilance météorologique JAUNE** – correspond soit à un pic de chaleur limité à un jour ou deux, soit à une approche des seuils de température qualifiant la canicule (IBM) avec éventuellement des prévisions d'intensification de la chaleur les jours suivants ;
- niveau 3 : **ALERTE CANICULE** (ancien niveau MIGA) – **Niveau de vigilance météorologique ORANGE** – niveau activé sur décision du préfet de département qui met en place, en fonction des circonstances, les mesures adaptées ;
- niveau 4 : **MOBILISATION MAXIMALE – Niveau de vigilance météorologique ROUGE** – niveau déclenché au niveau national sur instruction du Premier Ministre, dès lors que de fortes températures s'inscrivent dans la durée et que d'autres phénomènes aggravants et dépassant le champ sanitaire sont observés (hausse de la mortalité, pollutions, ruptures de réseaux, pénurie d'eau potable, saturation des établissements de santé...).

Le niveau 3 est du ressort départemental. Son activation par le préfet vise à mobiliser les services départementaux concernés et les maires, ainsi qu'à informer le public.

Les seuils de température et les niveaux de vigilance n'ont qu'une valeur indicative ; ils servent de référence pour aider à la décision. D'autres critères qualitatifs (facteurs météorologiques aggravants, pollution atmosphérique, critères sociaux...) sont également considérés pour apprécier la situation dans le département et contribuer à la décision d'activer le niveau « alerte canicule ».

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

ANNEXE N° 14 : Modèle d'arrêté de réquisition

Le maire de la commune de….

Vu la code général des collectivités territoriales et notamment son article L.2212-2,

Considérant :(l'évènement)……...…… ;……..……
……...……survenu le……..…...à……. heures.

Considérant qu'il est nécessaire de doter la commune des moyens nécessaires pour répondre à ses obligations.

Vu l'urgence : (à expliciter le plus possible)……

Arrête :

Article 1er : L'entreprise…….est réquisitionnée avec les moyens en personne et en matériel dont elle dispose en vue effectuer la mission (préciser la nature, le lieu de la prestation…) nécessaire au rétablissement de l'ordre public.

Article 2 : préciser toute indication utile à la bonne exécution de la réquisition et en particulier les nom, prénoms, qualité et fonction de l'autorité habilitée à constater le service fait.

Article 3 : La réquisition est exécutoire dès réception du présent ordre et jusqu'au …… / pour (X heures, voire jours.)

Article 4 : [le requis] sera indemnisé dans la limite de la compensation des frais directs, matériels et certains résultant de l'application du présent arrêté, ou en fonction du prix commercial normal et licite de la prestation, sans considération de profit, lorsque la prestation requise est de même nature que celles habituellement fournies par l'entreprise à la clientèle, conformément aux conditions prévues par l'article L.2215-1 du code général des collectivités territoriales.
Dans les conditions prévues au code de justice administrative, le tribunal administratif pourra accorder au requis, à sa demande, une provision couvrant tout ou partie de l'indemnité à venir.

Article 5 : A défaut d'exécution du présent ordre de réquisition, il pourra être procédé à son exécution d'office. La personne requise s'expose aux sanctions pénales ou administratives prévues à l'article L.2215-1 4° du code général des collectivités territoriales.

Article 6 : le présent arrêté peut faire l'objet d'un recours gracieux auprès du maire dans les deux mois suivant sa notification.
Il peut également faire l'objet d'un recours contentieux, auprès du tribunal administratif, dans le même délai, ou le cas échéant, dans les deux mois suivant le rejet du recours gracieux.
Article 7 : Le présent ordre de réquisition sera notifié à M.[requis]. Son ampliation sera affichée à…… et transmise à M. le Préfet.

Article 8 (exécution) : Le commissaire de police ou le commandant de la brigade de gendarmerie est chargé de l'exécution du présent arrêté.

Fait à…….. le … /…/….

Le maire,

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

ANNEXE N° 15 : Main courante

DATE	HEURE	ORIGINE	DESTINATAIRE	DESCRIPTIF DE L'EVENEMENT	ACTIONS DEMANDÉES AUX SERVICES	ACTIONS RÉALISÉES

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026

Accusé de réception en préfecture
084-218401453-20261006-2026ARD070-AR
Date de réception préfecture : 08/10/2026