**Les guides** de bonnes pratiques SMACL

**Les responsables des collectivités face au**

# > Risque Malveillance dans les bâtiments publics

"Partageons nos expériences pour prévenir nos risques"

APVF PETITES VILLES de France

Smacl
Assure ma ville, assure ma vie

# > Risque Malveillance dans les bâtiments publics

"Partageons nos expériences pour prévenir nos risques"

## Sommaire




**Les guides de bonnes pratiques SMACL** :
SMACL Assurances - 141 avenue Salvador Allende – 79000 Niort – 05.49.32.23.13 - Directeur de la publication : Michel Paves, Président du Conseil de Surveillance de SMACL Assurances – Directrice de la rédaction : Martine Martin - Rédacteur en chef : Jean-François Irastorza - Ont collaboré à ce numéro : André Robert (APVF), David Croizet, Patrice Daverat, Valérie Thirez (SMACL Assurances) – Conception, rédaction & Mise en page : Vibrato - Réalisation : SMACL Entraide, communication institutionnelle - Crédits photos : Cit'images (p.4, p.13) ; Fotolia (couverture, bandeaux têtières, p.2, p.5, p.6, p.8, p.9, p.10, p.11, p.15) ; Ville de Longvic (p.1) - ISBN : en cours d'attribution.

École incendiée, mairie vandalisée, gymnase visité ou squatté... la liste des bâtiments publics visés par des actes de malveillance s'allonge chaque année un peu plus, quelle que soit la taille de la collectivité. L'expérience démontre cependant que les sinistres les plus graves, issus parfois d'une banale effraction, frappent les sites les moins bien protégés.
Pour les rendre moins vulnérables, un large éventail de solutions existe : matériels et dispositifs de protection, de contrôle ou de surveillance... Reste à trouver, avec pragmatisme, la formule adaptée à ses besoins réels, avec le budget d'investissement ou de fonctionnement correspondant.

Dans ce guide, réalisé en partenariat avec l'Association des Petites Villes de France (APVF), SMACL Assurances vous propose un tour d'horizon de différents moyens techniques destinés à gérer au mieux le risque de malveillance, ainsi que quelques indispensables conseils de prévention.

Associé au guide *"Risque Incendie dans les ERP"*, il a pour objectif d'appréhender, par une approche globale et accessible, la problématique de la sûreté de votre patrimoine. Un sujet dont aucune collectivité ne peut aujourd'hui faire l'économie.

# Penser la sûreté **en amont**

*Contrairement au risque Incendie, il n'existe pas à proprement parler de réglementation spécifique concernant le risque Malveillance. Protéger les bâtiments de sa collectivité contre des actes de ce type nécessite donc* ***une étude détaillée*** *pour aboutir à un plan général de sécurité. Le plus en amont possible.*

La mise en sécurité d'un établissement ou d'un site, existant ou à construire, nécessite d'évaluer, au cas par cas, les risques d'intrusion, de vandalisme, d'incendie ou de vol. Une telle démarche doit naturellement prendre en compte les spécificités de chaque site : situation et environnement, moyens humains, flux et horaires

des visiteurs, mobilier et immobilier… On ne protège pas de la même façon un établissement scolaire, un gymnase, un centre technique ou des ateliers, un immeuble de bureaux ou une salle de spectacles… Une analyse détaillée permet de définir clairement les besoins et de déterminer les moyens appropriés.

## >5 objectifs à atteindre

Quels que soient les choix d'équipements ou d'installations opérés par la suite, la sécurisation d'un site devra toujours poursuivre cinq objectifs concomitants :

- dissuader toute personne de commettre un acte malveillant ;
- empêcher toute action de cette personne ;
- détecter une éventuelle intrusion le plus rapidement possible et donner l'alerte aussitôt ;
- retarder l'action malveillante ou la progression de l'intrusion pour permettre une intervention ;
- intervenir au plus tôt pour éviter l'action malveillante, et au plus tard avant son achèvement.

Sachant que le ‘’risque zéro” n'existe pas, il s'agit de faire preuve de cohérence dans la complémentarité des moyens mis en œuvre afin de limiter au maximum les menaces potentielles.

## >Travailler dès la conception

Sans prise de conscience du risque ni volonté d'agir, pas de protection efficace ! Mais l'expérience révèle que la mise en sécurité de bâtiments existants peut générer de fortes contraintes techniques et des efforts financiers importants. C'est pourquoi pour tout bâtiment neuf, mieux vaut travailler cette question dès l'étude des plans et du permis de construire, avec une logique de prévention. S'adjoindre les services d'un assistant maître d'ouvrage compétent se révèle souvent un atout déterminant. Concrètement, partout où l'on pense la sûreté en amont, on observe des gains sensibles pour la collectivité.

### 3 niveaux de protection

La sécurisation d'un bâtiment public peut s'effectuer indépendamment ou simultanément sur 3 niveaux :

**Périphérique :** en limite de propriété (clôtures, portail, espace vert ou jardin…)

**Périmétrique :** sur les limites constructives (fenêtres, portes, murs…)

**Volumétrique :** à l'intérieur (couloirs, pièces, local…)

# Protection mécanique : **élémentaire et indispensable**

## *A l'extérieur d'un bâtiment*

*On regroupe sous l'appellation "protection mécanique" tous les obstacles physiques susceptibles d'empêcher, ou de retarder, à l'extérieur comme à l'intérieur, l'entrée ou la progression d'un indélicat dans un site exposé. Aucun autre dispositif de sécurité ne peut être efficace si des mesures élémentaires de protection mécanique n'ont pas été mises en œuvre !*

### >Des clôtures dissuasives

Tous les accès d'un bâtiment doivent faire l'objet de moyens de défense, prioritairement les accès principaux. Un conseil basique : ne pas hésiter, quand c'est possible, à empêcher l'approche des véhicules à côté des bâtiments…

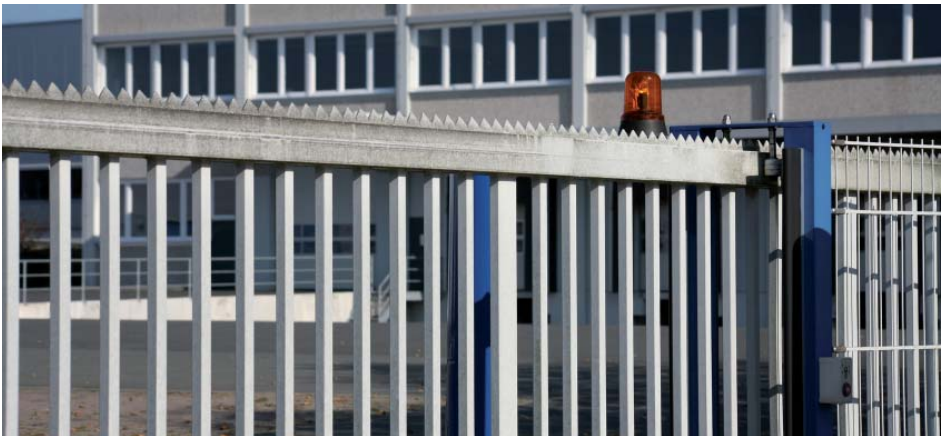
Le choix d'une clôture ou d'un portail, même si l'aspect esthétique et décoratif ne doit pas être oublié, dépend surtout de la nature du site, de son environnement et de sa fréquentation.

Côté clôtures, plusieurs options possibles :

- grillagées, composées de poteaux, fils et grillages en acier doux plastifié et galvanisé ;
- pleines, le plus souvent en dalles de béton ;
- mixtes, avec une dalle pleine en partie basse ;
- à barreaudages (espacement maximum des barreaux : 11 à 12 cm).

Pour renforcer leur caractère dissuasif, la plupart des clôtures intègre ou offre la possibilité d'ajouter des équipements de détection électronique *(voir p.10)*, utiles en cas de chocs ou de sectionnement par exemple. Pour des sites très sensibles, il existe également des barrières "immatérielles" (à infrarouge ou laser…) qui peuvent s'installer au-dessus ou à l'arrière de ces clôtures.

Dans tous les cas, l'installation d'une clôture devra prendre en compte plusieurs critères techniques : la nature du sol, les canalisations, l'alignement…



## >Un portail adapté

L'installation d'un portail (généralement métallique et de préférence avec serrure au point d'accès) peut faire appel à des techniques de plusieurs types :

- pivotant, s'ouvre "à la française" avec un ou deux vantaux ;
- coulissant, fonctionne au moyen d'un rail fixé au sol ;
- autoportant, sans rail au sol mais guidé par portiques.

Suivant le flux de visiteurs à gérer, la commande s'effectuera manuellement ou automatiquement. De même, afin de réguler les entrées/sorties, un système de barrières levantes pourra venir en complément.

## >Des équipements complémentaires

Plusieurs solutions efficaces permettent également de compléter la sécurisation d'un bâtiment public par l'extérieur : plots, barreaux sur les fenêtres et ouvertures accessibles, rideaux métalliques, volets roulants de sécurité, vitrages retardateurs d'effraction, portes et grilles coulissantes ou extensibles.

# Protection mécanique : **élémentaire et indispensable**

*A l'intérieur d'un bâtiment*

***La protection mécanique ne concerne pas seulement les dispositifs extérieurs. Les espaces intérieurs peuvent également accueillir des moyens spécifiques pour contribuer à mettre en échec d'éventuels indélicats.***

## >Des portes sécurisées

On trouve aujourd'hui des produits de grande qualité permettant de sécuriser la plupart des portes : portes d'entrée ou de communication, portes palières, portes coupe-feu… L'attention doit se porter sur l'ensemble du produit, notamment la robustesse du bloc-porte et des huisseries, le blindage étant bien entendu l'option optimale. Certains fabricants proposent des dispositifs "anti-effraction" dont il vaudra mieux s'assurer qu'ils répondent aux deux référentiels en vigueur :

- la norme européenne XP ENV 1627 (classification de la résistance aux tentatives manuelles d'effraction) ;
- la certification NF A2P applicable à l'ensemble "vantail, huisserie et quincaillerie", la serrure devant être elle-même obligatoirement certifiée NF A2P.

**Bon à savoir**

Pour limiter les actes de malveillance, un dispositif d'éclairage extérieur, judicieusement placé pour éviter les zones d'ombre, constitue un complément technique efficace. Liés à des détecteurs de présence, ces éclairages peuvent créer un effet de surprise dissuasif.

## >Des serrures et verrous résistants

Une serrure de porte, de fenêtre ou de volet n'est pas un objet anodin ! D'autant que de larges gammes de produits sont actuellement proposées sur le marché, avec une qualité variable de résistance à l'effraction.

Deux grandes familles se distinguent, les "mécaniques" et les "électroniques".

- Les serrures **mécaniques** associent des dispositifs de fermeture mono-point ou multipoints (on recommande les 3/5 points certifiées NF A2P) à des systèmes de clés à haute performance. Deux systèmes de fixation existent : "en applique", vissées sur la porte, ou "à mortaiser", c'est-à-dire encastrées dans l'épaisseur de la porte.
- Les serrures **électroniques**, voisines des multipoints mécaniques, s'en différencient par un système d'ouverture géré par une clé électromécanique, un clavier, une carte ou un badge. Elles peuvent également faire l'objet d'une gestion plus élaborée on-line ou off-line.

Au-delà de la qualité des serrures choisies, il faudra veiller au bon rangement des clés, au contrôle journalier de leur distribution, et d'une manière générale à leur bonne gestion. A ce titre, les armoires de consignation contribuent à un fonctionnement simple et sécuritaire. L'utilisation de clés hiérarchisées (ou de codes électroniques) permet en outre de faciliter le contrôle de la circulation des personnes.

## >Les coffres-forts, chambres et armoires fortes

Le choix d'installer ce type d'équipement est conditionné par trois principaux paramètres : l'importance des objets, documents ou valeurs que l'on envisage d'y déposer, la configuration des locaux et les éventuelles défenses environnantes. Largement usitée en Europe, la norme NF EN 1143-1, qui définit les exigences, classification et méthodes d'essai pour ces matériels, sert de référentiel à la plupart des certifications (comme la NF A2P). Elle représente donc un gage de qualité.

### Exigez la certification NF A2P

Les serrures et verrous certifiés NF A2P démontrent leur double résistance aux effractions destructives et à l'ouverture fine. Les critères utilisés pour mesurer leur performance reposent sur le temps de résistance, l'outillage d'essai et la méthode d'attaque.

# Contrôle d'accès : **de l'interphonie à la biométrie**

*Contrôler l'accès à un bâtiment public revient à identifier puis autoriser une personne à pénétrer dans un site protégé.*
*Parmi les systèmes de contrôle d'accès, le choix ne manque pas pour répondre à tous les types et tailles d'architecture. Pour une efficacité optimale, la solution retenue doit prendre en compte des critères essentiels, comme le nombre de personnes susceptibles de franchir chaque point de contrôle, ou les conditions d'exploitation spécifiques au bâtiment.*

## >L'ère du contrôle automatique

Les dispositifs de contrôle d'accès basiques nécessitent une demande : c'est le cas de la traditionnelle sonnette ou de l'interphonie. Ils supposent une intervention humaine pour valider l'autorisation d'accès, d'où une organisation parfois complexe en fonction des horaires d'ouverture du site protégé. Solution moins contraignante et plus fonctionnelle, le contrôle automatique délivre une autorisation d'accès par des systèmes d'identification que l'on peut répartir en trois catégories :

- l'identification par un élément que le demandeur possède (clé, carte ou badge…) ;

- l'identification par une information qu'il détient (code, général ou personnel) ;
- l'identification par la propre identité du demandeur (élément anthropométrique).

Autre avantage, l'autorisation d'accès délivrée peut être générale pour l'ensemble d'un bâtiment ou réservée à certaines zones.

**Changez les codes !**
Dans les systèmes utilisant des codes électroniques, il n'est pas rare de constater l'utilisation de combinaisons simplissimes (0000 ou 1234, par exemple)… à proscrire absolument pour éviter des déconvenues ! Et même avec des codes plus sécurisés, il convient par précaution de les modifier régulièrement.

## >Cartes ou badges, un classique

En quelques années, les systèmes de contrôle d'accès par cartes ou badges sont devenus les plus utilisés. Ils s'appuient aujourd'hui sur plusieurs types de technologies : magnétique, optique, électronique (active ou passive) à effet Wiegand, ou encore à circuit intégré… la fameuse "carte à puce" !

Chaque technologie présentant ses avantages et inconvénients, le choix sera guidé par des critères variés parmi lesquels l'application souhaitée (contrôle d'accès seul ou couplé avec une gestion des horaires, de la restauration, etc.), le degré de sécurité recherché, la catégorie d'utilisateurs…

Considérés aujourd'hui comme fiables et robustes dans de nombreux environnements, les cartes ou badges se sont rendus incontournables pour un contrôle d'accès qui offre également l'avantage d'une fluidité de passage.

## >Biométrie, l'avenir ?

A la pointe de la technologie, la biométrie se base sur la reconnaissance de caractéristiques propres à un individu : à partir de l'analyse d'une partie du corps (main, œil, visage...), le système cherche, dans une base de données, les critères morphologiques pour une personne déterminée et les compare à ceux qui ont été préalablement prélevés et stockés. L'entrée dans un bâtiment n'est autorisée que si les critères concordent.

systèmes biométriques permettent pourtant de renforcer la sécurité d'un accès par un process d'authentification fort et convivial. Ils offrent également l'avantage d'éviter les cartes perdues ou volées, les codes oubliés… Mais il reste encore quelques contraintes à surmonter, comme la fragilité du lecteur à l'extérieur, les règles imposées par la Cnil* ou l'investissement nécessaire.

La solution performante : associer, dans un système global de contrôle d'accès, la technologie à carte et la biométrie, en tirant parti de leurs avantages respectifs.

** Commission nationale de l'informatique et des libertés*

# Détection : **la télésurveillance au rapport**

*La détection électronique a pour objectif de protéger un bâtiment public des intrusions ou de l'incendie. Conçue sur le principe de la sécurité positive, elle consiste à signaler toute anomalie par le déclenchement d'une alarme. Le signal d'alerte peut prévenir un contact identifié (gardien, élu, personnel d'astreinte ou service extérieur...) et permet de provoquer éventuellement une intervention sur site. A ce titre, la télésurveillance des installations apporte une réelle valeur ajoutée.*

## > Détection électronique : à l'extérieur comme à l'intérieur

Complément efficace à la protection mécanique, la détection électronique utilise de multiples capteurs, contacteurs ou autres détecteurs. Pour l'extérieur, on peut les regrouper en trois types :

- sur clôture, pour déceler les tentatives d'escalade ou de découpe (détecteurs de chocs, de tension, de vibrations) ;
- à barrières immatérielles (détecteurs à infrarouge, à hyperfréquence, radars à ultrasons) ;
- enterrés (câbles rayonnants, tubes à pression, détecteurs sismiques ou géophoniques).

Pour l'intérieur, on distingue généralement quatre grandes familles de détecteurs :

- ponctuels (mécaniques, magnétiques, etc.) ;
- linéaires (infrarouge, photo-électrique) ;
- volumétriques (hyperfréquence, ultrasons, infrarouge) ;
- de surface (infrarouge, sismiques, piézoélectriques).

Ces différents moyens, seuls ou associés, permettent de couvrir à la fois la périphérie et la périmétrie d'un bâtiment. Le choix définitif sera notamment guidé par la prise en compte de son architecture et de son envi-

### Les dispositifs d'alarme

Pour assurer une certaine dissuasion, la détection reliée à une centrale d'alarme peut déclencher différents dispositifs. Si l'on pense spontanément à l'alarme sonore (sirène), il existe également des moyens visuels et d'éclairage (à éclat, flashes, gyrophares) ainsi que des diffuseurs de brouillard ou de fumée…

ronnement, sans oublier les spécificités locales, comme les conditions atmosphériques (fréquence des vents, pluies, brouillard ou neige...).

## > Télésurveillance : la valeur ajoutée

Réceptionner et traiter à distance les informations délivrées par le(s) système(s) de détection électronique, voilà la raison d'être d'une station de télésurveillance. Une réelle valeur ajoutée pour renforcer la vigilance des bâtiments !

Le report permanent des informations s'effectue via les réseaux de téléphonie traditionnelle, ou ADSL en liaison IP, ou hertziens GSM/GPRS. La mission de télésurveillance peut être exercée sur le site même (avec un poste de sécurité) ou décentralisée en un lieu géographiquement distinct. A ce titre, il est aujourd'hui possible d'opter pour une solution de gestion multigroupe, i.e un mode de télésurveillance à grande échelle (plusieurs sites ou bâtiments) à partir d'un seul et même poste. Une formule intéressante qui permet en outre de coupler la détection anti intrusion et la détection incendie.

### Règle APSAD R 31 : la référence !

La règle APSAD R 31 définit les exigences minimales auxquelles doivent répondre les stations de télésurveillance. Elle propose aussi une aide à la décision pour le choix d'une solution et la contractualisation d'une offre de services.

# Vidéoprotection : **caméras au point ?**

*La vidéoprotection consiste à placer des caméras de surveillance dans un lieu ou un établissement, public ou non, voire sur la voie publique, afin de prévenir tout acte de malveillance. Jusqu'à la loi Loppsi 2 de 2011, on parlait de vidéosurveillance. On parle aujourd'hui de vidéoprotection dans l'ensemble des textes juridiques, un glissement sémantique plus consensuel.*

## >Bien analyser ses besoins

Loin d'être la panacée, un dispositif de vidéoprotection peut s'utiliser à titre principal ou s'intégrer dans un plan global de sécurisation, en complément d'autres solutions (par exemple, en appui d'une détection d'intrusion). Indispensable, l'analyse des besoins *("de la vidéo, pour quoi faire ?")* permettra de définir l'architecture technique du système et de ses fonctionnalités : qualité d'image, choix du réseau et du mode d'exploitation, modalités du stockage. Il paraît essentiel que la solution retenue réponde à l'objectif assigné, quitte à se poser la question point par point : quel type d'image et quelle caméra pour quel besoin ?

D'une bonne analyse dépendront également la qualité de l'organisation humaine à mettre en place pour un fonctionnement efficace et le sérieux du chiffrage.

### Comment ça marche ?

La vidéoprotection fonctionne selon un principe relativement simple : une caméra, fixe ou mobile, permet de surveiller, de façon permanente ou non, un espace donné (c'est la fonction ''production des images"). Les images sont transportées par différents moyens (courant faible, fibre optique, faisceau hertzien, wi-fi…) vers un centre de surveillance vidéo situé sur place ou à distance (''transmission"). Elles peuvent être ensuite visualisées (''exploitation") en temps réel et/ou enregistrées (''stockage") pour une exploitation en différé.

## >Des choix techniques étendus

La vidéoprotection offre une multiplicité de dispositifs techniques, parfois complexes, de la technologie analogique au ''tout numérique", qui développe des possibilités quasi-infinies de traitement des espaces. Pour répondre à un besoin, différentes solutions se présentent : les technologies actuelles pouvant s'adapter à toutes les attentes, il convient de trouver

le meilleur rapport respect du cahier des charges / budget (investissement **et** fonctionnement). Ne pas oublier d'évaluer en amont les capacités d'évolution du système et l'indispensable maintenance, préventive et corrective, pour garantir un fonctionnement optimal.


## >Un encadrement règlementaire

- **Sur le plan technique**, les matériels de vidéoprotection doivent respecter des normes ou spécifications minimales définies par l'arrêté interministériel du 3 août 2007, complété par une annexe technique parue le 21 août 2007. Ces règles ont pour but d'assurer une bonne qualité des images en visualisation directe, ou après transmission et enregistrement, permettant les identifications nécessaires.
- **Sur le plan juridique,** la vidéoprotection dans les lieux publics et établissements ouverts au public est soumise à autorisation préfectorale. Une instruction de la demande vérifie que le but recherché vise la sécurité des personnes et des biens et que des précautions seront prises pour ne pas porter atteinte à la vie privée, notamment concernant la durée de conservation des images. Dans certains cas (images avec fichiers nominatifs), la vidéoprotection relève de la Cnil.

### Un site internet de référence

Le ministère de l'Intérieur consacre une section très complète de son site Internet à la vidéoprotection. Vous y trouverez des actualités, une documentation fournie et un guide méthodologique téléchargeable, en trois parties : votre démarche projet, des études de cas et des fiches thématiques, pour approfondir les aspects techniques, juridiques, organisationnels ou financiers. Une mine d'informations !
*www.interieur.gouv.fr/sections/a_votre_service/video-protection*

# Matériels et prestataires : **certifier, c'est gagner**

*Protéger les bâtiments de sa collectivité contre les actes de malveillance nécessite de réunir plusieurs conditions : une conception en amont pensée pour s'adapter aux besoins réels, du matériel fiable et efficace, des installateurs compétents et performants. La formule gagnante pour répondre à ces exigences de qualité ? La certification !*

Professionnels de l'assurance, de la sécurité et utilisateurs ont développé, en concertation avec les pouvoirs publics, trois systèmes de certification : A2P, APSAD et A2P Service.

## > A2P, la reconnaissance d'une sécurité renforcée

La marque collective A2P distingue les matériels de protection contre l'intrusion et contre l'incendie qui, par leur résistance, garantissent une sécurité renforcée. Elle est délivrée par le CNPP, organisme certificateur reconnu par la profession de l'assurance. Plus de 500 produits ont obtenu, à ce jour, le droit de porter la marque A2P, dans des applications telles que verrous, serrures, blocs portes et fermetures de bâtiments, ou encore des composants de systèmes, de détection intrusion (conjointement avec la marque NF).

## > APSAD, la certification de services

APSAD recouvre la certification de services pour l'installation et la maintenance des systèmes de sécurité dans le domaine de la malveillance. Elle distingue les professionnels qui, par leur compétence, leurs moyens et leur organisation, garantissent une prestation de qualité et certifiée après audits, contrôles de connaissances et vérifications en clientèle des prestations fournies. A ce jour, plus de 1 000 prestataires ont reçu cette certification dans divers domaines comme la détection d'intrusion ou la télésurveillance… Seules ces entreprises peuvent délivrer des déclarations de conformité et des comptes-rendus de vérification périodique.

Pour les systèmes électroniques de sécurité, APSAD est délivrée conjointement avec la marque NF Service, attribuée par AFNOR Certification.

**> A2P Service** recouvre la certification de service pour la pose et l'après-vente d'équipements de protection mécanique contre la malveillance.

Pour tout savoir sur les référentiels, les matériels et les prestataires certifiés : ***www.cnpp.com***

# L'irremplaçable **surveillance humaine**

*Une installation technique de sécurité, la plus performante soit elle, ne peut tout régler. La vigilance d'agents de gardiennage ou de prévention et de sécurité contribue largement à réduire la probabilité de survenance du risque.*

La surveillance humaine d'un établissement suppose bien entendu une parfaite connaissance du site et des locaux et nécessite une organisation et des procédures formalisées, souvent dans un règlement précis. Les agents affectés à cette mission accomplissent des tâches variées : rondes régulières (intérieures et extérieures), filtrage des visiteurs, contrôle d'accès, vérifications techniques des équipements de sécurité, surveillance par écran vidéo... Ils doivent en outre connaître les lois et décrets en vigueur dans le cadre de leurs interventions et respecter un « code de déontologie ».

## >Professionnalisme exigé

Toute collectivité peut faire le choix de confier le gardiennage et la surveillance de son patrimoine à un service interne ou à une entreprise de sécurité privée. Dans les deux cas, elle doit veiller à la formation et à la qualification de l'équipe, chargée d'intervenir dans des situations parfois délicates. D'ailleurs depuis 2009, le secteur privé exige obligatoirement une carte professionnelle, délivrée par le préfet de police, pour les agents de prévention et de sécurité (APS). Valable cinq ans, elle justifie d'une double garantie : habilitation de moralité et aptitude professionnelle.

### Que fait la police ?

En cas d'intrusion ou d'acte de malveillance constaté, le premier réflexe doit consister à avertir immédiatement la police nationale ou la gendarmerie, habilitées à intervenir. D'où l'intérêt de liaisons rapides par l'intermédiaire d'une station de télésurveillance ou d'une centrale de vidéoprotection. Dans le cadre de leur mission générale de sécurité intérieure, les forces de l'ordre peuvent également assurer une surveillance régulière des bâtiments publics par l'organisation de patrouilles ou de rondes.

# Audit de vulnérabilité : **Prévention SMACL à vos côtés**

*Votre assureur mutualiste vous accompagne, vous conseille et vous apporte une aide technique…*

Vos bâtiments publics sont souvent les premières cibles de malveillance et leurs dégradations viennent alourdir vos charges budgétaires. Pour améliorer et mieux garantir la protection et la préservation de votre patrimoine, SMACL Assurances vous propose de réaliser un audit de vulnérabilité. Ses objectifs consistent à rendre vos biens moins vulnérables, à garantir leur sécurité et entretenir ainsi une bonne image de votre collectivité...

Pour y parvenir, les experts du service Prévention s'engagent à vos côtés pour vous offrir :

- un inventaire et une évaluation des risques ;
- une aide personnalisée aux services techniques sur les bonnes pratiques ;
- un diagnostic et un accompagnement dans l'application des préconisations.

Pour vous aider à lutter contre le développement de sinistres au sein de votre collectivité, SMACL Assurances vous apporte également conseils et aide technique pour développer des plans de prévention sur mesure… qui vont de pair avec votre plan d'assurance. En lançant une démarche prévention, vous apportez des garanties sur le souhait de votre collectivité de réduire sa sinistralité. Votre mutuelle d'assurances ne peut qu'y être sensible !

**Votre contact :**
**Service Prévention SMACL Assurances**
Patrice Daverat
05 49 32 20 15
prevention@smacl.fr

# Pour compléter votre démarche prévention-protection...

Dans ce guide, réalisé en partenariat avec l'Association des Petites Villes de France (APVF), SMACL Assurances vous propose des réponses en matière de réglementation et de responsabilité quant au risque Incendie. Vous y trouverez également l'essentiel des mesures à prendre en matière de prévention et de prévision.

**N'hésitez pas à le demander, il est gratuit !**


Contactez le **SERVICE PREVENTION SMACL ASSURANCES**
**Tél. 05 49 32 20 15**
**prevention@smacl.fr**

# smacl.fr

Toujours disponibles...


**Stations d'épuration**

Pour en analyser les risques techniques et professionnels

**Risque routier professionnel**

Pour les responsables souhaitant engager une démarche d'évaluation et de plan de prévention

**Conduite en mission professionnelle**

Des conseils de prévention destinés à tous les agents concernés par la conduite

**Responsabilité civile personnelle des élus**

Pour clarifier des notions complexes à partir d'exemples concrets


**SMACL Assurances**

141, avenue Salvador Allende
79000 NIORT CEDEX 9

Tél. : + 33 (0)5 49 32 56 56
Fax : + 33 (0)5 49 73 47 20

**smacl.fr**