

GUIDE PRATIQUE PRÉCONISATIONS GÉNÉRALES DE SÛRETÉ TRAVAUX & RÉNOVATIONS

SOMMAIRE

SOMMAIRE	2
PREAMBULE.....	3
1. LES ZONES EXTERNES.....	4
1.1. Limite périmétrique de site	4
1.2. Zones extérieures	5
1.2.1. Surveillance et protection naturelle des lieux.....	5
1.2.2. Circulation et stationnement des véhicules	7
1.2.3. Enclaves	8
2. BÂTIMENTS	9
2.1. Conception et emplacement.....	9
2.2. Accès bâtimentaires	10
2.3. Autres accès bâtimentaires	13
2.4. Les parkings en sous-sol	14
2.5. L'intérieur des bâtiments et locaux sensibles	14
3. UNIFORMISATION DES MOYENS DE SÉCURISATION	15
3.1. Maintenance.....	15
3.2. Moyens de contrôles d'accès	15
3.3. Systèmes d'alarme intrusion	16
3.4. Systèmes d'alerte agression fixes.....	16
3.5. Vidéoprotection.....	17
3.6. Autres systèmes de protection et d'intervention	18
4. TRAVAUX ET INTERVENANTS EXTERIEURS	20
4.1. Etude de sûreté et de sécurité publique (ESSP)	20
1.1. Sécurisation des travaux.....	20
1.2. Rappel des règles d'accès	21
REFERENCES.....	23

PREAMBULE

Ce guide n'a pas pour objectif de se substituer à l'ensemble des concepts et normes de prévention situationnelle, aux recommandations de la prévention technique de la malveillance, ni d'évoquer toutes les mesures physiques du plan Vigipirate. Il s'agit d'une synthèse d'éléments concrets, posant les principes sûreté de base à intégrer en amont des projets de construction ou de rénovation, ainsi que les orientations à éviter pour la réalisation de nos structures.

Les mesures concernant l'intérieur des bâtiments et la gestion des flux internes ne sont pas détaillées. En effet, elles doivent faire l'objet d'analyses particulières par bâtiment. De même, les bâtiments et locaux sensibles requièrent des moyens de protection qui s'inscrivent dans un diagnostic sûreté dédié, ils ne sont donc être détaillés dans ce guide.

Chaque établissement de santé est doté au minimum d'un « plan de sécurisation d'établissement » (PSE) intégrant la menace terroriste, mais aussi la malveillance quotidienne qui ne l'épargne pas. Ce plan s'inscrit dans le cadre d'une politique globale et durable de sûreté d'établissement, qui concerne les zones et bâtiments existants, ainsi que les projets de construction et de rénovation. L'architecture des bâtiments et leurs agencements ne doivent pas être facteurs ou facilitateurs de malveillance, au contraire. Aujourd'hui, le curatif reste supérieur aux mesures préventives, c'est cet état qu'il convient de modifier. L'intégration du paramètre sûreté, dès l'origine de tous les projets de construction, restructuration et rénovation, constitue une source d'économie et d'efficacité.

Les notions de « lieu ouvert au public » et « d'hôpital ouvert sur la ville » ne sont pas incompatibles avec celles de la maîtrise des flux et de la prévention de la malveillance. Les exigences minimales de l'instruction ministérielle relative à la sécurisation des établissements hospitaliers, et autres recommandations issues des codes de la défense et de la sécurité intérieure, visent principalement à atteindre un seuil acceptable de risque. Le « juste risque », qui reste évolutif et adapté à chaque situation. Cependant, certaines dispositions minimales sont parfois encore absentes et pourtant le niveau requis au CHU de Bordeaux est supérieur aux autres établissements de la Région.

Parce que l'hôpital est essentiel à la vie de la nation, il doit être construit en capacité de se protéger pour assurer la continuité des soins prioritaires dans toute situation. Il est construit fermable au niveau périmétrique et bâtementaire, pour un fonctionnement global ouvert par défaut. Sa conception doit lui permettre de s'adapter à la situation et d'opérer des modes intermédiaires (fermeture nocturne, fermeture partielle, filtrage, zonage, protection d'urgence, confinement, évacuation etc.).

1. LES ZONES EXTERNES

1.1. Limite périmétrique de site

- **Le site est conçu fermé par une délimitation physique** permettant, entre autres, de l'isoler des entités juridiques et de la voie publique. Elle doit limiter le franchissement de véhicules par simple enfoncement et ne pas faciliter l'escalade des piétons ou la simple enjambée.
- **Le nombre d'accès doit être réduit au strict minimum en limite périmétrique de site** (véhicule ou piéton). Il convient au moins de ne pas les augmenter.
- **Les accès périmétriques disposent tous systématiquement de moyens de fermeture résistants et de portails à ancrage non actionnable de l'extérieur.** Ils prévoient des arrivées électriques et réseaux d'attente (possibilité de motorisation du portail, caméras, système de filtrage et/ou de contrôle d'accès).
- **Les flux publics et professionnels** (notamment logistique et livraison) **sont**, autant que possible, **dissociés sur le site**.

Lors de gestion de situations sanitaires exceptionnelles (Plan Blanc, NRBC, attentat) ou lors de situations plus courantes (envahissement de caravanes ou manifestants externes etc.), la gestion des accès périmétriques peut s'avérer primordiale. Les effectifs humains présents, ou parfois même avec du renfort, ne permettent pas cette gestion (en théorie, les effectifs présents prévoient deux agents sûreté/sécurité sur site par accès public véhicule ou piéton, pour permettre la gestion des extérieurs et d'assurer la surveillance et les interventions internes).

Ces accès doivent, d'une part disposer d'une fermeture et, d'autre part, être réduits au strict minimum pour faciliter toute gestion des flux.

Qu'il s'agisse de la limite périmétrique ou d'un bâtiment, l'augmentation du nombre d'accès ou un surnombre d'accès :

- ✓ Augmente les points de surveillance ou de gestion (sans effectif adéquat)
- ✓ Augmente les vulnérabilités du site et s'oppose à sa protection indispensable dans certaines situations (notamment NRC ou attentat)
- ✓ Constitue l'une première cause de neutralisation des organisations de gestion de situations sanitaires exceptionnelles
- ✓ Facilite la commission d'actes de malveillance du quotidien (plus de possibilités d'intrusion, plus de facilité de fuite, plus de points à surveiller et à gérer)
- ✓ Facilite les envahissements (quelles que soient les procédures internes)
- ✓ Dans une situation immédiate, soumet le site à la réactivité de renforts coûteux, qui ne seront pas toujours disponibles ou en nombre suffisant

La présence d'une barrière de filtrage en limite périmétrique n'est pas suffisante, elle doit systématiquement pouvoir être remplacée ou complétée par un portail résistant.

En dehors des anciennes bâtisses déjà existantes en centre-ville, l'installation de bâtiment en bordure périmétrique de site est à éviter. Néanmoins, dans une telle configuration, il est impératif qu'aucune issue, même de secours, ne soit positionnée sur la limite périmétrique de site. Dans tous les cas, il est nécessaire de chercher à réduire les accès périmétriques plutôt que d'en créer. Cette situation requière une résistance élevée des ouvertures (notamment vitrages) de façade côté voie publique (les normes existantes sont rarement appliquées).

1.2. Zones extérieures

1.2.1. Surveillance et protection naturelle des lieux

D'une manière générale, la densité et le type de flux déterminent les matériels à déployer. Par exemple, pour des raisons de maintenance, un obstacle escamotable ne pourra être activé qu'en cas de rupture d'une barrière ou sur déclenchement manuel. La nature de l'entrée et des flux prévus déterminent les choix en fonction des risques encourus.

- **Itinéraires piétons et 2 roues**

Des itinéraires sont dédiés, protégés de la circulation et du stationnement des véhicules, et bénéficient d'un éclairage homogène. Les cheminements des professionnels à vélo est également à matérialiser et intègrent le plan de circulation du site, afin d'éviter de créer des flux et des accès anarchiques.

Les parcs à vélo sont stratégiquement disposés à proximité des parvis, pour une surveillance naturelle, sans être accolés aux accès bâtimentaires, comme pour toute installation (kiosque, poubelle, poteau, abris...). En dehors des parcs et dispositifs à vélo dédiés, le mobilier ambiant au niveau des principaux parvis publics, n'offrent pas de faciliter d'attache (ou d'approche) des deux roues.

Les parcs pour les vélos des personnels sont solidement grillagés, bénéficient des droits d'accès par carte professionnelle CHU et font l'objet d'une certaine réactivité de réparation. La taille des zones de stationnement des deux roues des usagers (vélo, mais aussi deux roues motorisés) ne sont pas à négliger. Leurs systèmes d'attaches (arceaux...) sont solidement ancrés dans le sol et résistants.

- **Espace verts (ou zones sportives)**

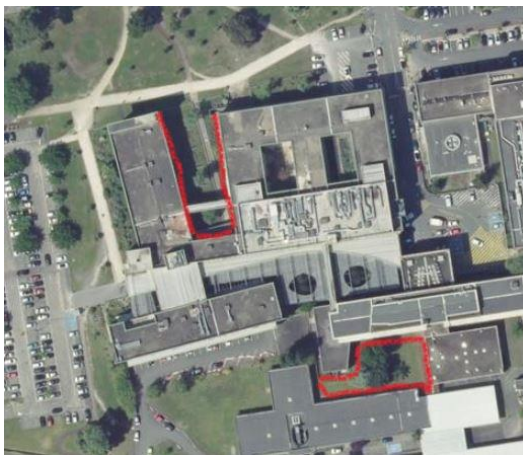
Le type de végétation du site doit être déterminé ainsi que l'entretien qui en est ou qui en sera réalisé. De même, il faut s'assurer que cette végétation ne forme pas exagérément un masque végétal isolant une zone, car ne permettant pas surveillance naturelle satisfaisante (visibilité).

Les zones associatives et sportives sont correctement délimitées et suffisamment protégées des intrusions en véhicules ou envahissements (fossé, merlon, barrière type IPN avec chicane). Une simple barrière avec cadenas ne permet pas de répondre à ce besoin et occasionne systématiquement des situations complexes, voire onéreuse (procédures, réparations, effectifs supplémentaires de gestion).

Il est à noter que la majorité des stades ne disposent évidemment pas d'accès aux véhicules, ce n'est pas par hasard. Les squats et envahissements sont facilités par l'absence de mesures préventives. Un parallèle peut être établi avec les communes qui ont appris, à leur dépend, à concevoir des installations publiques disposant de protections adaptées afin de mettre fin, ou de réduire considérablement, les procédures administratives d'expulsion, peu dissuasives mais coûteuses, ainsi que les destructions récurrentes aux préjudices souvent sous-estimés.

- **Structure des bâtiments ou espaces entre les bâtiments**

Toujours pour faciliter une certaine surveillance naturelle et ne pas générer de zones facilitant la malveillance ou un sentiment d'insécurité, les architectures « dents creuses » ou formant des zones isolées (cachées) sans activité doivent être évitées autant que possible. Lorsque de tels endroits ne semblaient pas prévisibles mais que les méfaits et interventions révèlent la vulnérabilité, des mesures correctives de fermeture efficace et/ou surveillance électronique s'imposent).



Exemples :

- . Dent creuse pour faciliter l'accès du public depuis les transports publics au Nord (et probablement question de luminosité). Mais s'avère de faible raccourci par rapport à l'accueil principal, ajoutant un accès faible au bâtiment, zone insécure soir et we (interventions police) : bénéfice avantages/risques non avantageux.
- . Zone isolée sans activité, lieu de trafic de stupéfiants et rixes et point d'intrusion récurrent.

- **Parvis**

Les parvis des principaux accès publics requièrent des dispositifs anti-véhicule bélièr qui peuvent être discrets et s'insérer dans le mobilier urbain (bornes, jardinières ou mobilier urbain d'un niveau de résistance adapté NF CEN TR 14383-8).

Aucun facilitateur de dépôt d'explosifs ne doit être installé à proximité des accès bâtimentaires sur les parvis où dans les halls d'accueil. Les poubelles nécessaires dans ces zones sont positionnées pour limiter au mieux le risque et ne permettent que l'utilisation de sacs transparents. Les mêmes principes s'appliquent avec les cendriers. Tout kiosque ou autre facilitateur, ainsi que les livraisons aux heures d'affluence, sont à proscrire (circulation à prévoir en conséquence).

- **Zones fumeurs**

Des « zones fumeurs » devront être prévues, clairement identifiées et accessibles, y compris la nuit, afin que les issues de secours ne soient pas utilisées à cette fin et maintenues ouvertes (il en va de même des accès verrouillés la nuit qui restent dans les faits ouverts « à la crémone »...). Cet aspect, souvent négligé, constitue le premier facteur d'intrusion et de neutralisation des contrôles d'accès. Pour les patients fumeurs, notamment de nuit, des patios ou aménagements spécifiques, même réduits, devraient être prévus pour ne pas avoir à sortir de l'enceinte du bâtiment.

1.2.2. Circulation et stationnement des véhicules

- **Principes généraux des flux véhicules**

Une mauvaise gestion des flux véhicules peut impacter la nécessaire gestion des flux internes en situation de crise. De manière plus courante, les stationnements anarchiques occasionnent des incivilités et nuisent aux exigences en matière de sécurité incendie, notamment en obstruant les voies d'urgence. Pour limiter les effets, certains prérequis de conception sont préconisés (en parallèle d'une organisation dédiée) :

- **Signalétique** d'information, limitée, claire et lisible, disposée **en amont du site** (voie publique si nécessaire) et dans le site : indication des places de stationnement restantes, orientation vers les principaux bâtiments.
- **Zones de stationnement** nommées, délimitées, **hermétiques** (il ne doit pas s'agir de voies de traversée du site qui sont à dissocier), ne permettant d'accès lorsque la capacité maximale est atteinte (marge acceptable possible).
- **Voie des urgences** dissociée, **sécurisée en matière de stationnement sauvage**, facilitant les flux urgents et disposant des normes et d'une signalétique de voie publique (pouvant favoriser un partenariat et une sollicitation occasionnelle des services répressifs).
- **Zone d'arrêt à durée limitée** (« arrêt minute »), payante au-delà de cette durée **avec des tarifs dissuasifs**, avec une signalétique claire sur ce point et des équipements routiers adaptés (gestion sous délégation de service public si nécessaire, pas de facilité pour les personnels sur ces zones déjà encombrées). Idéalement, les flux des véhicules de secours sont distincts des flux publics. Les dispositifs d'accès à la zone offre des possibilités de filtrage (sas avec rideaux et/ou barrière...). L'accès au service de soins est protégé contre les véhicules (pas d'élan ni d'accélération possible, plots ou dispositifs de protection etc.).
- **Zone d'accès restreint** (dédiée aux services de l'établissement comme les cuisines ou à certains prestataires/livreurs identifiés) : signalétique d'accès restreint, délimitation de la zone résistante, accès protégé et filtré (barrière filtrante, vidéophone, contrôle accès etc.).

- **Délégation de service public des zones de stationnement**

La mise sous délégation de service public des zones de stationnement, zones d'accès restreint et zones d'arrêt à durée limitée peut être solution retenue partiellement ou globalement. Dans ce cas, elle ne doit pas se limiter à la gestion des équipements et du paiement, elles englobent nécessairement :

- La participation à l'établissement du plan de circulation (dissociant des flux publics et des flux professionnels ou spécifiques logistique / livraison) systématiquement mis à jour avec les évolutions
- La sécurité des zones de stationnement (effectifs adaptés de surveillance, gestion et entretien) et les moyens associés (caméras aux normes, moyens de filtrage de qualité...)
- Les moyens et signalétiques de prévention adaptés contre les stationnements anarchiques
- Les procédures et moyens de gestion des stationnements anarchiques

A défaut d'une délégation, ces domaines devraient intégrer une organisation formalisée.

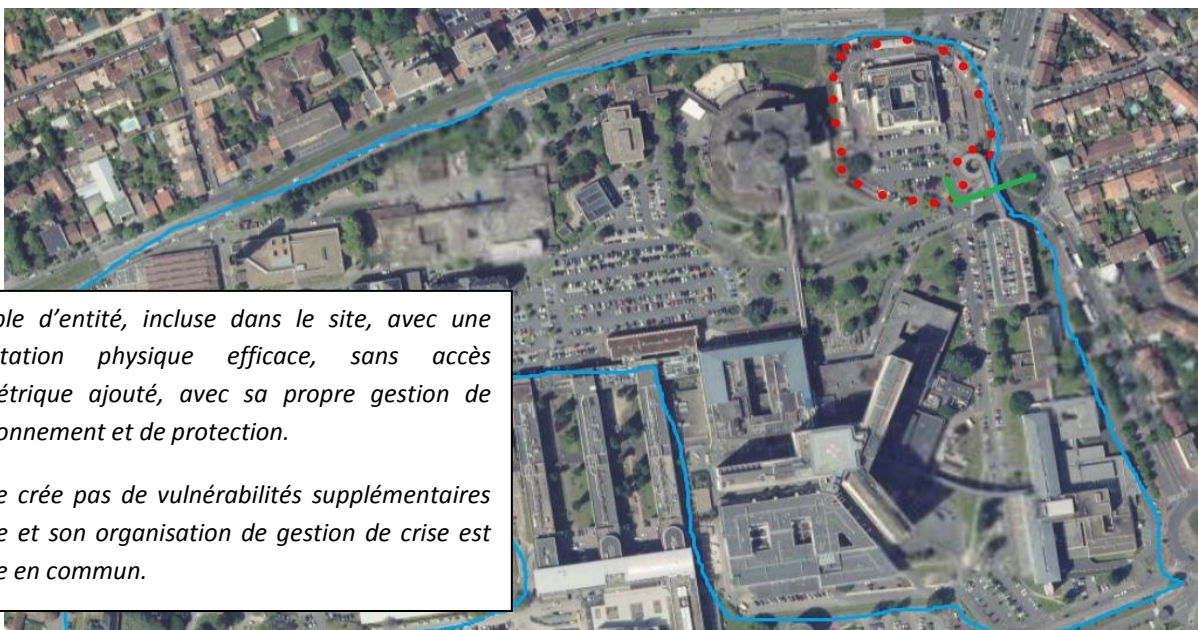
1.2.3. Enclaves

Les enclaves sur site d'entités distinctes du CHU ne doivent pas être source de vulnérabilités, notamment en créant des accès secondaires au site, et pire, des accès périmétriques. Ces deniers, même sécurisés, posent des problèmes de gestion des moyens d'accès (temps de gestion, perte, vol), de surveillance et de contrôle. L'ajout de périodes de vulnérabilités (accès plus facilement forcés ou détournés) et de besoin de maintenance est à prendre en compte.

Il est de loin préférable que les entités soient :

- totalement incluses sur le site et que les usagers utilisent les accès existants du site
- ou, au contraire, qu'elles soient physiquement dissociées du site, protégées contre la création d'accès sauvages vers le site (dégradation assurée si une simple clôture est mise en place) et obligeant également les usagers à utiliser les accès existants du site

Même s'il n'est pas souhaitable, un accès secondaire vers le site ne peut être que piéton (accès véhicule proscrit) et sérieusement sécurisé, comme la délimitation physique.



Exemple d'entité, incluse dans le site, avec une délimitation physique efficace, sans accès périmétrique ajouté, avec sa propre gestion de fonctionnement et de protection.

Elle ne crée pas de vulnérabilités supplémentaires au site et son organisation de gestion de crise est établie en commun.

2. BÂTIMENTS

2.1. Conception et emplacement

- **Architecture**

De la même manière que la structure et les espaces entre les bâtiments peuvent créer de zones d'insécurité, **la conception des bâtiments peut être facilitatrice d'intrusions et d'autres actes de malveillance.**

Les passerelles entre les structures, lorsqu'elles sont nécessaires, sont systématiquement sous contrôle d'accès et/ou dans une zone non accessible au public.

Les terrasses, les toitures et leurs accès doivent être sécurisées par des dispositifs fixes efficaces et des moyens d'accès strictement limités. En plus de l'intrusion, les groupes et prises d'air neuf disposés en toiture constituent souvent des points de vulnérabilités non négligeables. D'une manière générale, les toits-terrasses favorisent les incivilités et la malveillance.

Les portes et fenêtres s'ouvrant les terrasses aux étages soit ne sont pas être accessible par le rez-de-chaussée, soit bénéficient de d'ouvrants adaptés contre l'effraction (minimum portes métalliques à serrure A2P* et vitrage NF EN 356 classe P6B, avec châssis adaptés et/ou barreaudage ancré dans l'encadrement à faible espacement).

Exemples de toitures terrasses accessibles sans escalade



Exemple d'architecture permettant d'accéder aux terrasses et aux toitures sans escalade.



- **Façades et bâtiment en bordure de site**

Au niveau des accès publics, **des arrivées des réseaux électrique et informatique (POE+) sont à prévoir en façade** de chaque bâtiment.

En dehors des vieilles bâtisses en centre-ville, l'installation de bâtiment en bordure périmétrique de site est à éviter. Dans le cas contraire, il est impératif qu'aucune issue, même de secours, soit positionnée sur le limite périmétrique de site (accès voie publique). L'accès aux bâtiments doit être impossible depuis les fenêtres du rez-de-chaussée et du premier étage minimum, lorsqu'elles s'imposent.

Dans tous les cas, les caractéristiques et niveaux de résistance des matériaux de construction employés, notamment pour les ouvrants et ouvertures, sont définis.

En outre, les ouvrants des étages doivent être conçus pour rendre impossible la défenestration et disposent d'une serrure ou d'un système d'entrebâillement antichute non facilement démontable.

Ces ouvrants sont éviter ou doivent être particulièrement résistants sur les secteurs interventionnel, soins critiques, urgences, imagerie et médecine nucléaire, plateau de biologie, logistique médicale, logistique hôtelière, stérilisation, etc..

Les colonnes d'eau descendantes extérieures ou autres installations doivent être sécurisées afin de ne pas permettre leur escalade (ceint de piques avant l'ouvrant d'un étage par exemple, grille de pallier etc.).

2.2. Accès bâtimementaires

Tout bâtiment doit pouvoir être fermé la nuit (ou en situation de crise), y compris le sous-sol. Le public est dirigé vers les points d'accueil d'urgence dont l'accès offre la possibilité d'être filtré. Le personnel peut avoir recours à d'autres portes placées sous contrôle d'accès.

Les accès bâtimementaires, qu'il s'agisse des accès publics ou du personnel, **doivent être limités au strict minimum.** Ils doivent tous être de nature résistante à l'effraction et disposer de systèmes de fermeture et de verrouillage de qualité.

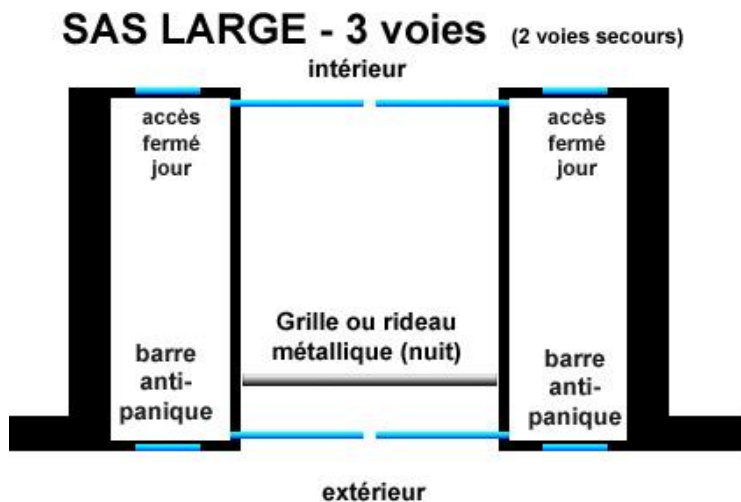
Les sas vitrés à ouverture automatique installés jusqu'alors, notamment aux principaux accès publics, ne sont plus adaptés à l'hôpital d'aujourd'hui et de demain. Ils sont tous aisément forcés des centaines de fois par an par le personnel ou toute autre personne désireuse de rentrer (et parfois de sortir). Ils constituent le point d'accès de plus d'un tiers des intrusions (pour vol ou autre). Alors que les accès secondaires se durcissent progressivement (portes résistances, moyens de verrouillages résistants et parfois contrôle d'accès), ces sas vitrés demeurent les points faibles du bâtiment, malgré une maintenance élevée et onéreuse.

Ces accès publics devraient, soit disposer d'ouvrants innovants, soit être complétés de moyens complémentaires s'ils conservent un sas automatique vitré.

Dans les deux cas, ils sont constitués de matériaux adaptés aux flux intenses et prévoient les possibilités de gestion et de filtrage évoqués s'ils sont d'utilisation permanente, ainsi qu'une vidéoprotection intérieure (en complément de l'extérieur).

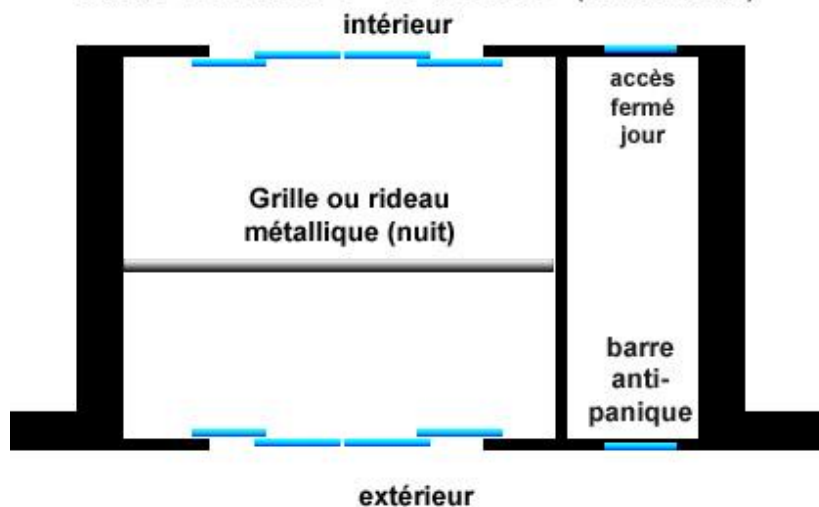
Exemple 1 :

SAS vitré fermé en période nocturne (fonctionnement non permanent) : grille métallique intermédiaire (dans le sas) et possibilité d'une ou deux voies de secours selon la taille du sas. Ces voies sont clairement signalées comme issues de secours et peuvent ne pas être actives en journée, voire asservie à la détection incendie. Elles ne permettent pas d'entrée et sont bien plus résistantes à l'effraction que les portes coulissantes (détection intrusion/ouverture possible et peu coûteux).



Exemple 2 :

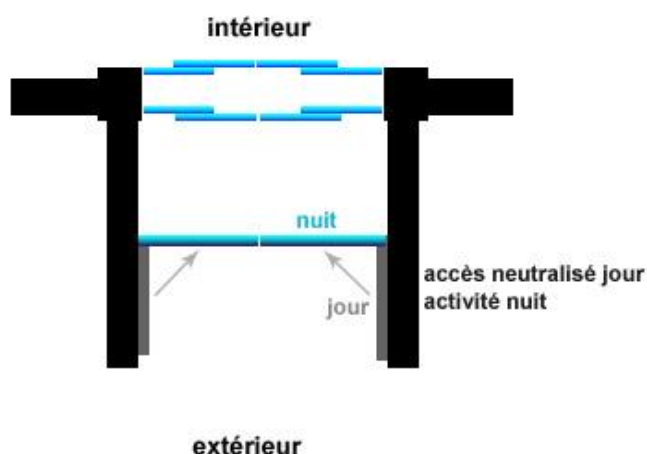
SAS LARGE - 2 voies (1 voie secours)



détection intrusion ou d'ouverture possible

Exemple 3 :

SAS vitré - 1 voie



vidéophones et contrôle d'accès activables en période nocturne

D'autres types d'accès publics, plus innovants et offrant les qualités de résistance et de filtrage requises, sont à étudier.

En attendant les rénovations, les sas actuels censés demeurer fermés la nuit devraient au minimum disposés d'une sirène locale et alarme reportée, paramétrées sur plage horaire automatique (déclenchement par détection d'ouverture ou volumétrique selon le type de sas).

Les accès du personnel sont placés sous contrôle d'accès, qui ne peut être activé qu'en période nocturne sur certains points, en fonction de l'activité. Ils disposent d'une alarme temporisée sur ouverture prolongée et d'un contact de porte reporté ou reportable (au PC).

Les vidéophones et systèmes de gestion des ouvertures à distance complètent le contrôle d'accès, en particulier lorsqu'il s'agit d'accès partagés ou dédiés aux prestataires. Mêmes dispositions sur les accès publics permanents. Ils permettent ainsi les trois principaux modes de fonctionnement, selon la situation et le niveau de risque associé :

- Mode ouvert (par exemple en journée), l'ouverture pouvant être automatique
- Mode filtrage (en permanence, uniquement en période nocturne ou sur situation sanitaire exceptionnelle)
- Mode verrouillage en cas de crise ou autre situation le nécessitant

Les issues de secours bâtementaires (ouverture vers l'extérieur) **sont verrouillées et ne peuvent s'ouvrir que sur détection d'incendie ou en situation de crise.**

Seuls les services sécurité détiennent les moyens d'ouverture de ces accès hors situation d'incendie (ouverture à distance et/ou ouverture de secours mécanique/clé électronique passive).

Les portes d'issues de secours au niveau extérieur doivent être de qualité suffisante pour résister à une tentative d'effraction et équipées de systèmes de temporisation d'ouverture, de détection d'effraction et de position.

En dehors des accès secondaires sous contrôle d'accès, les issues de secours donnant sur l'extérieur ne devront pas présenter de poignée (et si possible par d'autre prise) et seront dotées de ferme-porte efficaces régulièrement contrôlés (rôle du SSIAP lors de sa ronde de sécurité).

Il est préférable que le système d'ouverture interne soit constitué d'une « barre poussoir » (barre anti-panique) plutôt que tout autre type de poignée. Un contact de fond de gâche ou système équivalent est installé afin de déclencher localement une alarme sonore pour dissuader d'un détournement d'usage et connaître l'état de la porte (ouvert, fermé ou forcé) depuis le PC.

Dans les rares situations où le choix se pose, le sens d'ouverture des portes doit être pensé pour qu'elles résistent le mieux possible à une tentative d'effraction (disposition qui concerne plus généralement les accès internes ou intermédiaires).

Les systèmes de ferme porte sont à adapter à la fréquence des flux (il n'y a pas d'économie à installer un dispositif sous dimensionné, au contraire).

Domaine souvent négligé, les crémones pour les ouvrants à double battants doivent être composées de métal plein, solides (grosse section pour les accès bâtementaires) et suffisamment ancrées au sol et partie haute. De nombreuses crémones creuses actuelles s'enfoncent d'un simple coup d'épaule.

Les déclencheurs manuels (DM vert) souvent requis, permettent de neutraliser toutes les mesures de sécurisation par une simple pression, annulant tout équilibre des risques. Dans l'attente que la législation française évolue dans ce domaine, des contre-mesures peuvent être prises ; dont :

- Déporter le ou les DM vert dans des locaux à proximité, moins visibles (centralisés....).
- A défaut d'une position moins apparente et évidente, installer des DM vert à **sonnerie locale forte** (option alerte lumineuse) **et reportée** au Poste Central de Sécurité. Cela n'empêche pas la sortie, mais offre un certain niveau de dissuasion et limite les mauvaises pratiques locales.



2.3. Autres accès bâtimentaires

- **Circulation verticales extérieures** (escaliers, ascenseurs, échelles à crinoline)

Lorsqu'il s'agit d'accès de secours imposés par la réglementation incendie, ils sont rapidement détournés de leur fonction pour devenir des itinéraires secondaires ou raccourcis, créant des faiblesses non maîtrisées pour la protection des bâtiments et de leurs usagers. Les portes disposent donc des mêmes dispositions qu'évoquées précédemment (ouvrant métallique résistant, verrouillage par défaut, ouverture asservie détection intrusion, déclencheur manuel isolé et/ou protégé avec renvoi d'information...).

Lorsque l'escalier est enveloppé par une cage métallique, il est impératif que les protections contre les accès depuis rez-de-chaussée soient efficaces (pas de crochetage possible etc.).

Les échelles à crinoline sont utilisées pour les intrusions par la toiture ou permettent d'accéder à des groupes froids sensibles. Les protections d'accès (grille, plaque de protection, échelle sous cadenas sont systématiquement détournés par les entreprises intervenantes). L'emploi de cadenas à clé passive (sous caution, désactivable et traçabilité) constitue l'un des exemples pour pérenniser les protections en place qu'il convient de valider en amont de l'installation (réflexion contre la malveillance).

- **Galleries**

Les galleries doivent pour être totalement closes en période nocturne (grille avec asservissement détection incendie et présence d'un téléphone si réellement nécessaires). Si des flux s'imposent, ils sont limités et filtrés par contrôle d'accès (carte CHU et/ou vidéophone), mais uniquement aux points requis, cette disposition n'est pas à généraliser.

2.4. Les parkings en sous-sol

Ils facilitent naturellement le développement d'actes déviants (incivilité, extorsion, vol, dégradation, trafic de stupéfiants...). Inclus ou non dans une délégation de service public, les parkings souterrains exigent des moyens de surveillance et d'intervention particuliers, sans lesquels la situation se dégrade rapidement.

Ils sont à proscrire, d'autant plus s'ils sont publics, sous un service d'urgence à forte fréquentation, sous des blocs opératoires (notamment s'ils sont concentrés sur un secteur) ou sous le principal hall d'accueil public du site.

2.5. L'intérieur des bâtiments et locaux sensibles

Les préconisations sûreté relatives à l'intérieur des bâtiments ne peuvent faire l'objet que d'une analyse particulière, adaptée au projet. Pour la conception des lieux et les moyens à mettre en œuvre, elles viseront principalement :

- Les halls d'accueil principaux du public
- La maîtrise et la dissociation des circulations et accès publics /professionnels
- La protection naturelle des lieux sans activité en période nocturne (structurellement hermétiques et compartimentés, peu d'accès, fermeture automatique sans action humaine, pas de flux hors période d'activité ou complètement maîtrisés).
- La maîtrise des flux des accès des circulations verticales (escaliers, ascenseurs) et accès de secours (par contrôle d'accès si nécessaire).

Les obligations ou recommandations relatives aux bâtiments et locaux sensibles ne peuvent faire l'objet également que d'un diagnostic dédié. D'une manière générale, ils doivent disposer d'une protection permanente (renforcement du bâti, contrôle d'accès en temps réel etc.) et de systèmes d'alarme intrusion, voire d'alerte agression. Comme sur le bâtimentaire, les informations sont fournies en temps réel au poste central. La protection de ces locaux répond au schéma classique de zonage et de limitation des risques de malveillance par des barrières successives retardatrices (qui complètent des mesures organisationnelles, et non l'inverse) :

surveiller – contrôler – limiter – interdire – intervenir

Les principaux locaux sensibles en matière de sûreté concernent :

- Les énergies et réseaux indispensables au fonctionnement de l'hôpital (centrale électrique, centrale air médical, eau potable, salle serveur informatique/Datacenter...)
- Les locaux constituant des moyens rares ou uniques dans la Région (SAMU, unité de décontamination hospitalière, laboratoire L3, lactarium...)
- Les locaux indispensables à la gestion des situations sanitaires exceptionnelles (blocs opératoires s'ils sont concentrés, local plan blanc et stocks à portée régionale...)
- D'autres locaux particuliers (PPMS imposé pour les crèches, pharmacie, ...)

3. UNIFORMISATION DES MOYENS DE SÉCURISATION

3.1. Maintenance

Quel que soit le système technologique de protection ou de d'alerte installé, une maintenance (préventive et curative) est systématiquement prévue, afin de préserver le niveau de sécurité requis. Les systèmes actuels, aussi performants soient-ils et en particulier ceux qui utilisent le numérique, sont rapidement vulnérables sans entretien. A court ou long terme, l'absence de maintenance n'est pas synonyme d'économie, bien au contraire. Même si elle est externalisée (totale ou partielle), les services techniques doivent détenir une capacité d'intervention de premier niveau.

3.2. Moyens de contrôles d'accès

Pour répondre aux besoins de sécurisation des accès, on peut considérer qu'il y a 3 niveaux de sécurité, auxquels correspondent des technologiques adaptées à la protection et au contrôle d'accès :

- Le niveau le plus élevé concerne les accès bâtimentaires et accès des locaux sensibles :
Il offre une information et une gestion en temps réel, avec une possibilité d'interface au poste central de sécurité ou de sûreté. Par souci d'uniformisation des matériels (et d'économie vis-à-vis de l'existant), le choix est actuellement porté sur la marque **TIL** et son logiciel **MicroSésame**. L'ouverture se réalise par la carte CHU.
Sur ces accès, les serrures mécatroniques (plus ou moins motorisées) sont à privilégier par rapport aux ventouses magnétiques, qui ne devraient être utilisées que pour certains accès internes (hors bâtimentaire et local sensible). Les serrures mécatroniques permettent un verrouillage mécanique résistant réel (pas limité au pêne demi-tour) et appliquent le principe de : porte fermée = porte verrouillée.
Il s'agit d'un matériel de qualité, mais onéreux. Il n'est donc pas à développer dans tous les locaux, qui peuvent majoritairement se contenter des deux autres niveaux.
- Le niveau intermédiaire offre également du contrôles d'accès, mais la traçabilité et la gestion ne s'opèrent pas nécessairement en temps réel, le niveau de risque étant inférieur. La mise à jour des droits d'accès peut être réalisée borne Wifi, par contamination avec borne de rechargement etc. :
 - Des **béquilles autonomes non filaires** sont plutôt utilisées pour les locaux communs (ouverture avec carte CHU) – borne Wifi possible
Ex : vestiaires, local de stockage, entrée d'un service...
Idéalement, pour des raisons de gestion automatisée des droits d'accès, le système s'interface avec les autres (portail CHU et/ou MicroSésame).
 - Des **serrures à clé électronique passive** (type Winkhauss) peuvent être adaptées pour des locaux peu ou non partagés. A peine plus onéreuse que des clés mécaniques de qualité, elles offrent les avantages de traçabilité, de désactivation des droits d'accès (immédiat ou automatique sur délai fixé) et la clé passive, quel que soit son niveau dans l'organigramme, ne coûte qu'une dizaine d'euros. Inutile

donc d'avoir à changer tout l'organigramme des clés en cas de vol ou perte d'un pass (ce qui n'est pas appliqué dans les faits car trop onéreux et trop fréquent, d'où le nombre important de vols sans effraction au CHU).

- Les clés mécaniques

Le moins onéreux, mais ne convient que si l'organigramme est réellement tenable dans le temps, accompagné d'une maîtrise parfaite des détenteurs des clés (caution si nécessaire). Ces clés peuvent convenir pour des bureaux, locaux classiques ou locaux techniques non sensibles..., avec peu d'utilisateurs et surtout une faible rotation de ces utilisateurs.

- Vidéophones, interphones, tags...

D'autres systèmes intègrent les systèmes de contrôle d'accès.

- Tag : il permet un filtrage automatisé et facilité des véhicules CHU (logistique ...)
- Vidéophone : il permet un filtrage des personnes extérieures au CHU, sans carte CHU (ex : vidéophones, qui doivent offrir une certaine traçabilité : une photo pour les 100 derniers passages).

3.3. Systèmes d'alarme intrusion

Les alarmes à détection d'intrusion sont prioritairement installées dans les locaux sensibles et dans les locaux professionnels sans activité soir et/ou week-end, en particulier ceux qui possèdent du matériel présentant un risque non négligeable en termes de vol ou d'impact suite à dégradation.

Le PSE définit la liste exhaustive des priorités (à noter que les logements de fonction actifs n'intègrent pas le PSE et les missions d'intervention du prestataire sûreté).

L'uniformisation des matériels est requise et une centralisation s'opère par groupe hospitalier au PCSi/PCS.

D'une manière générale, l'alarme est automatique programmée sur plage horaire, néanmoins activable/désactivable par carte CHU (gestion MicroSésame). Par défaut, une sirène locale est installée dans les locaux protégés.

Lorsque les locaux ne bénéficient pas de réseau IP CHU (locaux vacants, logement de passage...), ils peuvent être équipés d'alarmes GSM le temps de l'inoccupation, afin de réduire le risque d'occupation illicite. Ce matériel est moins fiable, mais son coût est réduit. Le report d'alarme s'opère de la même manière vers les PCSi/PCS, qui sont systématiquement intégrés au projet ainsi que le prestataire sûreté.

3.4. Systèmes d'alerte agression fixes

Les accueils principaux recevant du public doivent être équipés d'un bouton d'appel pour faire intervenir les services de sécurité. Afin de garantir un certain niveau opérationnel et une certaine efficacité, ils doivent être installés en nombre limité sur un site et systématiquement validés en amont par le service sûreté. Ils concernent :

- Les postes d'accueil principaux
- Les postes des admissions à forte fréquentation
- Les services des urgences

Dans ce domaine également, l'uniformisation et l'interface avec le synoptique MicroSésame sont requis. Le bouton poussoir d'appel est également uniformisé (sauf cas particulier), il s'agit d'un bouton à appui horizontal, positionné discrètement sous bureau, d'enclenchement unique avec réarmement obligatoire. Ainsi, il ne génère pas d'alerte intempestive.

La pose d'un tel système s'accompagne systématiquement d'une note et d'une information du service bénéficiaire auprès de ses agents, suivant les recommandations du service sûreté.

3.5. Vidéoprotection

Le responsable sûreté et la direction des systèmes informatiques (DSI) sont systématiquement impliqués dans ce type de projet qui n'est neutre ni sur le plan technique et ni sur le plan juridique.

Les caméras de vidéoprotection sont privilégiées aux accès et parvis publics (intérieur et extérieur), aux halls d'accueil, aux zones d'accès restreint notamment extérieures, puis aux points de passage stratégiques définis ou à définir au PSE. Elles n'interviennent dans les secteurs sensibles qu'en complément des dispositifs de protection précités, mais pas de manière systématique, car une finalité réduite à une simple levée de doute n'est pas pertinente.

Il s'agit en effet de limiter le nombre de caméras à exploiter et à entretenir, ainsi que d'éviter la saturation du réseau vidéo et celui du CHU.

Sans délégation de service public et/ou d'effectifs dédiés, l'équipement des zones de stationnement et zones d'accès à durée limitée n'offre que peu d'intérêt, voir génère des impossibilités de gestion (réponse aux réquisitions et sollicitations très chronophage).

Dans cette situation, les équipements extérieurs se limitent aux parvis, certaines façades de bâtiments et aux accès périmétriques (s'ils sont en nombre restreint), en priorisant les accès publics.

Si techniquement le noyau du système peut être commun, en revanche la gestion opérationnelle d'un système de vidéoprotection ne sera évidemment opérée que par groupe hospitalier. Pour ceux qui ne disposent pas d'un PC sûreté, le choix du matériel et son architecture (compatible GENETEC) intégreront nécessairement la particularité d'une exploitation principale des images à posteriori.

Il est rappelé que les autorisations préfectorales sont un prérequis indispensable à toute installation de ce type (au moins 4 mois avant le début de l'installation).

A tort, le marché de maintenance est souvent négligé dans ce domaine. Il s'impose pourtant rapidement pour la partie logicielle (mise à jour dépannage) et le nettoyage de premier niveau (nettoyage des globes au minimum quatre fois par an).

Principaux prérequis techniques :

- **Le CCTP précise que la qualité des enregistrements demeure la priorité, notamment l'obligation de résultat en termes de reconnaissance et/ou identification visée.** Néanmoins, les débits ne doivent pas dépasser la limite de 10Mbits par caméra, et

500Mbits à 1Gbits pour les équipements centraux (serveurs, stockeur). Une étude particulière peut concerner un ou deux capteurs (caméra 4K par exemple). Il est considéré que le réseau CHU accepte 13,5 Mbits/s sur ses équipements, mais le nombre de caméras sur un local réseau peut remettre en cause ce débit Max. Globalement, il ne faut pas dépasser 10 caméras par local technique, même chose pour la partie POE.

- Les caméras, les optiques, les mécanismes d'orientation des caméras bénéficient de protections contre le vandalisme et les intempéries (boîtiers thermostatés etc.).
- Le système offre une grande compatibilité des matériels de type ONVIF et demeure compatible avec la compression H.265.
- Les caméras doivent offrir une bonne sensibilité à la vision nocturne, favorisant la qualité des enregistrements dans ce contexte. Dans les cas extrêmes, cette acuité visuelle du matériel peut être soutenue par un éclairage. L'utilisation de la technologie infrarouge (filtre ou projecteur) s'impose au besoin.
- Lorsque le contre-jour constitue un paramètre pouvant nuire à la qualité des images, il est imposé que les caméras concernées intègrent des fonctions de correction de ce phénomène. Il en est de même pour l'éblouissement des phares de véhicules ou autre lumière présente sur le site.
- Le système doit être évolutif et systématiquement prévoir une certaine marge de ressource.

3.6. Autres systèmes de protection et d'intervention

- **ALERTE ENLEVEMENT OU SORTIE DE SERVICE**

Il s'agit en général de systèmes à détection RFID ou équivalent. Les patients sont équipés de bracelet ou dispositif en mesure de déclencher une alerte lorsqu'ils sortent d'une zone définie.

Les systèmes qui concernent les patients adultes sont gérés par les service où ils sont installés. Le type d'alarme locale est à définir selon les finalités et les particularités du service. Les services sécurité ne sont impliqués que dans le cadre de la procédure de recherches des personnes vulnérables sorties à l'insu du service.

Les mêmes systèmes s'orientant vers la prévention d'enlèvement de nourrisson, sont également gérés par le service et disposent d'alarmes locales adaptées. Outre les modalités d'intervention qui s'étudient en amont du projet, un report d'alarme est à prévoir au PC Sûreté local (lorsqu'il existe).

- **SYSTÈME D'ALERTE MOBILE**

Les dispositifs PTI (protection du travailleur isolé) obligatoires relèvent de la réglementation du travail, ils sont mis en œuvre sous contrôle des préventionnistes du service sécurité incendie et gérés par les PCSi.

Les systèmes à Wifi 3D, doublés ou non de GSM seraient très onéreux à déployer tout en offrant une précision de localisation insuffisante, au vu de la complexité des bâtis du CHU. Toutefois, une évolution de ces matériels sera à prévoir.

D'autres systèmes GSM sur smartphones se développent, mais ils ne permettent pas de préciser avec fiabilité la position dans les bâtiments à étage (sauf installation d'un réseau dédié).

- **SONORISATION / MESSAGES VISUELS**

En priorité dans les zones ouvertes au public, l'ensemble des bâtiments devrait disposer de haut-parleurs permettant de diffuser en tout point, depuis le PC sécurité / PC sûreté, un message diffusé par micro ou par fichier préenregistré. Le dispositif devrait être activable par zone, un bâtiment pouvant constituer une zone.

Les principaux halls publics devraient également bénéficier de téléviseurs (ou écran vidéo) en mesure de diffuser des informations préventives en continu et d'alertes particulières en situation de crise.

4. TRAVAUX ET INTERVENANTS EXTERIEURS

4.1. Etude de sûreté et de sécurité publique (ESSP)

La réalisation d'un dossier ESSP s'impose pour les projets répondant notamment aux caractéristiques suivantes :

- Établissement Recevant du Public (ERP) de 1ère catégorie (plus de 1 500 personnes par jour) ou de 2ème catégorie (entre 701 et 1 500 personnes par jour).
- Localisation en agglomération de plus de 100 000 habitants.

L'ESSP est une pièce constitutive du dossier de permis de construire et fait l'objet d'une analyse préalable en sous-commission préfectorale.

Les études de sécurité et de sûreté publique (ESSP) sont une obligation réglementaire peu connue concernant les gros projets d'aménagement, en application de l'article 14 de la loi du 5 mars 2007 sur la prévention de la délinquance modifiant l'article L 111-3-1 du Code de l'urbanisme traduit dans un décret publié en août 2007.

Une circulaire et un décret publiés en 2010 et en 2011 étendent le champ d'application de la loi. Le législateur entendait ainsi amener les aménageurs à s'emparer du sujet de la sécurité, dont ils se seraient jusqu'à présent plutôt désintéressés

Étude de sûreté obligatoire ou non, dans les objectifs visés de pérennité, de performance et d'économie, l'intégration du paramètre en amont des projets de construction et de rénovation s'impose désormais. L'erreur courante de négliger cet aspect et de se retrouver dans des situations inextricables en termes de sécurité, de devoir engager par la suite des moyens coûteux et difficilement adaptables, ne devrait plus se reproduire au CHU de Bordeaux.

1.1. Sécurisation des travaux

Que ce soit pendant une phase de travaux ou une phase d'emménagement, pendant laquelle le CHU redevient responsable des lieux, il est impératif que le projet intègre financièrement les moyens humains nécessaires de surveillance et/ou filtrage contre les risques de vols ou de dégradations. Car ces moyens ne pourront pas être obtenus par des renforts sûreté classiques, aucun budget n'étant accepté pour ce type de mission et aucun site du CHU ne disposant d'effectif sûreté en mesure d'effectuer des missions statiques prolongées.

La demande classique de « ronde particulière », notamment sur les sites ne disposant que d'un agent sûreté (en charge des interventions, des surveillances particulières, de la gestion des accès périmétriques et bâtimentaires...), demeure illusoire et constitue un raccourci généralement inapproprié par rapport au niveau de risques.

1.2. Rappel des règles d'accès

Le règlement intérieur et le plan Vigipirate définissent les règles d'accès au domaine du CHU de Bordeaux.

Chaque entreprise ou intervenant extérieur dispose d'un référent CHU responsable du contrôle et de l'application de ces règles. Celles-ci doivent systématiquement paraître dans les accords-cadres, marchés publics ou convention, notamment les règles d'accès et de gestion des moyens d'accès.

Le principe de base est de maîtriser les flux des intervenants externes, d'identifier les catégories d'intervenants, leur fonction et les trajets empruntés pour chacun d'entre eux, d'avoir une traçabilité plus ou moins exhaustive en fonction des lieux fréquentés, de leur communiquer les dispositions du règlement intérieur et de prendre les mesures qui s'imposent en lien avec le référent lorsqu'elles ne sont pas respectées.

Certains lieux sensibles exigent une déclaration nominative préalable des intervenants et des conditions strictes d'accès.

Les mesures de sûreté et Vigipirate s'appliquent à toutes les personnes présentes sur l'un des sites du CHU de Bordeaux. La sécurité est l'affaire de chacun, en particulier sur certaines zones techniques ou de travaux, ainsi que dans les secteurs sous contrôle d'accès.

Des moyens d'accès CHU (carte, clé, tag, code...) peuvent être remis à un intervenant externe pour faciliter son activité et lui permettre d'accéder à des zones contrôlées. Ces moyens d'accès sont produits en nombre strictement limité, en fonction des capacités du secteur.



Ces moyens d'accès demeurent la propriété du CHU de Bordeaux et peuvent être retirés en cas de non-respect de leur utilisation ou du règlement intérieur, sans faire obstacle aux poursuites pénales et exclusions qui peuvent être engagées.

Les moyens d'accès sont remis contre les renseignements et les coordonnées de l'administration ou de l'organisme concerné, ainsi que l'identité complète du responsable local et des agents détenteurs d'un de ces moyens. Dans les zones d'accès restreint, l'immatriculation du véhicule autorisé à pénétrer sur la zone est précisée.

Les moyens d'accès :

- sont délivrés pour une durée limitée, dans le strict cadre de la mission, dans les jours et créneaux horaires autorisés. Ils sont obligatoirement remis à la fin de contrat.
- **sont strictement personnels** et ne peuvent être prêtés ou cédés à un tiers.
La modification d'un agent fait systématiquement l'objet d'une déclaration préalable.
- sont utilisés pour tout accès, même lorsque plusieurs personnes franchissent ou que l'accès à franchir est déjà ouvert.

Ne pas autoriser ou faciliter l'entrée d'une personne dépourvue d'un moyen d'accès CHU ou dont la carte ou la clé semble inactive ou non autorisée, vous engageriez votre responsabilité

En cas de perte, de vol ou de détérioration d'un moyen d'accès, un signalement sans délai est obligatoire auprès de votre référent CHU. Une nouvelle carte ou clé pourra être remise moyennant une contribution financière (actuellement de 17€).

Pour justifier de votre présence sur certains secteurs, présentez votre carte CHU aux agents de sûreté ou sécurité qui vous le demandent. D'une manière générale, facilitez les éventuelles opérations de contrôle.

Les matériels et effets sont placés sous la responsabilité de leur propriétaire et ne doivent, en aucun cas, conduire à une situation suspecte par négligence (bagages, matériels ou déchets abandonnés).

En cas de situation particulière, appelez prioritairement votre référent CHU ou le poste de sécurité (le cas échéant mentionné au plan de prévention).

Un comportement responsable et vigilant est attendu par tous

REFERENCES

Article 14 de la loi du 5 mars 2007 sur la prévention de la délinquance modifiant l'article L 111-3-1 du Code de l'urbanisme traduit dans un décret publié en août 2007

(circulaire et décret publiés en 2010 et 2011 étendant le champ d'application)

Guide des études de sûreté et de sécurité publique dans les opérations d'urbanisme, d'aménagement et de construction- Broché 22 octobre 2007

Instructions Générales interministérielles (IGI) incluant notamment les obligations de sûreté aux opérateurs d'importance vitale (OIV) secteur santé :

- IGI NRBC incluant confinement périmétrique 2005
- IGI 6600/SGDSN/PSE/PSDN 07.01.2014
- IGI 1300 13/11/2020

Mesures Vigipirate particulières de sécurisation d'Établissements de santé désignés - 2014

Guide de déclinaison des mesures de sécurisation périmétriques et bâtimentaires – Les Ministères sociaux.
« l'intégration du paramètre sûreté doit intervenir dès la phase de programmation des travaux » - 2014

PSE Instruction N°SG/HFDS/2016/340 relative aux mesures de sécurisation dans les établissements de santé - novembre 2016

Tome 1 à 3 Guide de la Prévention Technique de la Malveillance – Ministère de l'Intérieur

