



Edito

Chers clients, chers partenaires,
La sûreté des locaux n'est plus un sujet réservé aux grandes entreprises. Intrusions, vols, dégradations, agressions verbales ou physiques... Les risques de malveillance concernent aujourd'hui toutes les structures, y compris les TPE/PME.

Une bonne organisation de la sûreté permet de protéger vos salariés, mais aussi votre activité, vos données sensibles, vos matériels et votre image.

Dans ce numéro, je vous propose de faire le point sur les bases réglementaires, les bonnes pratiques et les leviers concrets pour sécuriser vos accès et limiter les situations à risque.

Bonne lecture,
Anthony B. – AF SST 56

Actualité réglementaire

✦ La sûreté, une obligation de protection du personnel et des biens

Le Code du travail (article L.4121-1) impose à l'employeur de prendre toutes les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des salariés.

Cette obligation inclut la prévention des risques liés :

- aux intrusions,
- aux agressions,

- aux actes de malveillance,
- et à l'accès non autorisé à des zones sensibles.

Ces risques doivent être évalués et intégrés au DUERP, au même titre que les risques opérationnels ou environnementaux.

Dans le cas d'un incident (vol, agression, intrusion), la responsabilité de l'employeur peut être engagée si les mesures de prévention étaient insuffisantes ou non adaptées.

Certaines activités (accueil du public, services à encaissement, zones de stockage, cabinets médicaux, etc.) nécessitent des mesures renforcées (alarmes, procédures d'accueil, sécurisation des flux).

👉 La sûreté n'est donc pas seulement un enjeu matériel : c'est une obligation légale visant à protéger les personnes, les biens, et la continuité de l'activité.

Astuce prévention

Clarifiez les règles d'accès.

Déterminez qui peut entrer, où et quand : salariés, prestataires, visiteurs, intervenants.

Attribuez des moyens d'accès adaptés (clef, badge, digicode) et supprimez les accès inutilisés.

👉 Une liste d'accès mise à jour régulièrement est l'un des meilleurs outils pour limiter les intrusions non souhaitées.

Focus du mois

Sûreté des locaux : anticiper les risques pour mieux protéger

Les menaces envers les entreprises évoluent : vol de matériel informatique, intrusions, dégradations, agressions en accueil, accès non contrôlés...

Une politique de sûreté efficace repose sur trois volets complémentaires : le contrôle des accès, la protection des zones sensibles et la vigilance humaine.

Contrôle des accès : la première barrière de sécurité

Le contrôle d'entrée doit être adapté à votre organisation :

- Clés, badges, digicodes, interphones,
- Gestion des droits d'accès (création, désactivation, suivi),
- Accès différenciés selon les zones (bureaux, stockage, données sensibles).

Une porte mal verrouillée ou un badge non désactivé après un départ peut suffire à créer un risque majeur.

Protéger les zones sensibles

Certaines zones nécessitent une vigilance accrue :

- Bureaux contenant du matériel informatique ou des documents confidentiels,
- Zones d'encaissement, ateliers, stocks à forte valeur, archives et données personnelles (RGPD).
- Armoire sécurisée, serrure renforcée, contrôle d'accès restreint : des mesures simples peuvent limiter fortement les risques.

Gestion des visiteurs et des prestataires

Toute personne extérieure doit être :

- Identifiée,
- Enregistrée (registre visiteurs),
- Accompagnée ou autorisée formellement.

👉 Un visiteur non encadré peut représenter un risque sans même en avoir conscience.

Prévenir les agressions et incivilités

Certains métiers exposent davantage aux tensions (accueil, santé, commerce, administrations).

Prévoir :

- Un espace d'accueil sécurisé,
- Des moyens d'alerte,
- Une procédure claire en cas de comportement agressif,
- L'analyse systématique après incident (mise à jour DUERP).

Références juridiques

- Code du travail – Articles L.4121-1 à L.4121-5 : obligation générale de sécurité.
- Code pénal – Articles 221-6 et 222-33-2 : responsabilité en cas d'agression ou mise en danger.
- RGPD (UE 2016/679) : obligation de protéger les accès aux données personnelles.
- Jurisprudence constante : responsabilité de l'employeur engagée en cas d'agression sur site faute de mesures suffisantes.

POINTS CLES A RETENIR

- La sûreté protège vos salariés, vos biens et votre activité.
- Le contrôle des accès doit être géré et mis à jour régulièrement.
- Les visiteurs doivent faire l'objet d'un accueil structuré.
- Les zones sensibles doivent être identifiées et sécurisées.
- Les risques liés à la malveillance doivent figurer dans le DUERP.

LE CONSEIL AF SST 56

Mettez-vous dans la peau d'une personne extérieure pendant quelques minutes.

Faites le tour de votre site et posez-vous la question :

➡ "Qu'est-ce qui pourrait être accessible facilement... et qui ne devrait pas l'être ?"

Cette démarche simple révèle souvent des failles importantes et permet de lancer des actions rapides, efficaces et peu coûteuses.

L'article du mois prochain :

Bilan prévention & plan d'actions 2026

👉 ActusSST 56, c'est aussi votre actu !

Envie de voir un thème abordé ? Envoyez vos suggestions à AF SST 56.

Pour nous contacter :

