



Restreignez l'accès aux locaux

Portes et armoires informatiques verrouillées, accès par badge



Déployez des alarmes anti-intrusion fiables

Tests réguliers, maintenance planifiée.



Protégez les clés et les codes d'alarme

Stockage sécurisé, traçabilité des emprunts, changement immédiat en cas de doute.



Gérez strictement les habilitations de la salle serveur

Liste à jour et revue périodique.



Encadrez l'accès des visiteurs

Hors accueil : accompagnement, identification et enregistrement.

Procédure salle serveur : [Modèle de procédure de gestion des visiteurs dans la salle serveur](#)



Prévoir une procédure en cas d'urgence hors heures ouvrables

Référent habilité, accès hors heures limités, même pour un prestataire régulier.



Ce qu'il ne faut pas faire

- Négliger la climatisation et les onduleurs
- Laisser les écrans ou les documents visibles
- Laisser un visiteur sans accompagnement
- Partager clés, codes ou badges
- Connecter un équipement non autorisé



**Centre
Régional de Ressources
en Cybersécurité**



+ d'informations sur
www.securnes.fr

Contact :
contact@securnes.fr

