5. CONTENU DE LA POLITQUE

5.1 Zonage des zones

5.1.1 Classification des zones

Type de zone	Accès autorisé	Moyens de contrôle	Exigences spécifique
Zone publique	Toute personne	Surveillance visuelle	• Libre circulation • Signalétique d'orientation
Zone restreinte	Collaborateur, prestataires identifiés	Badge nominatif	• Badge requis • Accompagnement obligatoire pour les visiteurs.
Zone hautement sécurisé	Collaborateur strictement autorisé	Badge nominatif + Code ou biométrie	• Double authentification • Vidéosurveillance • Accès limité

5.2 Contrôles d'accès

5.2.1 Gestion des accès visiteurs

- L'identité des visiteurs doit être authentifiée par un moyen d'identification officiel (Carte d'identité nationale, passeport, etc. La carte ne doit en aucun cas être copiée ni conservée ;
- Le port d'un badge visiteur est obligatoire pendant toute la durée de la visite.
- Les visiteurs doivent être systématiquement escortés par un personnel autorisé.
- Un registre des visiteurs doit être maintenu et comporter le nom et prénom, les trois derniers chiffres du numéro de la carte d'identité, la date et l'heure d'entrée et de sortie, ainsi que l'objet de la visite.

5.2.2 Gestion des accès Collaborateur

- Le contrôle d'accès physique aux locaux de l'organisation doit être assuré par des moyens sécurisés, tel que l'utilisation de badges ou de dispositifs biométriques (empreinte digitale ou reconnaissance faciale) ;

- Les accès sont accordés sur la base des besoins professionnels et révoqués immédiatement en cas de changement de fonction ou de départ.
- L'accès est accordé via badge nominatif, dont la couleur diffère selon le profil (Visiteur, employé, prestataire, stagiaire).

5.3 Sécurité physique

5.3.1 Localisation des installations sensibles

- Les installations critiques (salles serveurs, bureaux RH, etc.) doivent être physiquement isolées, inaccessibles au public et protégées contre les accès non autorisés.
- Les bureaux doivent rester discrets : absence d'enseignes signalant la fonction critique, tant à l'extérieur qu'à l'intérieur.

5.3.2 Vidéosurveillance

- Des dispositifs de vidéosurveillance doivent être installés dans toutes les zones critiques.
- Les caméras doivent couvrir les points d'entrée/sortie, couloirs principaux et zones de haute sécurité.
- Les enregistrements doivent être stockés dans des systèmes sécurisés et accessibles uniquement par des personnes autorisées.
- Un entretien régulier et des tests de bon fonctionnement des équipements de vidéosurveillance sont obligatoires.

5.3.5 Emplacement et protection du matériel

- Le matériel informatique sensible (serveur, équipements réseau, dispositifs de stockage) doit être protégé contre tout accès physique non autorisé.
- L'équipement ne doit pas être placé sous les fenêtres ni à proximité de sources de chaleur ou d'humidité.

5.3.6 Service supports et Sécurité du câblage « dans le plan d'action nous avons dit qu'il nécessité de visite sur terrain »

- Les conduites électriques, de données et de refroidissement doivent être protégées contre le sabotage ou le vol de données, en utilisant des chemins de câbles fermés et verrouillés.
- Les alimentations doivent être redondées (onduleurs et groupes électrogènes) et vérifiées selon un planning défini ;
- Les points d'accès réseau non utilisés doivent être désactivés ou physiquement obstrués.

5.3.7 Maintenance préventive des équipements

- Un plan de maintenance préventive documenté doit être établir pour tous les équipements de sécurité ;
- Ce programme doit inclure :
  - La périodicité (trimestrielle, semestrielle ou annuelle selon les équipements), ;
  - Les opérateurs responsables (interne ou sous-traitants)
  - Un registre des interventions, horodaté et signé
- Toute panne détectée doit être corrigée immédiatement, avec un rapport de rétablissement.

6. CONFORMITE

Toute personne qui enfreint cette politique peut faire l'objet de mesures disciplinaires, voire à des poursuites judiciaires, conformément aux règles internes et aux législations en vigueur.

7. SUIVI ET REVISION

Cette politique doit être réexaminée annuellement après son entrée en vigueur ou lorsqu'il y a des changements importants susceptibles d'impacter les périmètres de sécurité physique.