Procédures de sécurité physique - Neo Financia

Version: 1.0
Date: 21 avril 2025
Classification: INTERNE
Référence: PROC-SEC-PHYS-2025-V1.0

Table des matières

Introduction générale

Objectif du document

Ce document définit les procédures opérationnelles de sécurité physique pour les infrastructures critiques de Neo Financia. Il traduit les principes énoncés dans la Politique de Sécurité des Systèmes d'Information (PSSI-NFQ-2025-V1.0) en instructions pratiques et applicables au quotidien.

Champ d'application

Ces procédures s'appliquent à l'ensemble des sites de Neo Financia (Paris, Lyon, Londres) et concernent tous les collaborateurs, visiteurs et prestataires. Elles couvrent principalement la sécurité des bureaux, l'infrastructure technique locale et le contrôle d'accès.

Révision et mise à jour

Ces procédures font l'objet d'une revue annuelle sous la responsabilité du RSSI. Toute modification substantielle doit être validée par le Comité de Sécurité (COSEC).

Procédures pour le site de Paris (Siège social)

1. Introduction et cadre

1.1 Objectif spécifique

Ces procédures définissent les règles opérationnelles de protection physique applicables au siège social de Neo Financia à Paris. Elles établissent les mesures de sécurité visant à protéger les actifs, les personnes et les informations contre les menaces liées à l'accès physique non autorisé.

1.2 Portée d'application

Ces procédures couvrent :

- Les accès au bâtiment
- La sécurité des étages et zones spécifiques
- La gestion des visiteurs et prestataires

- La surveillance et la détection d'intrusion
- Les interventions en cas d'incident

1.3 Références

- Politique de Sécurité des Systèmes d'Information (PSSI-NFQ-2025-V1.0)
- Norme ISO 27001:2022
- Plan d'évacuation du bâtiment
- Contrat avec le prestataire de sécurité

1.4 Responsabilités

Fonction	Responsabilités
Responsable Sécurité Physique (RSP)	Coordination générale des dispositifs de sécurité physique
Société de sécurité externalisée	Surveillance 24/7, contrôle des accès, rondes, gestion des incidents
Responsable des Services Généraux	Maintenance des infrastructures et équipements de sécurité
RSSI	Validation des procédures, coordination avec la sécurité logique
Ressources Humaines	Gestion des badges, droits d'accès des collaborateurs

2. Classification et zonage de sécurité

2.1 Définition des zones de sécurité

Le siège social est divisé en zones de sécurité conformément à la PSSI :

Zone	Classification	Description	Exemple au siège de Paris
Z0	Zone publique	Accès libre sans contrôle	Hall d'entrée, accueil
Z1	Zone contrôlée	Accès général pour le personnel	Espaces de bureaux standards, cafétéria
Z2	Zone restreinte	Accès limité aux personnels autorisés	Bureaux de la direction, salles de développement
Z3	Zone sécurisée	Accès très limité avec double contrôle	Salle COMEX, salle sécurité
Z4	Zone critique	Accès hautement restreint	Salle serveurs locale, salle coffre

2.2 Plan de zonage du siège de Paris

- **Rez-de-chaussée** : Principalement Z0 (accueil) et Z1 (espaces communs)
- **Étages 1-7** : Principalement Z1 (bureaux standards) avec quelques zones Z2
- **8ème étage** : Direction, classification Z2 et Z3
- **Sous-sols** : Infrastructure IT (Z3 et Z4), locaux techniques (Z2)

2.3 Signalisation des zones

Chaque zone de sécurité doit être clairement identifiée par une signalétique appropriée :

- Signalisation visuelle à l'entrée de chaque zone
- Code couleur associé à chaque niveau de sécurité
- Affichage des restrictions d'accès

3. Procédures de contrôle d'accès

3.1 Système de contrôle d'accès

Le système de contrôle d'accès est basé sur des badges électroniques avec les caractéristiques suivantes :

- Badges RFID personnalisés pour tout le personnel
- Lecteurs de badges à tous les points d'accès entre zones
- Contrôles additionnels (code PIN) pour les zones Z3 et Z4
- Verrouillage automatique de toutes les portes de séparation entre zones

3.2 Attribution des droits d'accès

Profil	Processus d'attribution	Validation requise
Collaborateur standard	Droits Z0, Z1 par défaut	Responsable RH
Collaborateur service sensible	Droits Z2 pour son périmètre	Responsable hiérarchique + RSSI
Équipe de sécurité	Droits Z0-Z3	RSSI
Administrateurs systèmes	Droits Z0-Z3, Z4 sur demande	RSSI + DSI
Direction générale	Droits Z0-Z3	Directeur Général

3.3 Procédure de création et remise des badges

1. Demande initiale validée par le responsable hiérarchique
2. Création du badge par les RH avec photo d'identité
3. Configuration des droits d'accès dans le système
4. Remise du badge en main propre contre signature
5. Formation aux règles de sécurité physique

3.4 Procédure de révocation des accès

1. Notification immédiate aux équipes sécurité en cas de départ/changement
2. Désactivation du badge dans le système (délai maximal : 4h après notification)
3. Récupération physique du badge à la sortie définitive
4. Journalisation de la désactivation et de la récupération

3.5 Règles d'utilisation des badges

- Port visible du badge obligatoire dans les locaux
- Interdiction formelle de prêter son badge
- Obligation de signaler immédiatement la perte ou le vol d'un badge
- Utilisation individuelle des lecteurs (anti-tailgating)
- Verrouillage des postes de travail en cas d'absence

4. Gestion des visiteurs et prestataires

4.1 Procédure d'accueil des visiteurs

1. Pré-enregistrement obligatoire sur le portail visiteurs (24h à l'avance)
2. Validation par l'hôte interne
3. Présentation d'une pièce d'identité à l'arrivée
4. Enregistrement dans le système de gestion des visiteurs
5. Remise d'un badge temporaire avec droits limités
6. Accompagnement permanent par l'hôte dans les zones autorisées
7. Restitution du badge à la sortie et signature du registre

4.2 Accès des prestataires réguliers

1. Dossier d'habilitation complet avec vérification d'antécédents
2. Formation obligatoire aux procédures de sécurité
3. Attribution d'un badge nominatif à durée limitée
4. Droits d'accès strictement limités aux zones d'intervention
5. Journalisation renforcée des accès
6. Revue trimestrielle des habilitations

4.3 Interventions exceptionnelles

1. Demande formelle 48h à l'avance (sauf urgence)
2. Double validation (responsable zone + sécurité)
3. Accompagnement obligatoire par un responsable interne
4. Badge temporaire avec restrictions horaires
5. Compte-rendu d'intervention obligatoire

5. Surveillance et détection d'intrusion

5.1 Système de vidéosurveillance

- Caméras couvrant tous les points d'accès extérieurs et interzones
- Enregistrement continu 24/7
- Conservation des images pendant 30 jours (90 jours pour zones Z3-Z4)
- Consultation des enregistrements soumise à procédure d'autorisation
- Affichage des avis légaux d'information sur la vidéosurveillance

5.2 Système de détection d'intrusion

- Détecteurs volumétriques dans toutes les zones Z2 à Z4
- Contacts d'ouverture sur toutes les issues et accès critiques
- Détecteurs de bris de glace sur les fenêtres accessibles
- Système d'alarme relié au poste de sécurité 24/7
- Tests hebdomadaires du système d'alarme

5.3 Procédure de surveillance

- Poste de sécurité central opérationnel 24/7
- Minimum de 2 agents de sécurité présents en permanence
- Monitoring continu des systèmes de contrôle d'accès et d'alarme
- Rondes physiques programmées (toutes les 2h) et aléatoires
- Journal de sécurité tenu à jour en temps réel

5.4 Réponse aux alertes

1. Évaluation initiale de l'alerte par l'agent de sécurité
2. Vérification via le système de vidéosurveillance
3. Intervention sur site si nécessaire

4. Escalade selon la gravité (responsable sécurité, forces de l'ordre)
5. Documentation complète de l'incident et des mesures prises

6. Sécurité environnementale

6.1 Alimentation électrique

- Onduleurs couvrant tous les équipements critiques
- Groupe électrogène avec démarrage automatique
- Tests mensuels du groupe électrogène
- Contrat de maintenance préventive trimestrielle
- Procédure de basculement manuel en cas de défaillance

6.2 Climatisation et contrôles environnementaux

- Systèmes HVAC redondants pour les zones techniques
- Surveillance 24/7 de la température et de l'humidité (18-27°C, 40-60%)
- Alertes automatiques en cas de dépassement des seuils
- Intervention d'urgence sous 4h en cas de défaillance

6.3 Protection incendie

- Détection précoce dans toutes les zones
- Extinction automatique adaptée par zone
- Signalisation et éclairage de sécurité
- Exercices d'évacuation semestriels
- Formation des équipes de première intervention

6.4 Protection contre les dégâts des eaux

- Détecteurs de fuite dans les zones sensibles
- Surélévation des équipements critiques
- Procédure d'intervention d'urgence en cas de fuite

7. Protection des équipements

7.1 Sécurisation des actifs physiques

- Inventaire complet des équipements critiques
- Fixation anti-vol pour les équipements sensibles
- Armoires sécurisées pour le stockage des équipements mobiles
- Contrôles périodiques d'inventaire (mensuel pour actifs critiques)

7.2 Maintenance des équipements

- Planification anticipée des interventions
- Validation préalable par le responsable sécurité
- Accompagnement par un collaborateur habilité
- Journalisation détaillée des opérations réalisées
- Vérification post-intervention

7.3 Mise au rebut sécurisée

1. Autorisation formelle du RSSI
2. Effacement sécurisé des supports de stockage
3. Destruction physique si nécessaire
4. Certificat de destruction/recyclage
5. Mise à jour de l'inventaire

8. Procédures d'urgence

8.1 Réponse aux intrusions

1. Détection de l'intrusion (alarme, vidéosurveillance, signalement)
2. Confinement immédiat des zones critiques
3. Évaluation rapide de la situation par l'agent de sécurité
4. Notification aux responsables selon la gravité
5. Intervention des forces de l'ordre si nécessaire
6. Préservation des preuves
7. Rapport d'incident complet

8.2 Évacuation d'urgence

1. Déclenchement de l'alarme d'évacuation
2. Mise en sécurité des zones critiques (verrouillage)
3. Évacuation guidée par les équipiers d'évacuation
4. Rassemblement aux points de regroupement
5. Comptage du personnel évacué
6. Coordination avec les services d'urgence
7. Autorisation de retour après sécurisation

8.3 Communication de crise

- Liste de contacts d'urgence tenue à jour
- Chaîne d'escalade clairement définie
- Moyens de communication alternatifs
- Modèles de messages préparés
- Désignation des porte-paroles autorisés

9. Vérification et amélioration continue

9.1 Audits de sécurité physique

- Audit interne trimestriel
- Audit externe annuel
- Tests d'intrusion physique annuels
- Revue des incidents et presqu'accidents

9.2 Indicateurs de performance

- Taux de couverture des contrôles d'accès
- Délai moyen de traitement des incidents
- Taux de disponibilité des systèmes de sécurité
- Taux de conformité aux procédures

9.3 Revue des procédures

- Mise à jour annuelle systématique
- Révision immédiate après incident majeur
- Intégration des retours d'expérience
- Communication des modifications aux parties prenantes

Procédures pour le site de Lyon

1. Introduction et cadre

1.1 Objectif spécifique

Ces procédures définissent les règles opérationnelles de sécurité physique applicables au site de Neo Financia à Lyon. Elles établissent les mesures visant à protéger les actifs, les personnes et les informations dans un contexte de bureaux secondaires.

1.2 Portée d'application

Ces procédures s'appliquent à l'ensemble du site de Lyon, incluant tous les collaborateurs, visiteurs et prestataires. Elles tiennent compte des spécificités d'un site de taille moyenne.

1.3 Références

- Politique de Sécurité des Systèmes d'Information (PSSI-NFQ-2025-V1.0)
- Norme ISO 27001:2022
- Plan d'évacuation du bâtiment de Lyon
- Contrat avec le prestataire de sécurité

1.4 Responsabilités

Fonction	Responsabilités
Responsable du site de Lyon	Responsabilité globale de la sécurité du site
Société de sécurité externalisée	Surveillance 24/7, contrôle des accès, rondes, gestion des incidents
Correspondant sécurité local	Relais du RSSI sur le site, coordination des actions de sécurité
Services généraux Lyon	Maintenance des infrastructures et équipements de sécurité

2. Classification et zonage de sécurité

2.1 Définition des zones de sécurité

Le site de Lyon applique le même principe de zonage que le siège social :

Zone	Classification	Description	Exemple sur le site de Lyon
Z0	Zone publique	Accès libre sans contrôle	Hall d'entrée, accueil
Z1	Zone contrôlée	Accès général pour le personnel	Espaces de bureaux standards, cafétéria
Z2	Zone restreinte	Accès limité aux personnels autorisés	Bureaux des responsables, salles projet
Z3	Zone sécurisée	Accès très limité avec double contrôle	Salle serveurs locale

2.2 Plan de zonage du site de Lyon

- **Rez-de-chaussée** : Principalement Z0 (accueil) et Z1 (espaces communs)
- **1er étage** : Principalement Z1 (bureaux standards) avec quelques zones Z2
- **2ème étage** : Zones Z1 et Z2 (bureaux des responsables)
- **Sous-sol** : Infrastructure IT (Z3), locaux techniques (Z2)

2.3 Signalisation des zones

Signalétique identique à celle du siège de Paris pour garantir la cohérence du dispositif.

3. Procédures de contrôle d'accès

3.1 Système de contrôle d'accès

- Système de badges électroniques compatible avec celui du siège
- Lecteurs de badges à tous les points d'accès entre zones
- Synchronisation quotidienne avec le système central

3.2 Attribution des droits d'accès

Processus similaire au siège de Paris, avec validation par le responsable du site de Lyon.

3.3 Procédure spécifique pour les visiteurs du siège de Paris

1. Notification préalable au correspondant sécurité local
2. Validation des droits d'accès temporaires sur le site de Lyon
3. Procédure d'accueil standard
4. Accompagnement adapté selon le niveau d'habilitation existant

4. Gestion des visiteurs et prestataires

4.1 Procédure d'accueil des visiteurs

Similaire à celle du siège, avec adaptation aux spécificités locales :

- Pré-enregistrement obligatoire avec préavis de 24h
- Accueil centralisé au rez-de-chaussée
- Accompagnement permanent dans les zones autorisées

4.2 Accès des prestataires locaux

1. Validation préalable par le responsable du site
2. Vérification d'identité et création d'un dossier d'habilitation
3. Formation aux règles de sécurité spécifiques au site
4. Attribution d'un badge temporaire avec droits limités
5. Supervision par un référent interne

5. Surveillance et détection d'intrusion

5.1 Dispositif de surveillance

- Caméras de surveillance aux points d'accès principaux et zones sensibles
- Système d'alarme relié au poste de sécurité du site
- Télésurveillance avec le siège de Paris en dehors des heures de bureau
- Rondes régulières par les agents de sécurité

5.2 Gestion des alertes

1. Évaluation initiale par l'agent de sécurité sur place
2. Coordination avec le centre de sécurité du siège si nécessaire
3. Intervention selon protocole défini
4. Documentation et reporting systématique

6. Procédures spécifiques au site de Lyon

6.1 Coordination avec le siège

- Réunion mensuelle de coordination sécurité
- Reporting hebdomadaire des incidents et accès
- Échange d'information sur les visiteurs inter-sites
- Plan d'intervention commun en cas de crise majeure

6.2 Continuité de service

- Procédures de repli vers le siège en cas d'indisponibilité du site
- Dispositifs de connexion sécurisée de secours
- Tests périodiques des procédures de basculement

7. Vérification et amélioration continue

- Audit interne semestriel
- Revue annuelle des procédures
- Exercices conjoints avec le siège

Procédures pour le site de Londres

1. Introduction et cadre

1.1 Objectif spécifique

Ces procédures définissent les règles opérationnelles de sécurité physique applicables au site de Neo Financia à Londres. Elles tiennent compte du contexte spécifique d'un bâtiment partagé avec d'autres entreprises et des exigences réglementaires britanniques.

1.2 Portée d'application

Ces procédures s'appliquent aux espaces occupés par Neo Financia au sein du business center de Londres, incluant tous les collaborateurs, visiteurs et prestataires.

1.3 Références

- Politique de Sécurité des Systèmes d'Information (PSSI-NFQ-2025-V1.0)
- Norme ISO 27001:2022
- Règlement intérieur du business center
- Contrats avec les prestataires de sécurité
- Réglementations britanniques applicables

1.4 Responsabilités

Fonction	Responsabilités
Responsable du site de Londres	Responsabilité globale de la sécurité des espaces Neo Financia
Security Manager UK	Correspondant sécurité local, coordination avec le RSSI
Sécurité du business center	Sécurité périmétrique, accès au bâtiment
Prestataire de sécurité Neo Financia	Surveillance spécifique des espaces Neo Financia

2. Coordination avec la sécurité du bâtiment

2.1 Périmètres de responsabilité

Zone	Responsable sécurité	Mesures appliquées
Entrée du bâtiment et parties	Business center	Procédures du business

communes		center
Étages partagés - espaces communs	Business center	Procédures du business center
Espaces Neo Financia	Neo Financia	Procédures Neo Financia
Points d'interface	Responsabilité partagée	Procédures coordonnées

2.2 Protocole de coordination

- Réunion mensuelle avec le service de sécurité du business center
- Échange d'information sur les visiteurs attendus
- Procédure d'alerte commune en cas d'incident
- Exercices conjoints d'évacuation

2.3 Gestion des accès au bâtiment

1. Enregistrement de tous les collaborateurs Neo Financia auprès du business center
2. Réception et validation des badges d'accès bâtiment
3. Processus de notification pour les visiteurs (double validation)
4. Procédure de coordination pour les interventions après heures

3. Sécurité spécifique des espaces Neo Financia

3.1 Zonage de sécurité

Les espaces Neo Financia sont organisés selon le même principe de zonage que les autres sites, avec adaptation au contexte du bâtiment partagé :

Zone	Description	Application à Londres
Z1	Zone contrôlée	Espaces de bureaux généraux Neo Financia
Z2	Zone restreinte	Bureaux de direction, salles de réunion confidentielles
Z3	Zone sécurisée	Local technique, stockage données sensibles

3.2 Contrôles d'accès supplémentaires

- Système de contrôle d'accès indépendant pour les espaces Neo Financia
- Double validation pour l'accès aux zones Neo Financia (badge bâtiment + badge Neo Financia)
- Verrouillage automatique de toutes les portes d'accès aux espaces Neo Financia
- Système de surveillance spécifique aux heures non-ouvrées

3.3 Procédures pour les heures non ouvrables

1. Notification préalable obligatoire au business center (24h à l'avance)
2. Validation par le responsable du site de Londres
3. Enregistrement à l'entrée du bâtiment
4. Accès limité aux zones autorisées
5. Rapport de présence en fin d'intervention

4. Gestion des visiteurs et prestataires

4.1 Procédure d'accueil des visiteurs

1. Pré-enregistrement sur le système Neo Financia (48h à l'avance)

2. Notification au service d'accueil du business center (24h à l'avance)
3. Accueil par la réception du bâtiment et vérification d'identité
4. Contact de l'hôte Neo Financia
5. Escorte jusqu'aux espaces Neo Financia
6. Remise d'un badge visiteur spécifique Neo Financia
7. Accompagnement permanent dans les zones Neo Financia
8. Procédure de sortie coordonnée avec le business center

4.2 Accès des prestataires

1. Procédure d'habilitation standard Neo Financia
2. Enregistrement supplémentaire auprès du business center
3. Coordination des interventions techniques avec le gestionnaire du bâtiment
4. Supervision renforcée pour les interventions dans les zones partagées
5. Rapport d'intervention double (Neo Financia et business center si applicable)

5. Conformité aux exigences britanniques

5.1 Adaptations réglementaires

- Documentation bilingue (français/anglais) des procédures de sécurité
- Conformité aux exigences britanniques en matière de surveillance
- Déclarations aux autorités locales pour les systèmes de vidéosurveillance
- Adaptations post-Brexit pour le traitement des données
- Procédures spécifiques en cas d'intervention des autorités britanniques

5.2 Formation spécifique

- Formation adaptée aux spécificités réglementaires britanniques
- Sensibilisation aux différences culturelles et organisationnelles
- Exercices conformes aux standards britanniques
- Documentation conforme aux exigences locales

6. Gestion des incidents spécifique

6.1 Coordination en cas d'incident

1. Évaluation initiale de l'incident (interne ou concernant également le bâtiment)
2. Notification parallèle au SOC Neo Financia et à la sécurité du business center si nécessaire
3. Coordination des interventions selon le périmètre impacté
4. Communication adaptée aux parties prenantes britanniques
5. Documentation conforme aux exigences des deux pays

6.2 Plan d'escalade spécifique

- Points de contact d'urgence identifiés côté business center
- Chaîne d'escalade adaptée au contexte britannique
- Protocole de communication avec les autorités locales
- Coordination avec l'ambassade de France si nécessaire

7. Vérification et amélioration continue

7.1 Audits et contrôles

- Audit interne semestriel
- Participation aux exercices de sécurité du business center
- Évaluation annuelle de la coordination avec le business center
- Tests d'intrusion adaptés au contexte du bâtiment partagé

7.2 Indicateurs spécifiques

- Taux d'incidents liés à l'interface avec le business center
- Efficacité de la coordination en cas d'incident
- Conformité aux exigences britanniques
- Satisfaction des collaborateurs sur le dispositif de sécurité

Annexes

Annexe 1 : Formulaires de référence

- Formulaire de demande d'accès
- Formulaire d'enregistrement des visiteurs
- Checklist d'audit de sécurité physique
- Rapport d'incident type

Annexe 2 : Coordonnées et contacts d'urgence

- Liste des contacts sécurité pour chaque site
- Chaîne d'escalade en cas d'incident
- Contacts des autorités locales
- Prestataires de sécurité et maintenance

Annexe 3 : Plan de formation à la sécurité physique

- Programme d'onboarding sécurité
- Formation aux procédures d'urgence
- Formation des correspondants sécurité
- Calendrier des exercices et simulations