Politique de Sécurité Réseau

Neo Financia

RÉFÉRENCE	PSSI-RÉSEAU-2025-V1.0
CLASSIFICATION	INTERNE
VERSION	1.0
DATE D'APPROBATION	À définir
APPROBATION	Direction Sécurité & COMEX
PROPRIÉTAIRE	RSSI
PÉRIODICITÉ DE RÉVISION	Annuelle

Table des matières

1. Introduction et objectifs

1.1 Contexte

Neo Financia, en tant que néobanque européenne opérant exclusivement via des canaux digitaux, dépend entièrement de la fiabilité et de la sécurité de son infrastructure réseau. Avec 2 millions de clients et 1000 collaborateurs répartis entre Paris, Lyon et Londres, la sécurité de nos réseaux constitue un élément fondamental de notre stratégie de cybersécurité.

Notre modèle d'activité, basé sur une architecture multi-cloud (Azure 70%, OVHcloud 20%, AWS 10%) et incluant des interconnexions avec nos partenaires fintech (Mangopay, Lemonway), nécessite une approche rigoureuse et structurée de la sécurité réseau.

1.2 Objectifs de la politique

Cette politique de sécurité réseau vise à :

- Établir un cadre cohérent pour la conception, l'implémentation et la gestion de notre infrastructure réseau
- Définir les principes de segmentation adaptés à notre contexte de néobanque
- Garantir la protection des données sensibles et des transactions financières

- Assurer la conformité aux exigences réglementaires applicables (DORA, NIS2, RGPD, DSP2)
- Maintenir un équilibre entre sécurité, disponibilité et performance
- Définir les responsabilités et les processus de gouvernance liés à la sécurité réseau
- Fournir des bases solides pour la détection et la réponse aux incidents réseau

1.3 Portée et applicabilité

Cette politique s'applique à :

- L'ensemble des infrastructures réseau de Neo Financia, qu'elles soient physiques ou virtuelles
- Tous les sites de l'entreprise (Paris, Lyon, Londres)
- Les environnements cloud (Azure, OVHcloud, AWS)
- Les interconnexions avec les partenaires et prestataires
- Tous les équipements connectés au réseau de Neo Financia
- L'ensemble des collaborateurs, prestataires et partenaires utilisant le réseau

1.4 Principes directeurs

Les principes fondamentaux guidant notre approche de la sécurité réseau sont :

- **Défense en profondeur** : Superposition de multiples mécanismes de protection pour minimiser l'impact d'une défaillance
- **Moindre privilège** : Limitation des flux réseau au strict nécessaire
- **Segmentation** : Cloisonnement des environnements et des données selon leur niveau de sensibilité
- **Zero Trust** : Vérification systématique des accès, quelle que soit la provenance
- **Visibilité** : Surveillance complète des flux et détection des anomalies
- **Résilience** : Conception pour maintenir les services essentiels même en cas d'incident
- **Automatisation** : Standardisation et automatisation des configurations pour réduire les erreurs humaines

2. Gouvernance et responsabilités

2.1 Organisation et rôles

La gouvernance de la sécurité réseau s'inscrit dans le cadre global de gouvernance de la sécurité de Neo Financia :

Fonction	Responsabilités liées à la sécurité réseau
RSSI	- Définition de la stratégie de sécurité réseau - Validation des architectures - Supervision des audits et tests - Reporting au COMEX et au Comité des Risques
Équipe Réseau et Sécurité	- Administration des équipements réseau - Gestion des accès réseau et firewall - Protection périmétrique - Surveillance du réseau
DSI	- Mise en œuvre des mesures de sécurité - Gestion de l'infrastructure réseau

	- Application des correctifs
Cloud Security Team	- Sécurisation des environnements cloud - Configuration des réseaux virtuels - Gestion des interconnexions cloud
Correspondants Sécurité	- Relais de la politique dans leurs directions - Remontée des besoins spécifiques
Utilisateurs	- Respect des règles d'utilisation du réseau - Signalement des anomalies

2.2 Processus de gouvernance

Instance	Fréquence	Missions
Comité de Sécurité (COSEC)	Mensuelle	- Suivi des indicateurs de sécurité réseau - Revue des incidents et vulnérabilités - Validation des changements majeurs
Comité d'Architecture	Bimensuelle	- Validation des évolutions d'architecture réseau - Revue des nouvelles technologies - Alignement avec la stratégie technique
Revue Technique Sécurité	Hebdomadaire	- Suivi opérationnel des contrôles réseau - Traitement des alertes et incidents - Planification des actions correctives

2.3 Gestion des exceptions

Toute exception à cette politique doit suivre un processus formel :

1. Soumission d'une demande documentée incluant :
    - Justification business
    - Analyse de risque
    - Mesures compensatoires
    - Durée prévue
2. Validation selon le niveau de risque :
    - Risque modéré : Approbation RSSI
    - Risque élevé : Approbation COSEC
    - Risque critique : Approbation Comité des Risques
3. Documentation et suivi des exceptions dans un registre centralisé
4. Revue périodique des exceptions accordées

Les exceptions dont la durée dépasse 6 mois doivent faire l'objet d'un plan de retour à la conformité.

3. Architecture réseau sécurisée

3.1 Principes d'architecture

L'architecture réseau de Neo Financia repose sur les principes de défense en profondeur et de segmentation multiniveau :

- Segmentation en zones de sécurité distinctes avec contrôles aux frontières
- Filtrage restrictif des flux entre zones ("default deny")
- Architecture redondante pour garantir la disponibilité
- Séparation des environnements (production, pré-production, test, développement)
- Protection périmétrique multicouche
- Cloisonnement des services administratifs

3.2 Modèle de zonage

Notre architecture réseau est structurée en zones de sécurité distinctes :

Zone	Description	Niveau de protection	Usage
Internet / Externe	Réseaux publics non maîtrisés	Protection DDoS, surveillance avancée	Accès clients et partenaires
DMZ externe	Zone d'exposition contrôlée	WAF, IPS, filtrage applicatif	Services exposés (web, API Gateway)
Zone API	Couche d'orchestration des API	API Gateway, authentification forte	Exposition contrôlée des services internes
Zone applicative	Hébergement des applications métier	Micro-segmentation, flow control	Applications bancaires, services clients
Zone données	Stockage et traitement des données	Isolation stricte, contrôles d'accès renforcés	Bases de données, data lakes
Zone d'administration	Gestion des infrastructures	Bastions, PAM, surveillance renforcée	Administration technique
Zone utilisateur	Réseaux des postes de travail	NAC, filtrage des accès aux ressources	Collaborateurs internes
Zone partenaires	Interconnexions sécurisées	VPN dédiés, filtrage spécifique	Connexions avec Mangopay, Lemonway, etc.

3.3 Topologie des sites

Neo Financia dispose de trois sites principaux interconnectés :

Site	Rôle	Infrastructure
Paris (Siège)	Site principal	Équipements réseau redondants, connexion Internet principale, datacenter primaire
Lyon	Site	Infrastructure réseau redondante, connexion Internet

	secondaire	secondaire, capacité de reprise
Londres	Site britannique	Infrastructure locale, connexion VPN sécurisée avec le siège, pare-feu dédié

Les sites sont interconnectés via des liaisons sécurisées redondantes avec chiffrement de bout en bout.

3.4 Architecture Cloud

Notre infrastructure cloud suit une approche hybride multi-cloud :

- **Azure (70%)** : Hébergement des applications critiques et core banking
  - Architecture en Virtual Networks (VNets) avec segmentation
  - ExpressRoute pour les connexions privées sécurisées
  - NSGs (Network Security Groups) et Azure Firewall
- **OVHcloud (20%)** : Services non-critiques et applications secondaires
  - vRack privé
  - Pare-feu virtuel
  - Connexion sécurisée vers Azure
- **AWS (10%)** : Services spécifiques et capacité de débordement
  - VPCs (Virtual Private Clouds) dédiés
  - AWS Transit Gateway pour l'interconnexion
  - Security Groups et Network ACLs

3.5 Diagramme d'architecture de référence

[Insérer ici un diagramme d'architecture simplifié]

4. Politique de segmentation

4.1 Principes de segmentation

La segmentation réseau est un élément fondamental de notre stratégie de défense en profondeur. Elle vise à :

- Limiter la propagation des menaces en cas de compromission
- Protéger les données sensibles en isolant les systèmes qui les traitent
- Appliquer un contrôle granulaire des flux autorisés
- Faciliter la détection des comportements anormaux
- Répondre aux exigences réglementaires

4.2 Technologies de segmentation

Neo Financia s'appuie principalement sur deux technologies complémentaires pour implémenter la segmentation réseau :

1. **Software-Defined Networking (SDN)** :
   - Séparation logique programmable des environnements
   - Flexibilité dans la définition des périmètres de sécurité
   - Adaptation dynamique aux évolutions des besoins
   - Centralisation des politiques de sécurité réseau

- Automatisation des déploiements et modifications

2. **VLANs (Virtual Local Area Networks)** :
   - Isolation du trafic entre différents groupes fonctionnels
   - Limitation du domaine de broadcast
   - Séparation des environnements de production et non-production
   - Contrôle d'accès entre segments logiques
   - Déploiement sur l'infrastructure physique existante

4.3 Niveaux de segmentation

Neo Financia implémente plusieurs niveaux de segmentation complémentaires :

1. **Segmentation physique** : Séparation des infrastructures critiques
2. **Segmentation logique** : VLANs, sous-réseaux et zones de sécurité basées sur SDN
3. **Micro-segmentation** : Contrôles au niveau des charges de travail, particulièrement dans les environnements cloud
4. **Segmentation applicative** : Filtrage au niveau des flux applicatifs et APIs

4.4 Modèle de segmentation par classification

La segmentation est alignée avec la classification des données, avec une protection renforcée pour les données des transactions financières et les documents clients :

Classification	Types de données	Niveau de segmentation	Contrôles requis
P3 - Critique	Données de transactions financières, authentification	Isolation forte	- Environnement dédié avec SDN avancé - Contrôles d'accès multiples avec MFA - Flux restreints, documentés et chiffrés - Surveillance renforcée et analyse comportementale - Micro-segmentation au niveau des workloads - Protection DLP avancée
P2 - Confidentiel	Documents clients, données personnelles	Segmentation forte	- Zone réseau dédiée avec VLANs spécifiques - Flux limités et contrôlés via SDN - Authentification renforcée - Chiffrement en transit - Journalisation exhaustive des accès

			- Inspection profonde du trafic
P1 - Interne	Données administratives, documentation	Segmentation standard	- Séparation des environnements - Contrôles de base - Filtrage des flux externes - VLANs dédiés par service
P0 - Public	Informations marketing, documentation générale	Segmentation minimale	- Séparation de l'Internet - Contrôles d'intégrité - Protection contre les modifications non autorisées

4.4 Règles de filtrage entre zones

Les communications entre zones de sécurité suivent des règles strictes :

- Principe du "Deny All" par défaut
- Autorisation explicite des flux légitimes uniquement
- Documentation obligatoire de la justification business pour chaque règle
- Granularité maximale des règles (source, destination, port, protocole, application)
- Révision périodique de toutes les règles (trimestrielle)
- Suppression des règles temporaires à échéance

4.5 Matrice de flux

[Tableau à compléter avec la matrice détaillée des flux autorisés entre les différentes zones]

4.6 Micro-segmentation cloud

Dans les environnements cloud, Neo Financia applique une micro-segmentation avancée :

- Isolation au niveau des workloads et conteneurs
- Politique de sécurité basée sur l'identité des applications
- Contrôles adaptatifs selon le contexte
- Automatisation des règles via Infrastructure as Code
- Surveillance continue de la conformité des configurations

5. Contrôles de sécurité réseau

5.1 Défense périmétrique

Neo Financia met en œuvre une défense périmétrique multicouche :

- **Protection DDoS** : Service de mitigation DDoS (volumétrique et applicatif)
- **Pare-feu nouvelle génération** : Inspection approfondie du trafic avec analyse applicative

- **WAF (Web Application Firewall)** : Protection des applications web et APIs exposées
- **IPS/IDS** : Détection et prévention des intrusions
- **Filtrage de contenu** : Analyse des flux web sortants et protection contre les malwares
- **Protection de la messagerie** : Filtrage anti-spam, anti-phishing et anti-malware

5.2 Contrôles d'accès réseau

- **NAC (Network Access Control)** : Contrôle des équipements se connectant au réseau
- **802.1X** : Authentification des équipements sur les réseaux filaires et sans fil
- **VLANs** : Séparation logique des différentes catégories d'équipements
- **Gestion des équipements non conformes** : Mise en quarantaine automatique

5.3 Sécurité des communications

Toutes les communications sensibles doivent être chiffrées :

Type de communication	Standard minimum	Exigences complémentaires
Services web externes	TLSv1.2 obligatoire	- Certificate Extended Validation - Certificats renouvelés tous les 12 mois - Certificate Transparency - HSTS avec preloading
Communications internes critiques	TLSv1.2 minimum ou IPsec	- PKI interne avec validation stricte - Authentification mutuelle obligatoire - Rotation des certificats tous les 6 mois
API externes	TLSv1.2 minimum + jeton signé	- Signature des requêtes (JWS) - Validité limitée des jetons (15min max) - Chiffrement de charge utile sensible (JWE)
Connexions avec partenaires	VPN IPsec ou TLS	- Tunnel dédié par partenaire - Authentification par certificat - Monitoring spécifique des tunnels
Interconnexions Cloud	Liens privés chiffrés	- ExpressRoute/Direct Connect chiffré - Isolation des flux par VLAN - Monitoring en temps réel

5.4 Filtrage DNS et protection contre les menaces avancées

- Filtrage DNS pour bloquer les domaines malveillants
- Detection de tunneling DNS
- Analyse des requêtes DNS pour détecter les C&C et exfiltrations

- Protection contre les attaques sur l'infrastructure DNS

5.5 Protection des données en transit

- Chiffrement obligatoire pour toutes les données sensibles en transit
- Protocoles autorisés et interdits clairement définis
- Validation de l'intégrité des données transmises
- Contrôles anti-rejeu pour les communications critiques

6. Gestion des accès réseau

6.1 Accès distants sécurisés

Neo Financia a mis en place une politique de télétravail et accepte l'utilisation d'appareils personnels (BYOD). Pour sécuriser ces accès distants :

Type d'accès	Solution	Contrôles spécifiques	Usage
VPN collaborateurs	VPN SSL avec MFA	- Authentification forte obligatoire - Contrôle de santé du poste - Tunnel intégral ou split tunnel selon profil - Compatible avec appareils personnels (BYOD)	Télétravail, mobilité
VPN administrateurs	VPN dédié sécurisé	- Double authentification - Accès limité aux adresses autorisées - Enregistrement intégral des sessions - Uniquement depuis appareils professionnels	Administration d'urgence
Accès partenaires	API Gateway sécurisée	- Authentification par certificats clients - Filtrage granulaire des opérations autorisées - Monitoring permanent des appels API - Rate limiting adaptatif	Connexion Mangopay, Lemonway
Accès prestataires	Portail d'accès sécurisé	- Authentification dédiée par intervenant - Accès limité temporellement - Surveillance accrue des actions	Maintenance, support

		- Jump servers obligatoires	
Accès BYOD	Solution MDM/MAM	- Conteneurisation des données professionnelles - Politiques de sécurité spécifiques - Capacité d'effacement sélectif - Vérification de conformité	Accès email et applications non critiques

6.2 Sécurité des réseaux sans fil

Neo Financia implémente des contrôles spécifiques pour sécuriser ses réseaux sans fil :

Réseau	Protocole	Authentification	Contrôles supplémentaires
Wi-Fi Corporate	WPA3-Enterprise	802.1X avec EAP-TLS	- Certificats matériels - Intégration avec le NAC - Chiffrement individuel des sessions
Wi-Fi BYOD	WPA3-Enterprise	802.1X avec authentification utilisateur	- Segmentation dédiée - Accès limité aux ressources autorisées - Inspection du trafic sortant
Wi-Fi Invités	WPA3-Personal	Portail captif avec code temporaire	- Isolation complète du SI interne - Sortie Internet filtrée - Limitation de bande passante

6.3 Contrôle des flux entre zones

- Matrice de flux documentée et maintenue à jour
- Validation formelle des changements de règles
- Révision périodique des règles existantes
- Alertes sur les modifications non autorisées

6.4 Accès aux services cloud

- Connexions privées privilégiées (ExpressRoute, Direct Connect, vRack)
- Validation des endpoints exposés
- Restrictions géographiques d'accès quand applicable
- Surveillance renforcée des accès aux services cloud critiques

7. Sécurité des interconnexions

7.1 Interconnexions avec les partenaires fintech

Neo Financia a établi des connexions sécurisées avec ses principaux partenaires fintech principalement via des API sécurisées :

- **Mangopay** : API sécurisée avec authentification mutuelle par certificats, chiffrement TLS 1.3, signatures des transactions
- **Lemonway** : API avec OAuth 2.0, tokens JWT signés, validation d'intégrité des messages
- **Autres partenaires financiers** : API Gateway centralisée avec authentification forte et contrôles unifiés

Chaque API partenaire fait l'objet :

- D'une évaluation de sécurité préalable et d'une homologation formelle
- D'un contrat détaillant les exigences de sécurité des API
- D'une documentation technique complète des contrôles de sécurité
- D'une surveillance spécifique avec alertes sur comportements anormaux
- De tests réguliers de sécurité (tests de pénétration trimestriels)
- D'une vérification continue de conformité au standard OWASP API Security

7.2 Interconnexions inter-sites

Les sites de Neo Financia sont interconnectés via :

- Liaisons dédiées redondantes entre les sites principaux
- Chiffrement de bout en bout des communications
- Surveillance continue des performances et de la sécurité
- Plan de basculement en cas de défaillance

7.3 Interconnexions multi-cloud

Notre approche multi-cloud nécessite des interconnexions sécurisées :

- Architecture hub-and-spoke pour centraliser les contrôles
- Services d'interconnexion cloud dédiés (Azure Virtual WAN, Transit Gateway)
- Contrôles de sécurité uniformes entre clouds
- Traçabilité complète des flux inter-clouds

7.4 Gestion des APIs

La sécurité des APIs est critique pour notre modèle d'affaires et constitue le principal vecteur d'interconnexion avec nos partenaires fintech :

- API Gateway centralisée avec contrôles de sécurité uniformes
- Authentification forte pour toutes les API (OAuth 2.0, mTLS)
- Limitation des débits et quotas par client
- Validation des schémas de requêtes/réponses
- Détection des abus et comportements anormaux
- Chiffrement de bout en bout des données sensibles
- Contrôles spécifiques pour les API exposant des données transactionnelles
- Journalisation exhaustive de toutes les transactions API
- Surveillance en temps réel via le SOC SaaS
- Revue de code obligatoire pour toutes les nouvelles API
- Tests de sécurité automatisés dans le pipeline CI/CD
- Vérification périodique des dépendances et composants tiers

8. Environnements spécifiques

8.1 Environnement de production

L'environnement de production bénéficie des contrôles les plus stricts :

- Isolation complète des autres environnements
- Accès restreint et strictement contrôlé
- Changements soumis à un processus formel de validation
- Surveillance 24/7
- Redondance N+1 minimum

8.2 Environnements de non-production

Les environnements de non-production sont segmentés :

Environnement	Niveau de sécurité	Règles d'accès
Pré-production	Quasi-production	- Séparation stricte de la production - Données réelles anonymisées - Accès contrôlé
Test / Recette	Intermédiaire	- Isolation par projet - Données synthétiques - Accès limité aux équipes concernées
Développement	Standard	- Segmentation par équipe - Pas de données réelles - Restrictions des flux sortants

8.3 Environnements cloud

Chaque environnement cloud dispose de contrôles adaptés, avec des technologies de micro-segmentation spécifiques alignées sur notre PSSI :

- **Azure (70% de notre infrastructure)** :
  - Architecture hub-and-spoke avec Azure Virtual WAN
  - Azure Firewall et NSGs (Network Security Groups)
  - Private Link pour tous les services PaaS
  - Azure Security Center et Azure Sentinel pour la surveillance
  - Micro-segmentation via NSGs avancés et Azure Firewall
  - Application Security Groups pour le regroupement logique
  - Virtual Network Service Endpoints pour l'accès sécurisé aux services
  - Network Watcher pour l'analyse des flux et la vérification des règles
  - Architecture Zero Trust Network Access pour les accès administratifs
- **OVHcloud (20% de notre infrastructure)** :
  - vRack privé avec isolation physique
  - Anti-DDoS natif et protection avancée
  - Pare-feu virtuels distribués et centralisés
  - Réseaux privés isolés avec VLANs dédiés
  - Micro-segmentation via groupes de sécurité
  - Private Network pour les communications inter-services
  - Protection L7 pour les services exposés
  - Load Balancer avec filtrage avancé
- **AWS (10% de notre infrastructure)** :

    - Architecture multi-VPC avec Transit Gateway
    - Security Groups et NACLs avec règles granulaires
    - AWS Shield et WAF pour la protection périmétrique
    - GuardDuty pour la détection des menaces
    - Micro-segmentation via AWS Network Firewall
    - VPC Endpoints pour l'accès sécurisé aux services
    - Resource Access Manager pour le partage contrôlé
    - AWS Control Tower pour la gouvernance globale

8.4 Réseaux d'administration

Les réseaux d'administration font l'objet de mesures de sécurité renforcées :

- Réseau dédié et isolé pour l'administration
- Accès via des jumpbox sécurisés
- Authentification multi-facteurs obligatoire
- Enregistrement complet des sessions
- Surveillance spécifique des activités administratives

9. Surveillance et contrôle

9.1 Monitoring réseau

Neo Financia a déployé un dispositif complet de surveillance réseau :

- Collecte et analyse des flux réseau (NetFlow/IPFIX)
- Détection des anomalies de trafic
- Surveillance de la performance et disponibilité
- Visibilité sur les applications et protocoles
- Corrélation avec les autres sources de sécurité
- Intégration avec la solution SOC SaaS pour analyse avancée
- Tableaux de bord unifiés pour la surveillance multi-cloud

9.2 Détection des intrusions et menaces

- Systèmes IDS/IPS aux points stratégiques du réseau
- NDR (Network Detection and Response) pour l'analyse comportementale
- Honeypots pour la détection précoce
- Alertes sur les tentatives d'accès non autorisés
- Intégration avec le SOC SaaS externalisé pour analyse et réponse
- Règles de détection personnalisées pour les menaces visant le secteur financier
- Intelligence sur les menaces spécifiques aux environnements SDN et VLAN
- Détection avancée des menaces sur les API financières

9.3 Logging et traçabilité

- Journalisation centralisée de tous les événements réseau significatifs
- Conservation des logs selon les exigences réglementaires
- Protection de l'intégrité des logs
- Synchronisation temporelle précise
- Corrélation dans le SIEM

9.4 Indicateurs de performance

Des KPIs sont définis pour mesurer l'efficacité des contrôles réseau :

Indicateur	Objectif	Fréquence de

		mesure
Taux de disponibilité des liaisons critiques	> 99.99%	Temps réel
Délai de détection des incidents réseau	< 15 minutes	Mensuelle
Conformité aux politiques de segmentation	100%	Hebdomadaire
Vulnérabilités réseau non corrigées (critiques)	0	Quotidienne
Précision des alertes de sécurité réseau	> 90%	Mensuelle

10. Procédures opérationnelles

10.1 Gestion des changements réseau

Tous les changements sur l'infrastructure réseau suivent un processus formalisé :

- Classification par niveau d'impact et de risque
- Validation technique et sécurité
- Fenêtres de maintenance planifiées
- Tests préalables et plan de rollback
- Documentation des changements

10.2 Gestion des incidents réseau

En cas d'incident réseau, Neo Financia suit un processus structuré :

1. Détection et qualification
2. Isolation et confinement
3. Investigation et diagnostic
4. Résolution et restauration
5. Documentation et retour d'expérience

Des procédures spécifiques sont définies pour les types d'incidents courants.

10.3 Maintenance et mises à jour

- Planification des mises à jour de firmware et logiciels réseau
- Tests préalables en environnement de pré-production
- Analyse des correctifs de sécurité
- Validation post-déploiement
- Gestion des configurations (backup, versioning)

10.4 Documentation réseau

Une documentation complète et à jour est maintenue :

- Schémas d'architecture réseau
- Inventaire des équipements
- Configuration standard de référence
- Matrice de flux autorisés
- Procédures opérationnelles
- Contacts d'urgence

11. Conformité réglementaire

11.1 Exigences sectorielles

Neo Financia doit se conformer à plusieurs réglementations concernant la sécurité réseau :

Réglementation	Exigences réseau spécifiques	Contrôles mis en place
DORA	Résilience opérationnelle, tests réguliers, gestion des tiers	Architecture redondante, tests de basculement
NIS2	Sécurité des réseaux, notification d'incidents	Défense en profondeur, procédures de réponse
PCI-DSS	Segmentation, contrôle d'accès, surveillance	CDE isolé, pare-feu dédié, logs centralisés
RGPD	Protection des données personnelles	Chiffrement, contrôles d'accès, minimisation des flux
DSP2	Sécurité des paiements et communications	Authentification forte, canaux sécurisés

11.2 Souveraineté des données

En tant qu'institution financière européenne, Neo Financia applique des principes stricts de souveraineté des données conformément au RGPD :

- **Localisation des données** : Les données personnelles et financières des clients sont hébergées exclusivement dans l'Union Européenne
- **Cloisonnement des environnements** : Séparation stricte des données des clients européens et britanniques
- **Contrôle des flux transfrontaliers** : Chiffrement et journalisation de tous les transferts de données entre les sites de Paris/Lyon et Londres
- **Sécurité des API** : Les API exposant des données personnelles disposent de contrôles supplémentaires de conformité RGPD
- **Gestion des consentements** : Architecture réseau supportant la granularité des consentements et facilitant l'exercice des droits
- **Registre des traitements** : Cartographie précise des flux réseau pour tous les traitements impliquant des données personnelles
- **Minimisation des flux** : Limitation des données en transit au strict nécessaire opérationnel

Ces contrôles sont intégrés à l'architecture SDN et s'appliquent à tous les environnements, y compris cloud.

11.2 Contrôles de conformité

- Auto-évaluation trimestrielle de conformité
- Audits internes annuels
- Tests de pénétration externes
- Scans de vulnérabilités mensuels
- Revue annuelle complète de l'architecture

11.3 Gestion des preuves

- Conservation des logs et journaux d'événements
- Documentation des contrôles mis en place
- Résultats des tests et audits
- Suivi des actions correctives
- Rapports de conformité

12. Annexes

12.1 Glossaire

[À compléter avec les termes techniques et leur définition]

12.2 Documentation de référence

- Schémas d'architecture réseau détaillés
- Matrice complète des flux autorisés
- Procédures opérationnelles associées
- Cartographie des risques réseau
- Références aux standards et bonnes pratiques (NIST, ISO, etc.)

12.3 Historique des révisions

Version	Date	Modifications	Auteur	Validation
1.0	xx/xx/2025	Version initiale	RSSI	COMEX