# DIRECTIVE STRATEGIQUE

# 02. MOBILITE

## POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION DU GROUPE LA POSTE

| | |
|---|---|
| **Statut du document** | Validé |
| **Version** | V 1.0 |
| **Date d'enregistrement** | 20/09/2019 |
| **Responsable du document** | DSGG/DCG |

# Table des matières

# 1 Préambule

## 1.1 Objet du document

Cette directive fait partie du référentiel documentaire de la Politique de Sécurité des Systèmes d'Information du Groupe (PSSI-G). Elle décrit les mesures relatives à la mobilité.

Elle doit établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information, en cohérence avec le Cadre Général.

## 1.2 Positionnement dans le cadre de référence

La Sécurité des Systèmes d'Information (SSI) du Groupe La Poste s'inscrit dans un cadre structuré en quatre niveaux :

- **Niveau 1** : *le cadre général*, qui fixe les objectifs, les principes généraux en matière de sécurité des SI et l'organisation permettant d'assurer un déploiement homogène des règles du Groupe La Poste ;
- **Niveau 2** : *les chartes et les directives stratégiques* de la PSSI-G, qui regroupent les règles permettant l'application du cadre général, dont le document présent ;
- **Niveau 3** : *les directives tactiques* décrites au niveau entité s'ajoutent aux directives stratégiques afin d'intégrer des éléments spécifiques à la gouvernance et au contexte d'emploi des SI des entités telles que mentionnées dans le champ d'application ;
- **Niveau 4** : *les procédures opérationnelles et guides techniques*, qui décrivent de manière explicite, les mesures d'application et de mise en œuvre de la PSSI-G.

Ce présent document est de niveau 2. La directive doit être lue et connue de toute personne travaillant pour le Groupe La Poste, y compris les prestataires intervenants sur le périmètre des SI du Groupe La Poste, tel que défini dans le champ d'application.

## 1.3 Champ d'application

La PSSI-G s'adresse à tous les acteurs du Groupe La Poste, de ses branches et de ses filiales intervenant, ou contrôlant les SI, notamment :

- Les Responsables de la Sécurité des Systèmes d'Information (RSSI) des entités ;

- L'Audit Informatique du Groupe (AIG) et les services en charge du contrôle interne ;
- Le Service de Lutte Contre la Cybercriminalité (SLCC) de la Direction des Systèmes d'Information Groupe (DSI/G) et les centres de supervision de la cybersécurité des branches et filiales ;
- Les acteurs intervenant au quotidien sur l'ensemble des SI du Groupe :
  - l'ensemble des collaborateurs,
  - les partenaires, prestataires et fournisseurs (contractuellement ou par le biais de conventions) dès lors qu'ils stockent, traitent ou utilisent des données issues du SI du Groupe La Poste.

Le RSSI complétera une matrice d'applicabilité qui déterminera :

- Le périmètre d'application des règles ;
- La possibilité de mise en œuvre ;
- La justification de non applicabilité.

## 1.4 Validité, révision et processus d'exception

La directive est applicable dès sa validation.

Elle doit être mise en œuvre dès publication sur tous les nouveaux projets applicatifs et d'infrastructures. La période de mise en conformité pour les SI déjà existants est de trois ans.

Cette directive pourra évoluer pour prendre en compte des retours d'expériences, imprécisions ou modifications des textes de référence.

Les demandes de révision sont à envoyer à la Direction de la Cybersécurité Groupe (DCG) : direction.cyber@laposte.fr.

La définition des exceptions aux règles est décrite dans le Cadre Général. La gestion des exceptions est documentée conformément au processus mis en place.

# 2 Glossaire

| Terme | Description |
|---|---|
| Antipollution | Logiciel dont l'objectif est de protéger le système de toute intrusion, virus, logiciel malveillant ou hameçonnage pouvant nuire le poste de travail, les équipements mobiles, etc. |
| Authentification | L'authentification est l'opération par laquelle un équipement ou un traitement informatique (système, application) vérifie que l'accédant qui souhaite se connecter est bien celui qu'il prétend être.<br>S'authentifier c'est apporter la preuve de son identité.<br>Cette opération peut s'appuyer sur :<br>▸ Une information que l'accédant connaît : un secret, un mot de passe, etc. ;<br>▸ Une information que l'accédant possède : une carte à puce, un « token », etc. ;<br>▸ Une information qui lui est propre : une empreinte digitale, le son de sa voix, etc.<br>Dans le processus de connexion à un SI et à ses ressources, l'authentification est le premier point de contrôle logique. L'authentification est à ce titre un mécanisme incontournable permettant de maîtriser les accès aux ressources du Système d'Information. De sa qualité et de sa robustesse dépendent la sûreté de l'information et sa protection contre des accès illicites |
| BYOD | L'acronyme « BYOD » est l'abréviation de l'expression anglaise « Bring Your Own Device », qui désigne l'usage d'équipements informatiques personnels dans un contexte professionnel. |
| Equipements mobiles | ▸ Les postes de travail nomades (ordinateurs portables) mis à disposition par le Groupe La Poste, quelle que soit leur utilisation : utilisation bureautique classique, accès à des applications « métier », conduite d'opérations d'administration ou de supervision informatique, développement informatique, etc. ;<br>▸ Les tablettes, ainsi que les téléphones mobiles communicants (smartphones, etc.) ;<br>▸ Les supports de stockage externe (clés USB, disques durs externes, CDROM, DVDROM, etc.) ;<br>▸ Les moyens d'authentification forte (token) nécessaires pour une utilisation des équipements mobiles en situation de mobilité. |
| Nomadisme | Le nomadisme numérique désigne toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI de son entité d'appartenance ou |

| Terme | Description |
| --- | --- |
| | d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité |
| Supports de stockage externe | Regroupe notamment les équipements suivants : les clés USB, les disques externes, etc. |

# 3 Règles de sécurité applicables

## 3.1 Appareils mobiles et travail à distance

Objectif : Assurer la sécurité du travail en dehors des locaux du Groupe La Poste, de ses branches et filiales et de l'utilisation d'appareils mobiles.

Cette directive vise à assurer la sécurité des informations du Groupe La Poste et des matériels s'y connectant lors d'activités professionnelles en mobilité.

Les mesures préconisées ont pour objectif d'éviter la compromission des informations du Groupe utilisées dans des environnements non protégés.

### 3.1.1 Politique en matière d'appareils mobiles

Le Groupe La Poste met en place des mesures de sécurité adaptées afin de gérer les risques liés à l'utilisation d'appareils mobiles hors des locaux du Groupe.

#### 3.1.1.1 Attribution des équipements mobiles

L'attribution par le Groupe La Poste d'un équipement mobile à toute personne travaillant pour le Groupe La Poste est motivée par un besoin professionnel et justifiée par son supérieur hiérarchique.

Un processus formalisé de demande de matériel et logiciel existe et est appliqué.

Les équipements mobiles doivent être référencés au sein d'un catalogue de standards matériels des Métiers de chaque entité. Les équipements personnels et le BYOD sont interdits au sein du Groupe La Poste.

#### 3.1.1.2 Gestion du parc mobile

Le processus d'attribution trace et enregistre au minimum :

- ❑ L'identité du demandeur ;
- ❑ La validation du supérieur hiérarchique ;
- ❑ Le type de matériel attribué ;
- ❑ L'outil de chiffrement ;
- ❑ Les logiciels de sécurité installés ;
- ❑ Un profil utilisateur (principe du moindre privilège) ;
- ❑ La liste des logiciels et applicatifs nécessaires au demandeur.

Les équipements mobiles doivent être référencés au sein du catalogue des standards matériels du Groupe La Poste. Tous les supports de stockage externes doivent être fournis par les services informatiques.

La responsabilité de la bonne gestion de ce processus d'attribution incombe au support informatique qui doit répertorier, enrôler et suivre le parc d'équipement mobile professionnel.

#### 3.1.1.3 Connexion aux réseaux

Seuls les équipements mobiles validés et répertoriés peuvent être installés et connectés aux réseaux internes et aux postes de travail du Groupe La Poste.

L'accès à distance au réseau du Groupe La Poste à partir des postes de travail nomades doit être réalisé conformément aux exigences édictées au sein de la Directive « 09. Réseau ».

Toute connexion à distance s'effectue à l'aide d'un Virtual Private Network (VPN).

L'accès distant aux données du SI n'est possible qu'après une authentification double facteurs.

#### 3.1.1.4 Accès à Internet depuis un poste de travail nomade

L'accès à internet depuis un poste de travail nomade doit être réalisé exclusivement via un point de raccordement contrôlé par le Groupe La Poste afin de bénéficier des dispositifs de sécurité du Groupe.

#### 3.1.1.5 Contrôle d'accès et authentification de l'utilisateur

Par défaut, le démarrage des postes de travail nomades doit être soumis à la saisie d'un mot de passe, conforme à la politique de mots de passe Groupe.

L'accès aux tablettes ou aux téléphones mobiles communicants doit être protégé par une authentification native (mot de passe).

Les règles de contrôle d'accès aux postes de travail nomades doivent suivre les préconisations de la directive « 05. Contrôle d'accès ».

#### 3.1.1.6 Verrouillage automatique et mise en veille

Tous les équipements mobiles communicants doivent se mettre automatiquement en veille et se verrouiller après une période d'inactivité.

Une authentification de l'utilisateur doit être requise afin de restaurer la session.

#### 3.1.1.7 Chiffrement des données

Les disques durs des postes de travail nomades doivent être chiffrés pour réduire le risque de compromission d'informations en cas de perte ou de vol, conformément aux préconisations de la directive « 06. Cryptographie ».

#### 3.1.1.8 Synchronisation des équipements mobiles communicants avec les postes de travail du Groupe La Poste

Les équipements mobiles communicants doivent être uniquement synchronisés avec les postes de travail du Groupe La Poste au travers du logiciel de synchronisation fourni, installé et maintenu par les équipes informatiques du Groupe La Poste.

Tous les équipements mobiles doivent être régulièrement connectés au réseau afin de permettre la mise à jour des versions logicielles et l'application des correctifs.

#### 3.1.1.9 Application des mises à jour et des correctifs de sécurité

Compte tenu de leur plus forte exposition, les correctifs de sécurité et les mises à jour des logiciels antipollution doivent être installés sur tous les équipements nomades.

Un agent est déployé sur tous les matériels afin d'assurer les mises à jour prioritaires en cas d'alerte.

#### 3.1.1.10 Contrôle antipollution

Tout fichier ouvert, exécuté ou lu à partir d'un support de stockage externe doit être analysé par le logiciel de lutte contre les codes malveillants résidant sur l'équipement mobile auquel le support est connecté.

#### 3.1.1.11 Protection physique des équipements

Pour les équipements compatibles, les postes de travail nomades doivent être livrés à l'utilisateur final avec un dispositif antivol de type « câble de sécurité ».

L'ensemble des équipements mobiles doit être mis sous clé lors du départ de l'employé de son lieu de travail, ou emmené avec lui dans son lieu de résidence.

Les équipements mobiles ne doivent pas rester sans surveillance dans les espaces publics et dans les voitures.

Les procédures à suivre en cas de perte ou de vol doivent être définies, connues et mises en œuvre. Les services informatiques doivent être prévenus afin de bloquer les possibilités d'accès à distance au SI du Groupe La Poste depuis l'équipement mobile volé. Toute perte ou vol d'un équipement mobile doit être signalé et faire l'objet d'une main courante ou d'un dépôt de plainte avant tout remplacement.

#### 3.1.1.12 Sensibilisation des utilisateurs nomades

Les utilisateurs d'équipements mobiles doivent être sensibilisés aux risques spécifiques liés à ce type de matériel et à leur utilisation en situation de nomadisme.

L'utilisateur est responsable de la sécurité physique de ses matériels, que ce soit au sein des locaux du Groupe La Poste ou lors de déplacements.

La sensibilisation doit préciser à l'utilisateur que toute donnée stockée en local sur son équipement n'est pas sauvegardée sur le réseau du Groupe. Il est donc de sa responsabilité d'en assurer une sauvegarde.

L'utilisation d'un équipement mobile est strictement individuelle et professionnelle. Il ne doit pas être partagé avec d'autres personnes (collaborateurs, famille, prestataire, stagiaire, intérimaire, etc.).

Les supports de stockage externes contenant des informations sensibles ne peuvent être transmis à l'extérieur sans une autorisation formelle du propriétaire des données.

### 3.1.2 Travail à distance

Une politique et des mesures de sécurité complémentaires sont mises en place pour protéger les informations consultées, traitées ou stockées sur des sites de travail à distance.

L'activité professionnelle en travail à distance s'apparente au nomadisme. Toutes les règles édictées précédemment s'appliquent.

Que le travail à distance s'effectue à domicile ou dans un autre lieu de résidence déclaré ou en centre de proximité, l'accès distant au SI de l'entreprise ne peut être réalisé avec un équipement personnel.

#### 3.1.2.1 Dispositions de mise en place

Chaque entités du Groupe La Poste fournit, installe et entretient les équipements nécessaires au travail à distance qui restent son entière propriété.

Il assure la mise en œuvre des dispositions suivantes :

- La définition des tâches autorisées, les heures de travail, la classification des informations susceptibles d'être détenues, ainsi que les systèmes et services internes auxquels le travail à distance leur est autorisé à accéder ;
- Les méthodes de sécurisation de l'accès à distance ;
- La fourniture de services d'assistance et de maintenance matérielles et logicielles ;
- Les procédures relatives à la sauvegarde et à la continuité de l'activité ;
- L'audit et la surveillance liée à la sécurité ;
- La révocation des droits d'utilisation et des droits d'accès ;
- La restitution du matériel au terme des activités de travail à distance.

Une liste des services et applicatifs autorisée existe et maintenue à jour régulièrement.

Tout nouveau service ou applicatif accessible à distance nécessite la validation du RSSI de l'entité.

#### 3.1.2.2 Sécurité physique

Le lieu de travail à distance peut être soit le domicile ou un autre lieu de résidence déclaré, soit un centre de proximité, postal ou non.

Le travail à distance leur doit disposer d'un espace de travail adéquat et sécurisé et, doit fournir pour chaque lieu une attestation sur l'honneur de la conformité aux normes de sécurité des installations électriques de l'espace dédié au travail à distance. Cette activité doit être déclarée auprès de l'assureur du travail à distance leur.

### 3.1.2.3 Sécurité logique

Les services offerts aux utilisateurs se connectant à distance aux SI du Groupe La Poste doivent être adaptés à l'exercice de leur activité professionnelle, de préférence au travers de profils d'accès.

Les accès à distance aux SI du Groupe La Poste nécessitent systématiquement une authentification forte, et doivent être tracés conformément à la directive « 08. Sécurité liée à l'Exploitation ».

### 3.1.2.4 Sécurité des accès réseaux

Pour le travail à distance, l'utilisateur leur doit disposer d'une connexion internet dont les caractéristiques sont compatibles avec l'exercice d'une activité professionnelle à domicile.

En cas d'utilisation du réseau sans-fil domestique ou réseau local sans-fil « public », les dispositions de la politique en matière d'appareils mobiles s'appliquent.

Les postes de travail nomades doivent se connecter de manière sécurisée via l'infrastructure d'accès distant mise à disposition par le Groupe La Poste, puis accéder à internet et à leur messagerie une fois cette connexion sécurisée activée.

Les postes de travail nomades doivent être configurés afin de n'autoriser que les connexions entrantes et sortantes passant par cette infrastructure d'accès distant.

Cette infrastructure doit obligatoirement faire l'objet d'une homologation de sécurité (cf. directive « 11. Gestion de projet »).

### 3.1.2.5 Chiffrement des flux d'accès distants

Si l'accès a lieu via le réseau internet, l'acheminement des flux doit être assuré par un canal chiffré conformément à la directive « 06. Cryptographie ».

L'équipement de sécurité permettant la mise en œuvre du canal chiffré doit être validé par le RSSI de l'entité.

### 3.1.2.6 Devoirs du collaborateur travaillant à distance

Le collaborateur est responsable de l'intégrité du matériel mis à sa disposition et des données qui y sont stockées. En fonction de la sensibilité des données consultées ou transmises via le réseau de

communication, il doit faire preuve de vigilance quant à leur manipulation.

Le collaborateur respecte les règles fixées par le Groupe La Poste en matière de sécurité informatique (confidentialité, mot de passe, protection des données, etc.) qui lui sont communiquées lors de la signature de l'avenant de travail à distance à son contrat de travail (salariés) ou de sa convention individuelle (fonctionnaires). Il s'engage à mettre en œuvre les dispositions suivantes :

- ❑ Interdiction d'utilisation d'un matériel détenu à titre privé et non soumis au contrôle de l'organisation ;
- ❑ Interdiction d'accès aux informations et aux matériels par la famille et les visiteurs ;
- ❑ Souscription d'une assurance dédiée ;
- ❑ Information en cas d'arrêt de l'activité de travail à distance ;
- ❑ Restitution du matériel.

Le travailleur à distance s'engage à suivre un module de sensibilisation sur la protection des données (cf. « accord_teletravail_2018_2022 ») en e-learning avant d'accéder au travail à distance.

# 4 Annexe : liste des documents applicables dans le cadre du télétravail

https://www.netrh.extra.laposte.fr/teletravail

- QR télétravail ;
- Télétravail - Flyer A5 page à page ;
- Télétravail - Flyer A5 livret ;
- Télétravail - Affiche A4 ;
- Télétravail - Affiche A3 ;
- Télétravail - Guide télétravailleur ;
- Télétravail - Guide manager ;
- Accord Télétravail 2018 – 2022 ;
- Télétravail - présentation nouveautés accord télétravail ;
- Télétravail - questionnaire relatif aux conditions de sécurité ;
- Télétravail - modèle attestation conformité électrique ;
- Télétravail - modèle de déclaration pour l'assureur ;
- Télétravail - modèle autorisation télétravail en centre de proximité postal ;
- Télétravail - modèle récépissé de remise en main propre du matériel ;
- Télétravail - modèle de demande – fonctionnaires ;
- Télétravail modèle de réponse fonctionnaire 2019 ;
- Télétravail - modèle de demande – salariés ;
- Télétravail - modèle de réponse – salariés ;
- Télétravail-modèle réponse salarié demande modification ;
- Modèle réponse fonctionnaire demande modification télétravail 2019 ;
- Télétravail - modèle saisine commission de conciliation ;
- Télétravail - questionnaire sur les conditions de travail à la fin de la période d'adaptation ;
- Télétravail - modèle renouvellement période d'adaptation ;
- Télétravail - modèle de demande de modification ;
- Télétravail - modèle de demande fin – fonctionnaires ;
- Télétravail - modèle de demande fin – salariés ;
- Télétravail - modèle de décision fin de télétravail à l'initiative du responsable NOD – fonctionnaire ;
- Télétravail - modèle de demande fin télétravail à l'initiative du responsable hiérarchique – salarié ;
- Modèle de déclaration de sinistre télétravail ;
- Télétravail - Infographie 2017 ;
- Télétravail - Résultats enquête qualitative 2017.