DIRECTIVE STRATEGIQUE

15. CONFORMITE ET CONTROLE

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

Statut du document	Validé
Version	V 2.0
Date d'enregistrement	28/10/2020
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 conformité et au contrôle.

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 3 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
CNIL	Commission Nationale de l'Informatique et des Libertés
Collaborateur	Personne physique travaillant au sein du Groupe La Poste ou d'une de ses filiales
Délégué à la Protection des Données	Le Délégué à la Protection des données (DPD) remplace le Correspondant Informatique et Libertés (CIL), qui pouvait être désigné de façon facultative dans l'entreprise comme garant de l'application de la loi « informatique et libertés ». Le DPD a pour mission d'assurer une veille et un conseil interne auprès de l'employeur sur les obligations de protection des données personnelles. Il est également le référent de la CNIL
Entité	Terme générique désignant La Poste maison-mère, ses branches, ses holdings et ses filiales

3 Règles de sécurité applicables

3.1 Conformité aux obligations légales et réglementaires

Objectif : Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.

3.1.1 Identification de la législation et des exigences contractuelles applicables

Le cadre légal, réglementaire et contractuel applicable aux entités et aux différents systèmes d'informations est documenté et mis à jour. L'approche adoptée pour satisfaire ces obligations est également documentée.

3.1.1.1 Identification de la législation et des exigences

Les exigences légales, réglementaires et contractuelles en vigueur ainsi que l'approche adoptée pour satisfaire à ces exigences doivent être identifiées et formalisées avec un niveau de détail suffisant pour l'ensemble des SI du Groupe La Poste.

La direction juridique et la DCG assurent respectivement une veille juridique et réglementaire liées aux SI et en communiquent les résultats aux DSI. Une revue annuelle des évolutions juridiques et réglementaires est réalisée en comité de veille réglementaire.

Le Métier propriétaire du projet et tout porteur de projet informatique doivent s'assurer que les exigences légales, réglementaires et contractuelles en vigueur pour les SI sur leurs périmètres sont définies, documentées et maintenues dans le temps.

Les exigences exclues du périmètre doivent être justifiées et appliquées le processus de gestion des exceptions.

A des fins de management des risques, il est indispensable que cette justification soit apportée au dossier d'homologation du SI (cf. « Procédure d'homologation et de sécurisation des SI »).

3.1.2 Droits de propriété intellectuelle

La conformité aux exigences légales, réglementaires et contractuelles relatives aux droits de propriété intellectuelle et à l'utilisation de logiciels propriétaires, doit être garantie par des procédures appropriées.

3.1.2.1 Droits de propriété intellectuelle

Des procédures doivent être mises en place afin de garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives aux droits de propriété intellectuelle et à l'utilisation de logiciels propriétaires.

La violation des droits d'auteur peut déclencher une action judiciaire pouvant aboutir à des poursuites pénales.

3.1.2.2 Gestion de logiciels

Une procédure de gestion des conditions d'utilisation des licences doit être formalisée.

Les logiciels acquis au sein du Groupe La Poste le sont au travers de sources connues et réputées afin de s'assurer du respect des droits d'auteur.

L'utilisation des logiciels est conforme aux conditions générales d'utilisation.

3.1.2.3 Sensibilisation

La sensibilisation des utilisateurs en matière de protection des droits de propriété intellectuelle est effectuée conformément à la directive « 03. Ressources Humaines ».

3.1.2.4 Registre

Une liste des actifs soumis à des exigences de protection des droits de propriété intellectuelle existe et est tenue à jour conformément au modèle de classification de la directive « 04. Gestion des actifs et classification ».

Les preuves d'achat des licences sont conservées par les DSI ou par le Métier demandeur et suivies dans un registre.

3.1.2.5 Contrôles et revues

Les DSI et les demandeurs d'outils s'assurent que le nombre de licences correspond au nombre d'utilisateurs des outils déployés (revue du registre).

Les DSI s'assurent régulièrement que les outils installés sur les postes sont autorisés et sous licence valide.

3.1.2.6 Reproduction et copie

Les reproductions et copies, même partielles, doivent s'effectuer au regard de la législation sur les droits d'auteur en vigueur.

3.1.3 Protection des enregistrements

Les enregistrements sont des informations créées dans les applications informatiques. Ils doivent faire l'objet de mesures de sécurité garantissant leur protection contre la perte, la destruction, la falsification et, les accès et diffusions non autorisées, conformément aux exigences légales, réglementaires, contractuelles et aux exigences Métier.

Les règles et les procédures d'archivage sont définies en relation avec la direction des archives du Groupe et conformément à la réglementation en vigueur.

3.1.3.1 Procédure

Une procédure de stockage et de manipulation des enregistrements doit être définie. La durée de conservation de ces enregistrements doit y être fixée conformément à la réglementation en vigueur et aux règles d'archivage du Groupe émises par la DIRAG.

La protection des enregistrements s'effectue selon le modèle de classification décrit dans la directive « 04. Gestion des actifs et classification ».

Les enregistrements doivent être classés par types et font l'objet d'une indexation et/ou d'un classement adaptés aux besoins de leur gestion et de leur consultation. :

- Documents comptables et ressources humaines ;
- Enregistrements de base de données ;
- Journaux de transactions ;
- Journaux d'audit ;
- Procédures d'exploitation.

Pour chaque type d'enregistrement, sont définis la durée et les modalités périodes de conservation et ainsi que le type de support de stockage permis (papier, microfiche, support magnétique, support optique).

Les clés cryptographiques associées ainsi que les programmes relatifs aux enregistrements ou signatures électroniques chiffrées doivent être

stockés conformément à la directive « 06. Cryptographie » afin de permettre le déchiffrement des enregistrements pendant leur durée de conservation.

3.1.3.2 Accès aux données stockées

Le système de stockage et de manipulation garantit l'identification des enregistrements et la durée de conservation conformément aux besoins de sauvegarde opérationnels.

Il doit :

- ❑ Garantir l'accès aux données (lisibilité du support et du format) tout au long de la période de conservation afin de protéger les données contre toute perte, due à l'évolution de la technologie ;
- ❑ Permettre la récupération des données requises dans un délai raisonnable et sous un format lisible.

3.1.3.3 Destruction

Le système de stockage assure la destruction des enregistrements à l'issue de la période de conservation opérationnelle définie par l'entité.

3.1.4 Protection de la vie privée et protection des données à caractère personnel

La protection de la vie privée et des données est garantie par les mesures législatives et réglementaires en vigueur.

3.1.4.1 Obligations du Délégué à la Protection des Données

Le Délégué à la Protection des Données Groupe est nommé par le Président Directeur Général du Groupe La Poste.

Il remplit cinq missions :

- ❑ Informer et conseiller les responsables de traitement ;
- ❑ Produire des directives et des outils pour assurer son respect ;
- ❑ Veiller à la bonne application du Règlement Général pour la Protection des Données dans le Groupe et la contrôler ;
- ❑ Tenir le registre des traitements pratiqués dans le Groupe ;
- ❑ Être le point de contact avec la CNIL et coopérer avec elle.

Chaque entité du Groupe La Poste est responsable de sa conformité avec cette réglementation et met en place l'organisation et les moyens nécessaires pour le faire.

3.1.5 Réglementation relative aux mesures cryptographiques

Des mesures cryptographiques doivent être prises conformément aux accords, lois et réglementations applicables.

3.1.5.1 Mesures cryptographiques

Des mesures cryptographiques doivent être mises en œuvre conformément à la directive « 06. Cryptographie », aux accords, lois et réglementations applicables aux SI.

Ces mesures doivent tenir compte des restrictions suivantes :

- Restrictions en matière d'importation ou d'exportation de matériels et de logiciels destinés à l'exécution de fonctions cryptographiques ou à l'intégration des fonctions cryptographiques ;
- Restrictions en matière d'utilisation du chiffrement.

3.2 Revue de la sécurité de l'information

Objectif : garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux directives et procédures organisationnelles.

3.2.1 Revue indépendante de la sécurité de l'information

L'approche retenue par l'organisation pour gérer et mettre en œuvre la sécurité de l'information fait l'objet de revues régulières et indépendantes.

3.2.1.1 Réalisation des revues indépendantes

Des revues indépendantes régulières doivent être réalisées sur les SI en accord avec les exigences définies dans les normes et réglementations qui leur incombent (périmètre, fréquence, rapport, etc.). Ces revues, assurées par des professionnels qualifiés, permettent d'analyser les axes d'amélioration et les changements à apporter.

Les revues doivent systématiquement faire l'objet d'un rapport précisant les non-conformités ainsi qu'un plan d'action correctif.

Ces livrables doivent être enregistrés, communiqués auprès de la direction de l'entité à l'origine de la demande et conservés.

3.2.1.2 Suivi des revues indépendantes

Toutes les actions de correction feront l'objet d'un suivi formalisé et d'une vérification.

3.2.2 Conformité avec les politiques et les normes de sécurité

La conformité du traitement de l'information et des procédures est régulièrement revue par les responsables, conformément aux politiques, normes et autres exigences de sécurité applicables.

3.2.2.1 Contrôles de conformité

La conformité à la PSSI-G, aux directives opérationnelles des entités ainsi qu'à l'ensemble des exigences légales, réglementaires et contractuelles en vigueur est vérifiée par des contrôles réguliers.

Un plan de mise en conformité organisé par la DCG, est planifié et piloté dans chaque entité pour assurer la mise en conformité.

Toutes les actions nécessaires feront l'objet d'un suivi formalisé et d'une vérification.

Les RSSI de chaque entité conduisent des actions locales d'évaluation de la conformité à la PSSI-G et contribuent à la consolidation, dans un bilan annuel, de l'état d'avancement de sa mise en œuvre.

3.2.3 Examen de la conformité technique

Les SI sont régulièrement audités pour vérifier leur conformité technique avec les politiques et les normes de sécurité de l'information.

3.2.3.1 Audits de conformité technique

Des audits techniques sont effectués régulièrement sur les SI afin de maintenir leur niveau de sécurité. Ils sont réalisés en accord avec les exigences définies dans les normes et réglementations qui les encadrent (périmètre, fréquence, etc.) et de préférence à l'aide d'outils automatiques générant des rapports à soumettre à l'interprétation d'un spécialiste.

Les audits doivent systématiquement faire l'objet d'un rapport précisant les vulnérabilités du SI audité ainsi qu'un plan d'action de correction.

Toutes les actions de correction feront l'objet d'un suivi formalisé et d'une vérification.

3.2.3.2 Organisation des audits

Les audits doivent être documentés et les tests techniques doivent être planifiés. Ils sont exécutés avec la plus grande prudence pour éviter de compromettre le SI audité et réalisés par des personnes compétentes et autorisées.

4 Annexe

4.1 Textes extranationaux

[RGPD]	Règlement (UE) 2016/679 du parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)
[eIDAS]	Règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE
[NIS-EU]	Directive (UE) 2016/1148 du parlement Européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

4.2 Textes nationaux

[STRAT FR]	Stratégie de la France en matière de défense et de sécurité des systèmes d'information
[RGS]	Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques
[OIV]	Décret n°2015-351 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale
[PROT-SCI]	Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation

4.3 Instructions interministérielles

[IGI 1300]	Instruction Générale Interministérielle n°1300/SGDSN/PSE/SSD du 30 novembre 2011 sur la protection du secret de la défense nationale
[II 901]	Instruction interministérielle n°901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'information sensibles

4.4 Textes et notes de référence

[PSSI-G]	Politique de Sécurité des Systèmes d'Information du Groupe La Poste