DIRECTIVE STRATEGIQUE

12. RELATIONS AVEC LES FOURNISSEURS

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 relation avec les fournisseurs.

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
Fournisseur	Toute personne morale ou établissement fournissant aux entités du Groupe La Poste des biens ou des services nécessaires à leur activité
Responsable de contrat	S'assure, ou fait assurer par toute personne de son choix, que l'ensemble des règles de la présente directive est mis en œuvre et que les actions sont réalisées. Le fait de déléguer la vérification ne désengage pas le responsable du contrat de sa responsabilité
Tiers	Désigne un organisme ou une personne reconnu(e) comme indépendant(e) du Groupe La Poste et de ses entités
Plan d'Assurance Sécurité (PAS)	Document fourni par le prestataire présentant les règles de sécurité que ce dernier s'impose. Le PAS doit permettre d'offrir des garanties en termes de sécurité de l'information
PDIS	Prestataire de Détection d'Incidents de Sécurité
PRIS	Prestataire de Réponse aux Incidents de Sécurité
PASSI	Prestataire d'Audit de Sécurité des Systèmes d'Information

3 Règles de sécurité applicables

3.1 Sécurité de l'information dans les relations avec les fournisseurs

Objectif : garantir la protection des actifs de l'organisation accessibles aux fournisseurs.

3.1.1 Politique de sécurité de l'information dans les relations avec les fournisseurs

Les règles de la présente directive ont pour objectifs de fixer les moyens à mettre en œuvre pour garantir la protection des actifs du Groupe La Poste accessibles aux fournisseurs et de les documenter par l'une ou l'autre partie.

Seront décrites ci-dessous les règles à formaliser et à appliquer dans les relations avec les fournisseurs.

3.1.1.1 Gestion des relations avec les fournisseurs

L'entité identifie et collecte la documentation relative aux activités du fournisseur (services informatiques, services logistiques, services financiers, composants de l'infrastructure informatique, auxquels l'organisation accordera un accès à son information).

Un processus de gestion des relations avec les fournisseurs est organisé et normalisé.

Un processus interne permet de surveiller la conformité du fournisseur aux exigences de sécurité du Groupe La Poste, incluant une revue et une validation par une tierce partie si nécessaire (audit tiers).

Toute collaboration avec des fournisseurs doit être placée sous la responsabilité d'un acteur appelé le « responsable du contrat ». Celui-ci doit s'assurer que l'ensemble des règles de la présente directive est mis en œuvre et que les actions suivantes sont réalisées :

- ❑ Définition des responsabilités respectives des deux parties ;
- ❑ Désignation d'un responsable de la sécurité chez le fournisseur ;
- ❑ Communication des exigences de sécurité aux fournisseurs concernés ;
- ❑ Communication du niveau de service attendu ;
- ❑ Suivi du respect des engagements ;

- Clôture de la collaboration.

Durant toute la durée de la collaboration, le responsable du contrat s'assure du respect des engagements prévus dans le contrat. Il procède ou fait procéder à des contrôles ou audits si nécessaires.

3.1.1.2 Gestion des sous-traitants

Le fournisseur peut sous-traiter une partie des prestations de services ou des travaux qui lui sont confiés uniquement si le Groupe La Poste l'accepte formellement par contrat. Dans ce cas, le fournisseur est juridiquement responsable pour le sous-traitant, des engagements qu'il a pris vis-à-vis du Groupe La Poste, client de la prestation.

Les exigences initiales de la prestation fixées entre le Groupe La Poste et le fournisseur s'appliquent à l'ensemble des sous-traitants de la prestation. Le fournisseur doit garantir l'application de ces exigences.

3.1.1.3 Gestion des accès fournisseur

Conformément aux directive « 05. Contrôle d'accès » et « 07. Sécurité physique », les types d'accès logiques et physiques accordés aux fournisseurs doivent être définis, surveillés et contrôlés. La gestion des incidents et des impondérables liés aux accès des fournisseurs est prévue dans le contrat ou la convention de service.

Un profil approprié par type de fournisseur est élaboré selon les besoins et les risques de sa mission en vue de restreindre ses accès aux informations selon la classification de ceux-ci selon les exigences de la directive « 04. Gestion des actifs et classification ».

Le fournisseur s'engage à utiliser ses droits d'accès physiques et logiques (systèmes, réseaux, bases de données, applications, etc.) uniquement dans le cadre de sa mission et pendant la durée du contrat signé. Les modalités d'accès seront décrites dans le Plan d'Assurance Sécurité (PAS) signés entre les deux parties.

3.1.1.4 Disponibilité, Confidentialité et Intégrité des données

Les obligations applicables aux fournisseurs pour protéger les actifs du Groupe La Poste sont décrites pour en assurer leur confidentialité.

Des dispositions doivent être formalisées pour garantir la disponibilité, la résilience et le traitement conforme à la PSSI-G des données.

Des contrôles bilatéraux sont mis en place pour garantir l'intégrité de l'information et de son traitement.

Le fournisseur doit mettre en place des protocoles de transmission, stockage et traitement adaptés permettant de vérifier la conformité des données reçues à celles émises.

3.1.1.5 Sensibilisation du personnel du Groupe La Poste

Tout personnel impliqué dans le processus d'achat relatif aux produits et services informatiques doit être sensibilisé à la présente directive afin de garantir le bon respect des règles de sécurité établies par le Groupe La Poste dans les contrats avec les fournisseurs.

3.1.1.6 Contractualisation

Les exigences et mesures de sécurité de l'information sont documentées dans un accord signé par les deux parties qui intègre la présente directive et la PSSI-G. Ce document peut être annexé au contrat.

Le fournisseur s'engage à suivre les obligations légales et réglementaires applicables à l'activité et à prendre en compte toutes les évolutions associées. Cette règle doit s'appliquer en conformité avec la directive « 15. Conformité ».

Le contrat prévoit un engagement de non divulgation et une clause d'engagement de confidentialité.

Les éléments fonctionnels et opérationnels doivent être listés dans un PAS qui sera actualisé tout au long de l'instruction et annexé au contrat. Il précise notamment :

- Qualifications de l'entreprise (ISO 27001, PDIS, PRIS, PASSI, SecNumCloud etc.) ;
- Certifications individuelles des intervenants (ISO 2700x Lead auditor, PASSI, CISSP, etc.) ;
- Procédures d'habilitation/de criblage ;
- Qualification des produits (CSPN, RGS, CC EAL*, etc.) ;
- Evaluations permettant de diagnostiquer la maturité du partenaire : organisation de la sécurité des SI, RGPD (protection des données, privacy by design), etc. ;

- Auditabilité de la sécurité des prestations faisant l'objet du partenariat (fréquence, délais, conditions de déclenchement, coût etc.) ;
- Réversibilité des données ou obligations de destruction ;
- Pilotage des processus de gestion des incidents, de continuité d'activité (Plan de Continuité d'Activité, Plan de Reprise d'Activité, etc.).

3.1.1.7 Fin de contrat

La gestion de la transition est prévue sur une période donnée et documentée, par exemple par un Plan de Réversibilité (PREV).

En cas d'expiration ou de résiliation de tout ou partie des services ou du contrat pour quelque motif que ce soit, le fournisseur s'engage :

- A éviter toute interruption ou baisse de qualité des services avant la fin du contrat ;
- A assurer les opérations qui permettront au Groupe La Poste d'avoir toute la maîtrise nécessaire afin de reprendre ou de faire reprendre par un fournisseur les services dans les meilleures conditions (transfert de compétences, documents explicatifs, etc.) ;
- A veiller à ce que le niveau de sécurité soit maintenu ;
- A contrôler la suspension de l'ensemble des accès et habilitations mis à sa disposition ainsi que la destruction des données stockées sur ses matériels.

Le responsable du contrat du Groupe La Poste s'assure de la suspension de l'ensemble des accès et habilitations (ou accréditations) mis à disposition des fournisseurs.

L'intégralité des documents, des données et du matériel doit être restituée. Le fournisseur s'engage à ne pas en conserver de copie.

3.1.2 La sécurité dans les accords conclus avec les fournisseurs

Les contrats avec les fournisseurs incluent les conditions garantissant un niveau de sécurité adapté aux exigences de sécurité en matière de SI imposées par le processus ou le projet concerné. Elles sont définies dès la phase de cadrage du projet ou d'appel d'offre.

3.1.2.1 Sélection du fournisseur

Concernant les prestations (conseil, développement logiciel, services externalisés, etc.), un processus formel de sélection doit être décrit et appliqué à partir des exigences de sécurité identifiées et formalisées par le projet.

Le processus de choix des fournisseurs doit prendre en compte les réponses apportées par chacun d'entre eux aux exigences de sécurité exprimées dans le cahier des charges.

Le RSSI de l'entité doit être consulté dans le cadre du processus de choix et d'évaluation du niveau de sécurité apporté par le fournisseur (réponse à appel d'offre, soutenance, etc.). Son équivalent existe chez le fournisseur et est en charge des questions et livraisons des documents de sécurité nécessaires à la contractualisation. Il reste le contact privilégié durant toute la durée du contrat.

3.1.2.2 Cadrage de l'accès aux actifs

Le contrat prévoit que l'accès aux actifs s'effectue selon les modalités suivantes :

- ❑ Fournir la description des actifs et les méthodes d'accès à l'information ;
- ❑ Formaliser le plan de classification de l'information relatif au projet (cf. directive « 04. Gestion des actifs et classification) ;
- ❑ Décrire les règles d'utilisation et les conditions d'utilisation non admises ;
- ❑ Informer les ressources du fournisseur des procédures spécifiques, exigences de sécurité de l'information, chartes, etc. Les documents nécessaires leur sont remis à leur prise de fonction.

3.1.2.3 Respect de la conformité réglementaire

Les accords contractuels prennent en compte :

- ❑ Les exigences légales et réglementaires, y compris la protection des données, les droits de propriété intellectuelle et les droits d'auteur ;
- ❑ Les politiques de sécurité de l'information pertinentes en cas de spécificité ;
- ❑ Les réglementations à prendre en compte concernant la sous-traitance ;

- L'obligation du fournisseur à se conformer aux exigences de sécurité du Groupe La Poste.

3.1.2.4 Contrôle de l'activité

Chaque partie s'oblige contractuellement à contrôler les activités liées à la prestation :

- Contrôle d'accès ;
- Revue des performances ;
- Surveillance des activités ;
- Rédaction de rapport et audit.

Concernant le contrôle d'accès, une liste nominative des salariés du fournisseur autorisés à accéder à l'information est fournie en vue de gérer les conditions liées à l'octroi et au retrait d'autorisations.

3.1.2.5 Gestion des problèmes

Les exigences et les procédures de gestion des incidents, notamment la notification et la collaboration lors de la résolution sont prévues dans les contrats.

Les processus de résolution des anomalies et des conflits sont aussi prévus.

Le fournisseur devra fournir la preuve de l'existence d'un Plan de Continuité d'Activité (PCA) pour l'ensemble des éléments sensibles de l'infrastructure mise en place.

Le Responsable du contrat, en s'appuyant éventuellement sur l'expertise du RSSI de son entité, s'assure que les dispositifs nécessaires à la couverture des risques sont bien mis en place.

Le résultat des tests de PCA réalisés par le fournisseur ainsi que le plan d'amélioration devront être disponibles lors de toute demande du Groupe La Poste.

L'expression de besoins en termes de continuité d'activité incombe à l'entité contractante du Groupe La Poste.

3.1.2.6 Audit fournisseur

Le contrat prévoit le droit d'auditer les processus et les mesures de sécurité du fournisseur en rapport avec le périmètre projet.

Le fournisseur se doit de communiquer périodiquement un rapport indépendant sur l'efficacité des mesures de sécurité mises en œuvre au sein de son entreprise par rapport à la PSSI-G du Groupe La Poste. Il devra apporter les preuves des plans d'actions correctifs menés pour corriger les vulnérabilités relevées.

3.1.3 Traitement des risques associés à la chaîne d'approvisionnement informatique

Les fournisseurs doivent inclure dans leurs accords avec le Groupe La Poste des exigences sur le traitement des risques de sécurité de l'information associés à la chaîne d'approvisionnement des produits et des services informatiques.

3.1.3.1 Communication des exigences de sécurité

Chaque entité du Groupe La Poste définit et communique les exigences de sécurité de l'information à appliquer lors de l'achat de produits ou de services informatiques.

Le fournisseur a l'obligation de diffuser les exigences et les pratiques de sécurité de l'entité du Groupe La Poste jusqu'au dernier maillon de la chaîne d'approvisionnement, y compris s'il sous-traite une partie du contrat.

Les entités du Groupe La Poste et le fournisseur définissent les règles de partage de l'information concernant la chaîne d'approvisionnement et les problèmes éventuels.

3.1.3.2 Contrôle de la qualité de la Sécurité des Systèmes d'Information

La mise en œuvre d'un processus de surveillance et de méthodes éprouvées confirme que les produits et les services informatiques livrés respectent les exigences de sécurité stipulées dans la PSSI-G.

Le fournisseur garantit que les produits informatiques et services livrés ne présentent aucune vulnérabilité connue.

Il garantit aussi que les composants critiques et leur origine peuvent être tracés tout au long de la chaîne d'approvisionnement.

Le fournisseur prévoit des processus spécifiques de gestion du cycle de vie des composants informatiques et de leur disponibilité. Cela inclut la gestion des risques de rupture de stock, le fournisseur ayant cessé son

activité ou ayant arrêté de produire ces composants en raison des avancées technologiques.

3.2 Gestion de la prestation du service

Objectif : maintenir un niveau convenu de sécurité de l'information et de prestation de services, conformément aux accords conclus avec les fournisseurs.

3.2.1 Surveillance et revue des services fournisseurs

Les prestations de services assurées par les fournisseurs doivent être régulièrement surveillées, révisées et auditées.

3.2.1.1 Gouvernance des fournisseurs

Des revues périodiques sont planifiées entre le contractant et le fournisseur pour :

- Surveiller les niveaux de performance des services et vérifier ainsi qu'ils sont conformes aux accords ;
- Revoir les rapports de service produits par le fournisseur et organiser des réunions régulières sur l'avancement comme l'exigent les accords ;
- Revoir les aspects liés à la sécurité de l'information dans les relations du fournisseur avec ses propres fournisseurs.

3.2.1.2 Revue des incidents

Le fournisseur transmet l'information relative aux incidents et évènements liés à la SSI via un processus de signalement défini.

Il en assure une revue conjointe comme l'exigent les accords définis dans le PAS. Les plans de résolution sont aussi fournis.

3.2.1.3 Audit et contrôle

Afin de vérifier le respect des engagements définis dans le contrat, Le Groupe La Poste peut procéder ou faire procéder, à tout moment, par toute personne de son choix conformément aux dispositions prises dans le contrat, à un audit et des contrôles des procédures et des moyens liés à la sécurité de l'information et des SI, mis en place par le fournisseur.

La procédure d'audit sera conforme aux règles décrites dans le contrat établi avec le fournisseur (clause d'auditabilité et clause réglementaire des contrats du Groupe La Poste).

3.2.2 Gestion des changements apportés dans les services des fournisseurs

Les changements effectués dans les prestations de service sont gérés en tenant compte du caractère critique de l'information, des systèmes et processus concernés et, de la réappréciation du risque. Ces changements intègrent également l'amélioration des politiques, procédures et mesures existantes en matière de sécurité de l'information.

3.2.2.1 Règles de gestion des changements fournisseurs

Tout contrat de prestation doit intégrer la possibilité de révision, d'amélioration et de modification.

Ces changements doivent permettre d'adapter les contrats à l'évolution du contexte ou de la prestation comme précisés ci-dessous :

- Les changements apportés aux accords passés avec les fournisseurs ;
- Les changements effectués par le Groupe La Poste pour mettre en œuvre :
  - des améliorations aux services offerts,
  - le développement d'applications et de systèmes nouveaux,
  - des changements ou des mises à jour des directives et des procédures du Groupe,
  - des mesures nouvelles ou modifiées permettant de résoudre les incidents liés à la sécurité de l'information et d'améliorer la sécurité.
- Les changements dans les services assurés par les fournisseurs pour mettre en œuvre :
  - des changements et des améliorations apportées aux réseaux,
  - l'utilisation de nouvelles technologies,
  - l'adoption de nouveaux produits ou des versions/des éditions plus récentes,
  - des outils et des environnements de développements nouveaux,
  - des changements apportés à l'emplacement physique des équipements,
  - des changements de fournisseurs,
  - la sous-traitance à un autre fournisseur.

3.2.2.2 Communication et mise en œuvre du changement

Toute modification de la prestation (provenant du fournisseur ou du Groupe La Poste) doit donner lieu à une communication et à l'actualisation du dossier et du contrat, ainsi que de l'analyse des risques associée à la prestation, notamment en cas de perte de certification ou de qualification du fournisseur.

Dans l'hypothèse où ces éléments ont un impact sur la SSI, ils doivent être soumis à nouveau à la validation du RSSI de l'entité, selon un processus similaire à celui mis en œuvre lors des phases d'instruction et de contractualisation initiales.