# DIRECTIVE STRATEGIQUE

# 03. RESSOURCES HUMAINES

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

| | |
|---|---|
| **Statut du document** | Validé |
| **Version** | V 1.0 |
| **Date d'enregistrement** | 08/10/2019 |
| **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 gestion des Ressources Humaines dans la sécurité des Systèmes d'information (SI).

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 sur les SI du Groupe La Poste, y compris les prestataires, tel que défini dans le champ d'application.

Ce document s'adresse particulièrement aux responsables des Ressources Humaines en charge du recrutement et du suivi du personnel travaillant sur les SI du Groupe La Poste. Toutes personnes susceptibles de recruter du personnel interne ou externe intervenant sur les SI du Groupe sont aussi concernées par cette directive.

## 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) 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 contrats et contrats cadres. Pour les contrats existants, elle est mise en œuvre de manière rétroactive. La période de mise en conformité 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 |
|---|---|
| Actifs essentiels | Ressource informationnel ou processus qui a de la valeur pour l'entité. Les actifs essentiels représentent le patrimoine informationnel, ou les « biens immatériels », que l'entité souhaite protéger, c'est-à-dire ceux pour lesquels le non-respect de la disponibilité, de l'intégrité, de la confidentialité et de la traçabilité, mettrait en cause la responsabilité de l'utilisateur, ou causerait un préjudice à eux-mêmes ou à des tiers (actifs classifiés C3 et C4). |
| Collaborateur | Personne physique travaillant au sein du Groupe La Poste ou d'une de ses filiales |
| Entité | Terme générique désignant La Poste maison-mère, ses branches, ses holdings et ses filiales |
| Evénement de sécurité | Changement d'état d'un système lié à sa protection et indiquant l'émergence d'un risque |
| Tiers | Désigne un organisme ou une personne reconnu(e) comme indépendant(e) du Groupe La Poste et de ses entités |

# 3 Règles de sécurité applicables

## 3.1 Avant l'embauche

Objectif : s'assurer que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier.

### 3.1.1 Sélection des candidats

Les vérifications des informations concernant les candidats à un poste au sein du Groupe sont proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.

#### 3.1.1.1 Contrôles pour tous les candidats à l'embauche

En conformité avec la législation en vigueur, le dossier de tous les candidats à l'embauche ou en mobilité interne doit faire l'objet, à minima, des contrôles suivants :

- ❑ Vérification du degré d'exhaustivité et d'exactitude du curriculum vitae ;
- ❑ Validité des formations et qualifications alléguées.

#### 3.1.1.2 Contrôles pour les candidats à l'embauche sur un poste sensible

Lorsqu'un poste implique l'accès aux moyens de traitement d'informations sensibles (actifs essentiels niveau C3), l'entité doit effectuer les contrôles complémentaires suivants :

- ❑ Contrôle de l'identité ;
- ❑ Extrait de casier judiciaire.

La règle s'applique sur les nouveaux arrivants, personnel en mobilité et personnels externes.

#### 3.1.1.3 Organisation des contrôles à l'embauche

La direction des ressources humaines de chaque entité est responsable de la mise en œuvre et de la conformité juridique du contrôle des dossiers des candidats internes.

#### 3.1.1.4 Contrôles du personnel temporaire et des stagiaires

Les contrôles réalisés au profit du personnel temporaire et des stagiaires doivent être effectués au même niveau que pour le personnel interne. Des contrôles complémentaires, similaires à ceux du personnel interne, doivent être effectués pour le personnel temporaire et les stagiaires dont les postes impliquent l'accès aux moyens de traitement d'informations sensibles.

Les relations contractuelles doivent prévoir ces contrôles.

La responsabilité du contrôle est portée ici par le responsable interne de la prestation ou par le maître de stage.

#### 3.1.1.5 Encadrement du personnel temporaire et des stagiaires

Tout personnel employé de manière temporaire dans l'entité doit être placé sous la responsabilité d'un membre du personnel interne pendant toute la durée de son contrat.

### 3.1.2 Sélection des candidats

Les accords contractuels avec les salariés et les contractants tiers prévoient leurs responsabilités en matière de sécurité de l'information.

#### 3.1.2.1 Fiche de poste

La fiche de poste de chaque candidat à l'embauche doit mentionner son rôle et ses responsabilités à l'égard du respect des règles de la PSSI-G. Elle prévoit aussi l'application des règles SSI de l'entité et le devoir de signalement des évènements de sécurité des SI.

Est inclut le besoin d'habilitations au Secret de la Défense Nationale ou à l'enquête administrative sur les postes sensibles le nécessitant.

#### 3.1.2.2 Charte informatique

La charte informatique doit détailler les obligations contractuelles des salariés ou du personnel temporaire et notamment :

- Les règles de protection de l'information en vigueur au sein de l'entité ;
- Les responsabilités relatives à la classification des informations et à la gestion des actifs de l'entité ;

- Les actions engagées par l'entité si le salarié ou le contractant ne tient pas compte des exigences en matière de sécurité.

La charte informatique est annexée au contrat de travail et doit être signée en même temps que ce dernier.

#### 3.1.2.3 Information des candidats

Chaque candidat, avant sa prise de fonction au sein de l'entité doit être clairement informé sur ses droits et devoirs en matière d'usage des systèmes d'information de l'entité. Cette information est formalisée par la signature de l'engagement de responsabilité afférent à la charte informatique de l'entité. La direction des Ressources Humaines de chaque entité est responsable de l'application de cette règle. La signature de l'engagement de responsabilité est intégrée au dossier RH de chaque candidat.

## 3.2 Pendant la durée du contrat

Objectif : s'assurer que les salariés et les contractants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités.

### 3.2.1 Responsabilités de la direction

La direction de l'entité doit faire appliquer la présente PSSI-G ainsi que l'ensemble des procédures de sécurité en vigueur à tous les salariés et les tiers de son périmètre.

#### 3.2.1.1 Responsabilité en terme d'application des règles de la PSSI-G

Chaque responsable hiérarchique doit s'assurer que les membres de son équipe, internes ou externes :

- Sont sensibilisés à la SSI dans le cadre de leur fonction ;
- Sont informés et respectent les règles de la PSSI-G ;
- Disposent des moyens nécessaires à la mise en œuvre des règles de la PSSI-G ;
- Ont la possibilité de signaler tout incident relevant de la SSI.

#### 3.2.1.2 Responsabilité en terme de formation à la SSI

Chaque responsable hiérarchique doit s'assurer que les membres de son équipe en charge du développement, de l'administration et de la

sécurisation des systèmes d'informations soient régulièrement formés à la sécurité des systèmes d'informations en vue de maintenir leurs qualifications.

#### 3.2.1.3 Responsabilité en terme de sensibilisation à la SSI

Les RSSI de chaque entité doivent superviser l'organisation de la sensibilisation des collaborateurs. Ils assurent, en lien avec les gestionnaires des ressources humaines, le suivi du taux de collaborateurs sensibilisés annuellement.

### 3.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information

Les salariés et les contractants tiers appartenant à une entité du Groupe La Poste doivent être formés et sensibilisés régulièrement à la PSSI-G et à la sécurité informatique en fonction de leur poste.

#### 3.2.2.1 Sensibilisation à la SSI

Tout collaborateur ayant accès au SI d'une entité doit être sensibilisé à la SSI au moins une fois par an.

#### 3.2.2.2 Programme de sensibilisation à la SSI

Le programme de sensibilisation à la SSI doit, au minimum, intégrer les items suivants :

- Présentation du référentiel réglementaire (règles et obligations applicables) de la sécurité de l'information ;
- Organisation de la SSI dans le Groupe et au sein de chaque entité ;
- Imputabilité des actions réalisées sur les SI ;
- Responsabilités en matière de protection des informations de l'entité ;
- Procédures et mesures élémentaires en matière de sécurité de l'information (sécurité des mots de passe, protection contre les logiciels malveillants, politique du bureau propre, etc.) ;
- Détail des points de contact et des ressources permettant d'obtenir des informations complémentaires et des conseils sur les questions de sécurité de l'information.

Le programme de sensibilisation à la SSI est actualisé annuellement afin de prendre en compte les évolutions de l'environnement technique, juridique, réglementaire et les incidents ou nouveaux risques impactant les SI.

#### 3.2.2.3 Validation du programme de sensibilisation à la SSI

Le programme de sensibilisation à la sécurité des systèmes d'informations doit être validé par les RSSI de chaque entité. Il doit être adapté au public concerné (utilisateur, développeur informatique, chef de projet SI, administrateur des SI, cadre, dirigeant, stagiaire, intérimaire, etc.).

#### 3.2.2.4 Formation à la SSI

Les collaborateurs de chaque entité en charge du développement, de l'administration et de la sécurisation des systèmes d'informations doivent être régulièrement formés à la SSI.

#### 3.2.2.5 Contrôle de l'efficacité de la sensibilisation à la SSI

Chaque entité met en place des moyens pour mesurer l'efficacité du programme de sensibilisation à la sécurité des systèmes d'information.

### 3.2.3 Processus disciplinaire

Un processus disciplinaire formel est connu de tous afin de prendre des mesures à l'encontre des salariés ou contractants ayant enfreint les règles liées à la sécurité de l'information.

#### 3.2.3.1 Non-respect des règles SSI

Le non-respect des consignes de sécurité des SI expose un collaborateur à des sanctions disciplinaires. Pour toute personne (interne, externe, temporaire) des sanctions civiles et pénales peuvent être encourues en cas de violation des législations et réglementations applicables en matière de SSI. Pour les prestataires, une sanction suffisamment grave peut conduire à la résiliation du contrat avec l'entreprise qui l'emploie.

#### 3.2.3.2 Déclenchement du processus disciplinaire

Le déclenchement du processus disciplinaire ne peut pas se faire avant d'avoir vérifié et prouvé l'existence de faute professionnelle.

Les violations délibérées des règles peuvent entrainer des actions immédiates.

#### 3.2.3.3 Processus disciplinaire

Le processus disciplinaire doit répondre aux exigences suivantes :

- Garantie du traitement correct et juste des collaborateurs suspectés d'avoir enfreint les règles de SSI ;
- Mise en œuvre d'une réponse graduée prenant en considération la nature et la gravité de la violation ainsi que son impact sur l'activité de l'organisation ;
- Prise en compte de facteurs comme la récidive, la formation adéquate délivrée en amont, les dispositions légales applicables, etc. ;
- Caractère dissuasif empêchant les collaborateurs d'enfreindre les politiques et procédures relatives à la SSI.

## 3.3 Rupture, terme ou modification du contrat de travail

Objectif : protéger les intérêts de l'organisation dans le cadre du processus de modification, de rupture ou du terme d'un contrat de travail.

### 3.3.1 Achèvement ou modification des responsabilités associées au contrat de travail

Les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue du terme du contrat de travail sont définies et communiquées au salarié et au tiers.

#### 3.3.1.1 Mouvements des collaborateurs et personnels temporaires

Tout collaborateur ou personnel temporaire amené à quitter l'entité, définitivement ou dans le cadre d'une mutation, doit expressément restituer tous les équipements informatiques et les données mis à sa disposition pour la réalisation de ses missions.

Les accès du collaborateur interne et externe sont résiliés afin d'interdire, notamment, tout accès au réseau après la date de fin du contrat conformément à la directive « 05. Contrôle d'accès ». Un collaborateur ou personnel temporaire n'est pas autorisé à conserver des données professionnelles après son départ.

#### 3.3.1.2 Gestion du mouvement des collaborateurs et personnel temporaires

Chaque entité doit définir une procédure de gestion des mouvements de collaborateurs et personnels temporaires. Elle formalise les actions à effectuer lors d'une arrivée, d'une mutation ou d'un départ. Cette procédure décrit au minimum :

- La création et la révocation des droits d'accès aux SI (réseaux et applicatifs) et aux locaux ;
- Les habilitations au Secret de la Défense Nationale ;
- L'affectation des équipements informatiques et téléphoniques.

#### 3.3.1.3 Responsabilité lors du mouvement des collaborateurs et personnel temporaires

Lors du mouvement d'un collaborateur ou d'un personnel temporaire, sa hiérarchie à la responsabilité de :

- S'assurer que l'intéressé a restitué la totalité de ses équipements ;
- De faire révoquer les profils et droits d'accès de l'intéressé.