DIRECTIVE STRATEGIQUE

10. SECURITE DES COMMUNICATIONS

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

Statut du document	Validé
Version	V 1.1
Date d'enregistrement	28/11/2019
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 sécurité des communications.

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
Terminal	Désigne un ensemble de périphériques se situant à l'extrémité d'un réseau informatique. Cela désigne communément un ordinateur portable, un smartphone, etc.
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

Le périmètre de cette Directive couvre principalement les types de services suivants :

- Les messageries « classiques » : permettant à un employé de La Poste d'envoyer et de recevoir des messages depuis un client de messagerie installé localement sur son Poste de Travail.
- Les Webmails : permettant à un employé de La Poste d'envoyer et de recevoir des messages depuis une interface « Web » accessible depuis un navigateur, en distinguant :
  - les services de Webmail proposés par La Poste ou Webmails internes, accessibles depuis Internet ou depuis le réseau interne de La Poste,
  - les services de Webmail externe, qu'il s'agisse de services « publics » (Yahoo ! Mail, Gmail, Hotmail, etc.) ou des solutions d'entreprise de certains tiers travaillant avec le La Poste (Webmail d'entreprise d'un prestataire par exemple).
- Les Webmails « Client » : cas particulier de Webmails faisant l'objet d'une offre de service propre proposée aux clients de La Poste (laposte.net par exemple).

3.1 Transfert de l'information

Objectif : maintenir la sécurité de l'information transférée au sein de l'organisation et vers une entité extérieure.

Toute information transférée au sein de l'organisation ou vers l'extérieur doit satisfaire aux exigences de sécurité de l'information définies par la PSSI-G (cf. directive « 04. Gestion des actifs et classification ») afin de garantir son intégrité et son niveau de confidentialité, quel que soit le type d'équipement de communication.

Le transfert d'informations peut se produire par le biais de nombreux types d'équipements de communication différents, dont la messagerie électronique, la voix, la télécopie et la vidéo.

3.1.1 Politiques et procédures de transfert de l'information

Les transferts d'information effectués par tous types d'équipements de communication sont réalisés conformément aux politiques et procédures de l'entité.

3.1.1.1 Documentation relative au transfert de l'information

La documentation relative au transfert de l'information prévoit :

- Les procédures conçues pour protéger l'information transférée contre l'interception, la reproduction, la modification, les erreurs d'acheminement et la destruction ;
- Les directives ou les procédures décrivant succinctement l'utilisation acceptable des équipements de communication ;
- L'utilisation de techniques de cryptographie ;
- Les mesures et les restrictions liées à l'utilisation des équipements de communication ;
- L'interdiction de laisser des messages comportant de l'information sensible sur les répondeurs.

L'accès aux infrastructures et aux données qu'elles contiennent est strictement encadré.

Il convient de prendre en compte les implications commerciales, légales et en termes de sécurité liées à l'échange de données électroniques, au commerce électronique et aux communications électroniques, ainsi que les exigences en matière de contrôles.

3.1.1.2 Sensibilisation des utilisateurs au transfert de l'information

Les utilisateurs de services de communication du Groupe La Poste doivent être sensibilisés régulièrement aux risques liés à ces services, ainsi qu'aux bonnes pratiques à adopter afin de limiter les risques liés aux transferts d'informations, en particulier sur :

- La responsabilité des utilisateurs des SI de ne pas compromettre l'organisation, en s'assurant de ne pas contribuer à des actes de diffamation, de harcèlement, d'usurpation d'identité, de renvoi de chaînes de messages, d'achats non autorisés, de divulgation de l'information sensible ;
- La nécessité d'identifier dans chaque message électronique le niveau de classification de celui-ci (C0 à C3) ;
- Les risque liés aux :
  - spam ou pourriel, envoi massif de messages à des fins publicitaires ou malhonnêtes,
  - mail-bombing, envoi massif de messages visant à saturer une boîte ou toute une infrastructure de messagerie,

- phishing ou hameçonnage, technique visant à extorquer des informations sensibles à un utilisateur dans le but de perpétrer une usurpation d'identité (typiquement ses coordonnées bancaires),
- scam, pratique frauduleuse visant à extorquer des fonds à un utilisateur,
- hoax ou canular avec la diffusion de fausses informations,
- vols ou détournements d'informations sensibles.

❑ Rappeler au personnel les problèmes qu'entraîne l'utilisation de télécopieurs ou de services de télécopie.

Les responsabilités des utilisateurs et administrateurs sont décrites dans les chartes du Groupe et des entités relatives à l'utilisation des S.I. et des accès aux informations.

3.1.2 Accords en matière de transfert d'information

Les accords passés avec les Tiers prévoient les modalités de transfert sécurisé de l'information entre les parties.

3.1.2.1 Accords en matière de transfert d'information

Dans le cas où un accord concernant le transfert sécurisé de l'information serait signé entre le Groupe La Poste et un tiers, ce dernier doit prendre en compte :

❑ Les responsabilités de gestion pour contrôler et informer de la transmission, de la répartition et de la réception ;
❑ Les procédures pour garantir la traçabilité et la non-répudiation comprenant la tenue à jour de la traçabilité de l'information en transit ;
❑ Les normes techniques minimales pour l'encapsulation et la transmission ainsi que la cryptographie pour la protection des pièces sensibles (cf. directive « 06. Cryptographie ») ;
❑ Les accords de séquestre ;
❑ Les normes d'identification coursiers ;
❑ Les obligations et les responsabilités en cas d'incident lié à la sécurité de l'information, comme la perte de données ; L'utilisation convenue d'un système de marquage pour l'information sensible ou critique, permettant de garantir une compréhension immédiate des marques et la protection appropriée de l'information ;
❑ Les normes techniques pour l'enregistrement et la lecture de l'information et des logiciels.

Les règles de la présente directive sont complétées et doivent s'appliquer conformément à la directive « 12. Relations avec les fournisseurs ».

3.1.3 Messagerie électronique

Des mesures de sécurité sont mises en œuvre afin de protéger l'information transitant par la messagerie électronique.

3.1.3.1 Autorisation des messageries électroniques

Tout service de messagerie électronique mis en œuvre au sein des SI du Groupe La Poste doit être connu et autorisé par la DSI de l'entité.

Aucun service de messagerie électronique ne pourra être utilisé avant d'avoir été autorisé par le Responsable de la Sécurité des Systèmes d'Information (RSSI) en collaboration avec sa DSI, cette autorisation dépendant de la conformité du service avec la présente directive.

Cette autorisation porte sur l'ensemble des composants techniques et organisationnels permettant de rendre, administrer et exploiter le service :

- Clients de messagerie ;
- Serveurs de messagerie ;
- Outils d'administration et d'exploitation ;
- Solutions de sécurité ;
- Procédures fonctionnelles et opérationnelles.

3.1.3.2 Services de sécurité des messageries électroniques

Chaque service de messagerie électronique adopté par le Groupe La Poste doit mettre en œuvre les composants permettant d'assurer un niveau de sécurité en rapport avec la criticité de ce service et de prévenir les risques inhérents au service.

Les composants doivent permettre de :

- Protéger les informations transférées contre l'interception, la reproduction, la modification, les erreurs d'acheminement et la destruction ;
- Assurer la détection et la protection contre les logiciels malveillants ;
- Protéger l'information logique sensible.

3.1.3.3 Autorisation des clients de messagerie

Seuls les clients de messagerie validés par le Groupe La Poste peuvent être installés sur un terminal utilisateur du Groupe La Poste. La présence d'un client de messagerie non validé par le Groupe La Poste sur un terminal utilisateur du Groupe La Poste constitue une faille de sécurité et doit donc être traitée comme un incident de sécurité.

3.1.3.4 Annuaire des comptes de messagerie

Tout compte permettant d'accéder à un service de messagerie électronique du Groupe La Poste doit être stocké dans un annuaire consultable et acceptant les requêtes légitimes d'authentification d'un autre équipement.

3.1.3.5 Règles liées aux flux de messagerie

Pour tout message émis et reçu via un service de messagerie électronique du Groupe La Poste, la chaîne de liaison mise en œuvre doit garantir :

- Qu'aucune pollution ne transite par le réseau interne du Groupe La Poste ;
- Qu'aucune pollution engageant la responsabilité du Groupe La Poste ne soit émise depuis son réseau interne.

Ces règles sont à appliquer conformément à la directive « 09. Réseau ».

3.1.3.6 Continuité de service des messageries électroniques

Des niveaux de réponse et de réactivité garantissant la continuité de service des messageries électroniques doivent être clairement définis et formalisés selon le niveau de criticité de ces derniers après analyse de risques.

3.1.3.7 Configuration du client de messagerie

La configuration des clients de messagerie, qu'il s'agisse de clients « lourds » installés localement sur le poste de travail ou de clients Web accessibles depuis un navigateur, doit faire l'objet d'un durcissement en matière de sécurité.

3.1.3.8 Antispam et antivirus

La chaîne de liaison d'un service de messagerie électronique doit mettre en œuvre, au minimum des fonctions antispam et antivirus équivalentes pour les messages émis et reçus.

Chaque serveur de la chaîne de liaison d'un service de messagerie électronique (relais et serveurs de messagerie) doit disposer de ses propres fonctions antispam et antivirus.

3.1.3.9 Gestion des notifications

Tout rejet d'un message reçu doit faire l'objet d'un message de notification au(x) destinataire(s) ainsi qu'aux administrateurs du service de messagerie électronique.

Tout rejet d'un message émis doit faire l'objet d'un message de notification à l'émetteur.

Concernant la notification des destinataires, elle est proscrite lorsqu'il s'agit d'un message externe.

Dans tous les cas, les administrateurs du service de messagerie sont notifiés.

3.1.3.10 Prévention des fuites d'information

Chaque architecture de messagerie du Groupe La Poste doit disposer d'une solution technique permettant de détecter les tentatives de fuites d'information et remonter des alertes documentées.

La détection d'une fuite d'information doit être traitée comme un incident de sécurité.

3.1.3.11 Usage exclusif de moyens qualifiés « secrets »

Aucun document ou information classifié C4 - Secret ne doit être échangé par les services de messagerie électronique courants du Groupe La Poste : messagerie « classique », Webmail, messagerie instantanée (cf. directive « 04. Gestion des actifs et classification »).

Dans le cadre précis de cette directive, la notion de document couvre aussi bien l'objet et le texte d'un message électronique que les éventuels fichiers joints.

L'échange de documents de cette nature est autorisé exclusivement par des moyens sécurisés qui doivent être préalablement validés et répertoriés par le RSSI de l'entité.

Dans le cas de réception d'informations sensibles par un tiers, cette règle doit s'appliquer.

3.1.3.12 Gestion des traces de messagerie électronique

La conservation, l'accès et l'exploitation des traces de messagerie électroniques doivent être conformes aux règles prévues par la directive « 08. Sécurité liée à l'Exploitation ».

Ces systèmes de gestion des traces de messagerie électronique contiennent des données personnelles (adresses de messagerie des émetteurs et destinataires) et doivent à ce titre, faire l'objet d'une inscription dans le registre du Règlement Général sur la Protection des Données. Pour les autres pays, il convient de se référer aux réglementations qui s'y appliquent.

3.1.3.13 Gestion des accès aux messageries électroniques

L'accès à un service de messagerie électronique du Groupe La Poste n'est pas autorisé depuis un terminal personnel.

L'accès à un service de messagerie électronique du Groupe La Poste depuis un équipement mobile communicant (Smartphones, tablettes, etc.) validé, répertorié et « enrôlé » par le Groupe La Poste est permis dans le respect des règles prévues par cette directive et par la directive « 02. Mobilité ».

3.1.3.14 Frontal avec Internet

Tout message provenant d'Internet ou émis vers Internet doit passer par une passerelle SMTP isolée du réseau interne du Groupe La Poste.

3.1.3.15 Utilisation de la messagerie électronique par une application

L'utilisation de la messagerie électronique par les applications des SI doit être strictement contrôlée, sécurisée et se limiter à l'envoi de message.

Cette règle s'adresse uniquement à des applications utilisant la messagerie pour l'envoi de mails vers des collaborateurs (par exemple des messages liés à la formation / la gestion du temps des collaborateurs,

etc.). Elle ne s'adresse pas à des applications participant à des processus Métiers (engagements contractuels ou commerciaux).

Le serveur de messagerie recevant un message à envoyer par une application doit authentifier le client SMTP utilisé par cette application.

Les comptes de messagerie applicatifs sont gérés au même titre que les comptes de messagerie de personne physique (cf. directive « 05. Contrôle d'accès »).

3.1.3.16 Utilisation de boîtes fonctionnelles

L'utilisation de boîtes fonctionnelles doit être strictement contrôlée et sécurisée. Elle répond aux mêmes exigences de sécurité applicables comptes de messagerie individuelle des collaborateurs, pour chaque boîte fonctionnelle son propriétaire est désigné nominativement.

3.1.3.17 Accès à la messagerie électronique par les tiers

Lorsque sa mission le justifie, un tiers peut accéder aux différents services de messagerie électronique du Groupe La Poste.

Cet accès doit être limité dans le temps et géré conformément aux règles d'accès aux SI prévues par la directive « 12. Relations avec les fournisseurs ».