DIRECTIVE STRATEGIQUE

04. GESTION DES ACTIFS ET CLASSIFICATION

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 gestion des actifs et à la classification.

Elle établit 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
Accédant	L'accédant peut être une personne physique, un équipement ou un traitement informatique (système, application, etc., cf. directive « 05. Contrôle d'accès »)
Actif	Toute ressource nécessaire à la réalisation de ses objectifs. On distingue les actifs essentiels et les actifs supports
Actif essentiel	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
Actif support	Composant technique ou non technique d'un système d'information sur lequel repose un bien essentiel. Les actifs supports regroupent les systèmes informatiques et de téléphonie, les organisations et les locaux qui hébergent les autres biens supports et fournissent les ressources
Donnée à Caractère Personnel (DCP)	Toute information relative à une personne physique susceptible d'être identifiée, directement ou indirectement, peu importe que l'information soit confidentielle ou publique (cf. directive « 15. Conformité et contrôle »)
Événement de sécurité	Changement d'état d'un système lié à sa protection et indiquant l'émergence d'un risque
Impact	Conséquence directe ou indirecte de l'insatisfaction des besoins de sécurité sur l'organisme ou sur son environnement
Incident	Evénement de sécurité identifié correspondant à une menace et affectant le fonctionnement nominal de tout ou partie d'un système d'information. Un incident porte atteinte à la disponibilité, l'intégrité, la confidentialité ou la traçabilité d'un système d'information
Intégrité	Propriété de protection de l'exactitude et de l'exhaustivité des actifs. Le critère d'intégrité défini la nécessité, pour un actif d'être identique et inaltérable dans le temps et dans l'espace et de certifier son exhaustivité, sa validité et sa cohérence
Niveau de sensibilité	Classification d'un actif suite à une évaluation du besoin de confidentialité. Les actifs doivent être manipulés en fonction de leur niveau de sensibilité et faire l'objet de mesures de sécurité adaptées. Tous les actifs doivent faire l'objet d'un marquage informant du niveau de sensibilité
Système d'information	Ensemble d'actifs supports organisé pour traiter des actifs essentiels

Terme	Description
Traçabilité	Journalisation des opérations pour permettre l'investigation en cas de dysfonctionnements ou d'incidents. Le critère de traçabilité fixe : ▸ le degré de preuve d'un événement ou de l'existence d'une information, ▸ le niveau de vérification du bon déroulement d'un traitement à l'aide de mécanismes d'audit, de traçabilité, d'imputabilité ou de non-répudiation.

3 Règles de sécurité applicables

3.1 Responsabilités relatives aux actifs

Objectif : identifier les actifs de l'organisation et définir les responsabilités appropriées en matière de protection.

3.1.1 Inventaire des actifs

Les actifs associés à l'information et aux moyens de traitement de l'information sont identifiés et tenus à jour au travers d'un inventaire.

3.1.1.1 Identification des actifs

Au sein du patrimoine informationnel, les actifs sont identifiés et classés en tant qu'actif essentiel ou actif support.

La granularité du niveau d'identification des actifs est dépendante du SI concerné.

L'exclusion d'un actif du périmètre de la revue, quel que soit la raison, doit être justifiée.

Le processus d'identification des actifs prend en compte les relations entre actifs.

L'inventaire des actifs est validé par le propriétaire.

La liste des actifs essentiels, des actifs supports et de leurs propriétaires respectifs est maintenue à jour.

3.1.1.2 Inventaire des actifs essentiels

Pour chaque actif essentiel, il faut au minimum mentionner les données suivantes :

- Nom du processus Métier ;
- Information essentielle concernée ;
- Utilisateur ;
- Propriétaire (nominatif ou fonctionnel).

A titre d'exemple, l'inventaire des actifs essentiels donne lieu à l'élaboration du tableau suivant :

Processus	Information essentielle	Utilisateur	Propriétaire
Gérer le contenu du site Web	▸ Informations société ; ▸ Fiche contact ; ▸ Charte graphique	Service communication	Directeur communication

3.1.1.3 Inventaire des actifs supports

Pour chaque actif support, il faut au minimum mentionner les données suivantes :

- ❑ Identification interne ;
- ❑ Spécifications techniques ;
- ❑ Emplacement géographique ;
- ❑ Propriétaire (nominatif ou fonctionnel) ;
- ❑ Prestataire (s'il y a lieu).

A titre d'exemple, l'inventaire des actifs essentiels donne lieu à l'élaboration du tableau suivant :

Processus	Identification	Spécification technique	Emplacement	Propriétaire	Prestataire
Gérer le contenu du site Web	SrvWebIntra	▸ Serveur RHAL 7.5 ; ▸ Apache 2.4	Salle serveur	DSI	Néant

3.1.2 Propriété des actifs

Un propriétaire est désigné pour chaque actif de l'inventaire.

3.1.2.1 Propriété des actifs

Conformément à la directive « 01. Organisation de la Sécurité des SI », les directions métiers de chaque entité doivent identifier et nommer un responsable métier – nominatif ou fonctionnel – en tant que propriétaire d'actif, pour chacun de leurs actifs essentiels et supports.

A chaque actif correspond un propriétaire unique.

Le propriétaire d'un actif est responsable de l'évaluation des risques pour les actifs dont il a la charge. Pour cela, il s'assure de leur classification et de leur protection.

Il définit et revoit périodiquement les classifications et les restrictions d'accès aux actifs. De même, il s'assure que leur suppression ou leur destruction soit convenablement réalisée.

Le propriétaire d'un actif est responsable et redevable pour cet actif (il n'est pas propriétaire au sens du droit de la propriété). Il s'assure de l'application des mesures de sécurité issues de l'analyse des risques.

Les directions métiers veillent à la continuité de la fonction de propriétaire d'actif, notamment en cas de mutation ou de départ du titulaire.

3.1.3 Utilisation correcte des actifs

Des règles d'utilisation de l'information, des actifs associés à l'information et des moyens de traitement de cette information sont définis, documentées et mises en œuvre.

3.1.3.1 Information des utilisateurs

Le propriétaire d'actifs s'assure que les utilisateurs de ses actifs soient informés des règles relatives à l'utilisation des actifs essentiels et supports.

3.1.3.2 Formalisation de l'utilisation des actifs

Les règles d'utilisation des actifs supports et essentiels sont formalisées au travers de documents de mise en œuvre, tenus à jour régulièrement.

3.1.4 Restitution des actifs

Au terme de leur période d'emploi (contrat ou accord), les salariés et les tiers doivent restituer l'ensemble des matériels appartenant à l'entité.

3.1.4.1 Fin de mission ou d'emploi

Toute fin de mission ou d'emploi doit s'accompagner d'un processus formalisé incluant la restitution de tous les actifs physiques appartenant à l'organisation.

Tout départ d'un collaborateur entraine la restitution des actifs essentiels en sa possession.

3.1.4.2 Mise au rebut et dé-commissionnement

Lorsqu'un actif support quitte définitivement une entité, le propriétaire de l'actif s'assure que les actifs essentiels qu'il contient sont effacés selon une procédure adaptée au niveau de sensibilité de l'actif concerné.

3.2 Classification de l'information

Objectif : s'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance pour l'organisation.

3.2.1 Classification des informations

Des critères sont définis afin de classer les informations détenues par l'entité (par exemple les informations peuvent être classées en termes de valeur, d'exigences légales, de sensibilité ou bien du caractère critique de ces informations pour l'entité).

3.2.1.1 Obligation d'évaluation des besoins de sécurité

Chaque actif support ou essentiel, qu'il soit utilisé de façon ponctuelle ou récurrente, de manière interne ou externe, doit être évalué.

Pour chaque Projet, la classification des actifs essentiels et supports concernés doit être réalisée au démarrage du Projet, conformément à la directive « 11. Gestion de projet ».

L'évaluation concerne son besoin de sécurité et le niveau d'impact en cas d'évènement redouté.

3.2.1.2 Critères d'évaluation des actifs

La classification des actifs doit être réalisée en évaluant leurs besoins de sécurité.

Cette classification consiste à évaluer, pour chaque actif essentiel ou support, son niveau de protection à appliquer en fonction des critères de disponibilité, d'intégrité, de confidentialité et de traçabilité.

Ces critères sont quantifiés selon l'échelle de besoins de sécurité ci-dessous :

Niv.	Confidentialité	Disponibilité	Intégrité	Traçabilité
0	C0 – Public L'actif est accessible publiquement après autorisation d'une entité habilitée à communiquer en dehors du Groupe et ne nécessitant aucune mesure de sécurité particulière			
1	C1 – Interne L'actif ne doit être accessible qu'à des accédants internes	D1 – Faible A déterminer dans les procédures opérationnelles	I1 – Détectable A déterminer dans les procédures opérationnelles	T1 – Faible A déterminer dans les procédures opérationnelles
2	C2 – Restreint L'actif ne doit être accessible qu'à des accédants issus de groupes ou de catégories de personnes identifiés	D2 – Importante A déterminer dans les procédures opérationnelles	I2 – Maîtrisée A déterminer dans les procédures opérationnelles	T2 – Nécessaire A déterminer dans les procédures opérationnelles
3	C3 – Confidentiel L'actif ne doit être accessible qu'aux accédants explicitement désignés et ayant besoin d'en connaître	D3 – Critique A déterminer dans les procédures opérationnelles	I3 – Intègre A déterminer dans les procédures opérationnelles	T3 – Essentielle A déterminer dans les procédures opérationnelles
4	C4 – Secret L'actif ne doit être accessible qu'à un nombre restreint de personnes nommément désignées	D4 – Vitale A déterminer dans les procédures opérationnelles	I4 – Intègre A déterminer dans les procédures opérationnelles	T4 – Vitale A déterminer dans les procédures opérationnelles

3.2.1.3 Évaluation de l'impact

Cette évaluation consiste à attribuer une valeur à l'impact sur le processus Métier d'un évènement redouté survenant sur un actif essentiel ou support.

L'évaluation de l'impact s'appuie sur l'échelle Groupe suivante :

Impact		Perte de CA	Perte de marge / résultat	Social	Sécurité du personnel	Atteinte à l'image
I1	Mineure	A compléter au niveau des entités	A compléter au niveau des entités	Débrayage ponctuel	Inconfort des agents	Doléances limitées de clients
I2	Significatif	A compléter au niveau des entités	A compléter au niveau des entités	Mouvement social local	Blessures légères ou stress élevé	Doléances importantes de clients
I3	Critique	A compléter au niveau des entités	A compléter au niveau des entités	Mouvement social local prolongé	Blessures moyennes	Campagne média locale
I4	Grave	A compléter au niveau des entités	A compléter au niveau des entités	Mouvement social massif et prolongé	Décès ou blessures sévères	Campagne média nationale

Une fois la note fixée pour chaque colonne, c'est la note la plus haute qui est retenue pour l'évaluation de l'impact de l'actif concerné.

3.2.1.4 Révision de la classification

La classification d'un actif est révisée régulièrement afin de prendre en compte toute évolution de son environnement.

Seul le propriétaire d'un actif peut valider le changement de son niveau de classification.

3.2.1.5 Niveau de classification des DCP

La classification des données à caractère personnel est réalisée conformément à la directive conjointe de la Direction de la Cybersécurité et du Délégué à la Protection des Données Groupe.

3.2.2 Marquage des informations

Des procédures permettant le marquage de l'information sont élaborées et mises en place conformément au plan de classification.

3.2.2.1 Marquage des documents numériques

Afin de communiquer sur la sensibilité de l'information qu'ils contiennent, les documents numériques doivent porter la mention de classification selon le critère de confidentialité.

Dans les emails, ce marquage est indiqué avant la signature.

Dans les documents de la suite office, ce marquage est réalisé dans les en-têtes ou les pieds de page.

3.2.3 Manipulation des actifs

Des procédures de traitement des actifs sont élaborées et mises en place conformément au plan de classification.

3.2.3.1 Règles de manipulation des documents numériques

La manipulation des documents classifiés doit faire l'objet de procédures détaillées, précisant comment manipuler, traiter, stocker et communiquer l'information en fonction de sa classification.

Pour chaque niveau de classification des actifs, les accès sont restreints en conséquence.

L'enregistrement des personnes autorisées à recevoir les actifs est formalisé et tenu à jour.

Les documents classifiés au niveau « C4 – secret » sont interdits dans l'environnement « pointCOM1 ».

4 Annexe – Liste des actifs supports

Type	Catégorie	Nom	Définition	Exemple
SYS	MAT	Ordinateur	Matériel informatique permettant de traiter automatiquement des données et comprenant les organes nécessaires à son fonctionnement autonome, ses interfaces de communication (ports, connecteurs et adaptateurs), et ses périphériques indispensables (écran, clavier, souris, etc.), qu'il soit fixe (conçu pour ne pas être déplacé manuellement et utilisé dans les locaux de l'organisme) ou mobile (conçu pour être déplacé manuellement et utilisé en des lieux différents)	Serveur, poste de travail, ordinateur central (mainframe), centre multimédia (media center), micro-ordinateur portable, assistant personnel, ardoise électronique
SYS	MAT	Périphérique informatique	Matériel informatique, optionnel, que l'on doit connecter à un ordinateur par une interface de communication (ports, connecteurs et adaptateurs), et qui réalise l'entrée ou la sortie de données	Imprimante, scanner, copieur multifonctions, périphérique de sauvegarde amovible (lecteur/graveur CD-ROM ou DVD-ROM, etc.), microphone, caméra, télécommande
SYS	MAT	Périphérique de téléphonie	Matériel de téléphonie qui réalise l'entrée ou la sortie de données	Téléphone analogique fixe, téléphone analogique sans fil, téléphone IP, téléphone mobile
SYS	MAT	Relais de communication	Dispositif intermédiaire ou relais, actif ou passif, informatique ou de téléphonie, qui transporte et aiguille des données	Pont, routeur, hub, commutateur téléphonique (PABX, IPBX), modem
SYS	MAT	Support électronique	Support électronique connectable à un ordinateur ou à un réseau informatique pour le stockage de données numériques.	CD-Rom, DVD-Rom, clé USB, cartouche de sauvegarde, disque dur amovible, bande, carte mémoire (Compact Flash, Memory

Type	Catégorie	Nom	Définition	Exemple
			Il est susceptible de contenir de grand volume de données tout en restant de petite taille. Il est utilisable à partir d'équipement informatique standard	Stick, Multimedia Card, Secure Digital, Smartmedia, etc.), disquette, cassettes
SYS	LOG	Application	Ensemble de composants logiciels (structure de stockage de données, librairies, interfaces conversationnelles, etc.) fournissant des services aux utilisateurs (génériques ou spécifiques à leur métier) en automatisant des tâches, fonctions ou processus. Il peut s'agir d'un produit commercialisé, développé spécifiquement ou personnalisé	Navigateur web, portail web, client de courrier électronique, suite bureautique, logiciel de comptabilité, téléprocédure administrative, application de pilotage de machine-outil, forum de discussion, logiciel réseau
SYS	LOG	Système de gestion de base de données	Ensemble de programmes permettant l'accès (séquentiel, par hachage ou indexé), l'ajout, la mise à jour et la recherche au sein d'une base de données	Ingres, PostgreSQL, DB2, Oracle, SQL Server, Informix
SYS	LOG	Intergiciel (middleware)	Logiciel de communication entre un système d'exploitation des applications, gérant les appels de fonctions de l'application ou de renvoi des résultats (par une interface de programmation), et mettant en forme des données pour la couche transport (par un protocole d'accès formaté)	EAI (Enterprise Application Integration), ETL (Extract-Transform-Load), CORBA (Common Object Request Broker Architecture), ODBC (Open DataBase Connectivity), NEXUS, ORB (Open Request Broker), moniteur transactionnel, MOM (Message Oriented Middleware)
SYS	LOG	Système d'exploitation	Logiciel d'un ordinateur constituant le socle opérationnel sur lequel vont s'exécuter l'ensemble des autres logiciels (services ou applications). Il comprend un noyau et des fonctions ou services de base. Selon les architectures, un système d'exploitation peut être monolithique ou	GCOS, MVS, Solaris, Linux, Windows95, Windows2000, WindowsXP, PalmOS, WCX, MacOS

Type	Catégorie	Nom	Définition	Exemple
			constitué d'un micro-noyau et d'un ensemble de services systèmes. Le système d'exploitation contient principalement tous les services de gestion du matériel (CPU, mémoire, disques, périphériques et interfaces réseaux), ceux de gestions des taches ou processus et ceux de gestion des utilisateurs et de leurs droits	
SYS	LOG	Micrologiciel (firmware)	Logiciel (interne, embarqué ou d'exploitation) intégré dans un composant matériel au sein d'une mémoire volatile (effacée lorsqu'elle n'est plus alimentée en électricité) ou non	BIOS (Basic Input Output System), gestionnaire de composants d'un téléphone mobile, programme stocké dans une clé USB équipée d'un microprocesseur, gestionnaire d'injection électronique d'un moteur à explosion
SYS	RSX	Canal informatique	Vecteur de communications informatiques et téléphoniques sous forme numérique	Cordon réseau, fibre optique, ondes radio, wifi
SYS	RSX	Canal de téléphonie analogique	Vecteur de communications téléphoniques sous forme analogique	Ligne téléphonique
ORG	PER	Personnes	Ce type de biens supports est constitué de l'ensemble des individus, catégories d'individus ou groupes sociaux homogènes, qui ont accès à tout ou partie des biens essentiels. On peut ainsi distinguer différentes fonctions (direction, encadrement, responsable, subordonné, etc.), métiers (secrétaire, juriste, informaticien, commercial, ingénieur, comptable, dépanneurs, etc.), ou statuts	Employés (développeur d'applications métiers, direction générale, chef de projet, manager, autorité d'homologation, utilisateur standard, exploitant, administrateur système ou de données, opérateur de sauvegarde, Help Desk, etc.), personnes ne faisant pas partie de l'organisme mais placées sous sa responsabilité (stagiaire, thésard, prestataire en régie, etc.), groupe projet

Type	Catégorie	Nom	Définition	Exemple
			(contractuel, fonctionnaire, stagiaire, visiteur, contracté, etc.)	
ORG	PAP	Supports papier	Ce type de biens supports est constitué de l'ensemble des supports statiques non électroniques contenant des données	Document manuscrit, document imprimé, diapositive, transparent, documentation, fax, photographie, radiographie
ORG	CAN	Canaux interpersonnels	Ce type de biens supports est constitué de l'ensemble des circuits organisationnels (canaux et processus organisationnels) et des échanges verbaux en face à face, qui transportent tout ou partie des biens essentiels	Circuit de validation par parapheur, processus de décision, circuit courrier, réunions, discussions de couloir
LOC	LOC	Locaux	Ce type de biens supports est constitué des infrastructures immobilières hébergeant, et nécessaires au bon fonctionnement, des systèmes informatiques (SYS) et des organisations (ORG), dans lesquels sont utilisés tout ou partie des biens essentiels	Site de Rennes, site d'exploitation au Maroc, usine au Pays-Bas, siège à Paris, locaux de l'organisme, périmètre particulier au sein des locaux, bureaux, bâtiment ou partie de bâtiment à usage de bureaux, de stockage, industriel, d'habitation ou mixte, pièce de stockage, salle serveur, salle de conférence, salle de réunion