DIRECTIVE STRATEGIQUE

07. SECURITE PHYSIQUE

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 de la sécurité physique et environnementale s'appliquant aux 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 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
Collaborateur	Personne physique travaillant au sein du Groupe La Poste ou d'une de ses filiales
Contrôle anti-piégeages	Activité visant à détecter et retirer les systèmes implantés frauduleusement dans les bâtiments du Groupe, visant à collecter du renseignement
Entité	Terme générique désignant La Poste maison-mère, ses branches, ses holdings et ses filiales
Local sécurisé	Appellation d'un local protégé par des mesures de sécurité particulière en fonction de la sensibilité des actifs qu'il renferme
Point d'importance vitale	Correspond aux composants névralgiques au sein du système de production. Ces derniers doivent être proposaient comme points d'importance vitale et font l'objet d'une protection particulière. Une directive nationale de sécurité spécifie les menaces à prendre en compte, les enjeux, les vulnérabilités et les objectifs de sécurité correspondants par secteur d'activité
Salle serveur	Espace clos et dédié dans lequel se trouvent les serveurs. Ces salles doivent faire l'objet de mesures de sécurités particulières afin de protéger les serveurs contre tous types de risques
Système sensible	Classification d'un actif ou d'une zone 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
Zone à Régimes Restrictifs (ZRR)	Correspond aux locaux abritant des activités de recherche ou de production stratégiques. Ces espaces reçoivent le statut de zones protégées, qualifiées de ZRR. Il peut s'agir notamment de bureaux, de laboratoires ou de plates-formes expérimentales. Ce statut permet légalement d'en interdire l'accès et prévoit des poursuites pénales en cas de tentative de captation ou d'intrusion sans autorisation préalable
Zone protégée	Appellation d'une Zone à Régimes Restrictifs
Zone réservée	Zone ayant pour but d'apporter une protection renforcée aux informations et supports ainsi qu'aux systèmes d'information classifiés au niveau Secret Défense. Une zone réservée ne peut être créée en dehors d'une zone protégée. Elle peut être incluse dans une zone protégée ou lui correspondre

3 Règles de sécurité applicables

3.1 Périmètres sécurisés

Objectif : empêcher tout accès physique non autorisé, tout dommage ou intrusion pouvant menacer les informations et les moyens de traitement de l'information de l'entité.

3.1.1 Périmètre de sécurité physique

Un site abritant des moyens de traitement des informations doit être physiquement solide, limiter les intrusions et convenablement protégés contre les accès non autorisés.

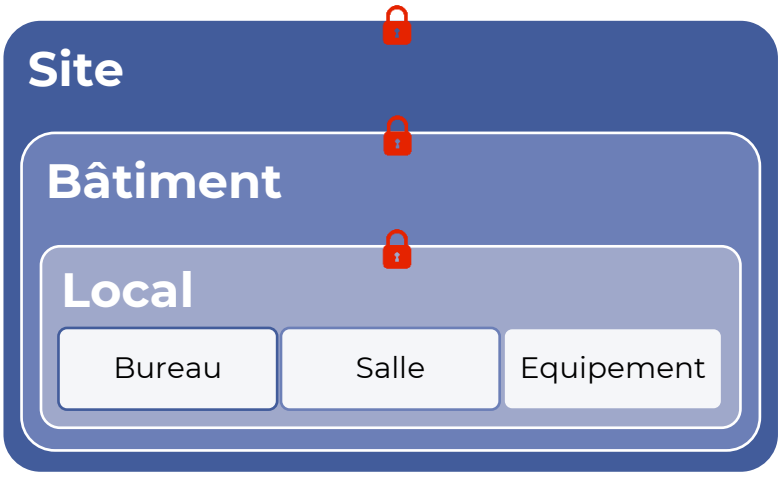
3.1.1.1 Définition du périmètre

Les périmètres de sécurité physiques sont formellement définis en prenant en compte :

- L'organisation de chaque activité ;
- Les règlementations applicables ;
- Les exigences relatives à la sécurité des actifs situés à l'intérieur ;
- Les conclusions de l'appréciation du risque.

Un périmètre de sécurité est défini au maximum par trois zones :

- Le ou les sites ;
- Le ou les bâtiments ;
- Le ou les locaux.



3.1.1.2 Evaluation du risque pour les sites hébergeant des infrastructures

Le choix d'implantation (l'emplacement) ou de sécurisation d'un site (ou d'un bâtiment ou d'un local) doit faire l'objet d'une analyse de risque avec un professionnel de la sécurité (par défaut le RSSI de l'entité concernée). Cette analyse déterminera le niveau requis de résistance du site (ou du bâtiment ou du local) et, la façon la plus adéquate de protéger les informations et les supports les plus importants qui y sont stockés ou archivés (communément appelés, les « biens essentiels »).

Si l'étude (analyse de risque) recommande de faire appel à au moins l'un des trois dispositifs règlementaire cité ci-dessous, le Directeur de la Sécurité Globale du Groupe (DSGG) devra être informé et consulté sans délais de tous les projets de : « zones protégées », « zones réservées », « points d'importance vitales », « zones à régimes restrictifs » :

- Dispositif règlementaire Protection du Secret de la Défense Nationale (PSDN) ;
- Dispositif règlementaire Sécurité des Activités d'Importance Vitale (SAIV) ;
- Dispositif règlementaire Protection du Patrimoine Scientifique et Technique (PPST).

3.1.1.3 Création de périmètres de sécurité

Des périmètres de sécurité sont définis et utilisés pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.

Ces périmètres de protection sont adaptés aux particularités techniques et économiques de l'organisation, tout en réduisant les risques mis en avant dans l'étude.

Le découpage de ces périmètres doit être effectué, en liaison avec le RSSI de l'entité et les services en charge de l'immobilier, de la sécurité et des moyens généraux.

Les moyens de traitement de l'information du Groupe La Poste sont séparés physiquement de ceux des opérateurs tiers.

3.1.1.4 Moyens de contrôles d'accès physique

Chaque zone doit bénéficier d'un dispositif de contrôle d'accès.

Des mécanismes de contrôle d'accès aux périmètres sécurisés doivent être mis en place. Ces mécanismes sont au minimum les suivants :

- Procédure de gestion des accès physique ;
- Limitation des accès aux seules personnes autorisées ;
- Personnel à l'accueil ;
- Système de surveillance ou télésurveillance ;
- Détection d'intrusion sur les portes extérieures et les fenêtres accessibles ;
- Alarme, verrous et portes coupe feux ;
- Protection contre les pannes électriques ;
- Protection contre les inondations ;
- Protection, le cas échéant, contre les menaces extérieures environnementales.

Ces mécanismes se conforment aux normes requises sur la résistance physique et la prévention des incendies.

Les procédures et les mécanismes doivent être régulièrement testés.

3.1.2 Contrôle physique des accès

Des contrôles adéquats à l'entrée des périmètres sécurisés sont mis en place afin de garantir que seul le personnel autorisé est admis.

3.1.2.1 Contrôle physique des accès

L'accès aux zones doit reposer sur un dispositif d'identification et d'authentification (contrôle d'accès par badge).

Ce dispositif doit bénéficier d'un maintien en condition de sécurité pérenne.

L'accès doit être réservé aux personnes ayant reçu une autorisation spécifique à travers un processus formel. Les instructions relatives aux exigences de sécurité de la zone et aux procédures d'urgence associées leurs sont remises.

L'ensemble des accédants doit porter son moyen d'identification visible.

Les locaux techniques (salles serveurs) sont considérés comme des zones à risques. A ce titre elles doivent bénéficier d'un contrôle d'accès approprié et renforcé. Une liste des personnes/fonctions autorisées à accéder à ces zones doit être formalisée. Cette liste doit être

régulièrement mise à jour en fonction des besoins d'accès réellement nécessaires (ajouts et retraits) et validée par un responsable.

3.1.2.2 Traçabilité et revue des accès

Une traçabilité électronique ou un journal physique de tous les accès est tenu à jour. Ces journaux sont conservés de manière sécurisée pour audit ultérieur.

Ces traces sont conservées un an, dans le respect des textes protégeant les données personnelles.

Un contrôle régulier des droits d'accès et des journaux d'accès devra être effectué. Les accès obsolètes sont révoqués suite à cette revue.

3.1.2.3 Accès accordés à des tiers

Une autorisation doit être accordée au personnel d'une organisation tierce chargé de l'assistance technique. Cet accès doit être limité aux zones et aux moyens de traitement de l'information, et uniquement en fonction du besoin.

Le tiers accédant intervient obligatoirement sous surveillance d'un personnel interne dans la salle serveur.

3.1.2.4 Accès aux sites réglementés

Certains processus de gestion et d'autorisation d'accès sont déjà explicités dans leurs cadres règlementaires respectifs : PSDN, SAIV, PPST.

Ces processus doivent respecter les exigences réglementaires des documents applicables.

3.1.3 Sécurisation des locaux et des équipements

Des mesures de sécurité physiques sont appliquées aux bureaux, aux salles et aux équipements.

3.1.3.1 Sécurisation des locaux

Dans la mesure du possible, les bâtiments sont discrets et donnent le minimum d'indications sur leur finalité, sans signe manifeste, extérieur ou intérieur, qui permette d'identifier la présence d'activités de traitement de l'information.

3.1.3.2 Sécurisation des équipements

Les équipements de la salle serveur ne sont pas accessibles au public et sont protégés des intrusions.

Les équipements sont configurés pour empêcher la divulgation des informations qu'ils contiennent.

Les activités des salles serveurs ne sont pas visibles et écoutables de l'extérieur.

3.1.4 Protection contre les menaces extérieures et environnementales

Des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents doivent être mise en œuvre.

3.1.4.1 Protection contre les menaces extérieures et environnementales

Des mesures préventives élaborées avec des spécialistes sont documentées pour éviter les catastrophes naturelles ou accidentelles.

Des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents sont conçues et appliquées en fonction de l'analyse de risque effectuée.

3.1.5 Travail au sein des locaux sécurisés

Des procédures pour le travail en zone sécurisée doivent être définies et appliquées.

3.1.5.1 Mesures organisationnelles

Des procédures pour le travail dans les périmètres sécurisés sont conçues et appliquées.

Seul le personnel ayant le besoin d'en connaître est informé de l'existence de périmètres sécurisés.

Tout équipement d'enregistrement (audio ou vidéo) est interdit sauf autorisation spécifique.

Le travail des tiers non supervisé/encadré en périmètre sécurisé doit être évité (hors salle serveur), tant pour des raisons de sécurité personnelle que pour prévenir toute possibilité d'acte malveillant.

Le travail des tiers non supervisé est interdit en salle serveur.

Les zones sécurisées inoccupées doivent être verrouillées physiquement et contrôlées périodiquement afin de s'assurer de l'intégrité du dispositif.

3.1.6 Zones de livraison et de chargement

Tous points d'accès et zones de livraison et de chargement par lesquels des personnes non autorisées peuvent pénétrer dans les locaux sont contrôlés.

3.1.6.1 Opération de livraison et de chargement

L'accès à la zone de livraison et de chargement depuis l'extérieur du bâtiment est limité au personnel identifié et autorisé.

Cette zone doit permettre de charger et de décharger des marchandises sans que le personnel ait accès aux autres parties du bâtiment.

Les portes extérieures des zones doivent être fermées lorsque les portes intérieures sont ouvertes.

3.1.6.2 Contrôle des produits entrants

Les produits entrants sont contrôlés pour vérifier la présence éventuelle de substances dangereuses ou de possibles altérations survenues lors de leur acheminement, avant qu'ils ne quittent la zone de livraison et de chargement.

Dès lors qu'une anomalie est constatée sur un produit entrant, il convient de prévenir immédiatement le personnel de sécurité.

Les produits entrants doivent être enregistrés conformément aux procédures de gestion des actifs (cf. directive « 04. Gestion des actifs et classification ») dès leur arrivée sur le site.

3.2 Matériels

Objectif : empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation.

3.2.1 Emplacement et protection du matériel

L'emplacement du matériel doit être déterminé et protégé en vue de réduire les risques liés à des menaces et dangers environnementaux et les possibilités d'accès non autorisés.

3.2.1.1 Emplacement du matériel

Un emplacement est déterminé pour le matériel afin de réduire au minimum les accès inutiles aux zones de travail.

Les matériels manipulant des données sensibles sont positionnés afin de réduire le risque que l'information puisse être vue par des personnes non autorisées.

Les emplacements doivent faire l'objet de mesures de protection adaptées à la classification des actifs hébergés.

3.2.1.2 Moyen de protection contre les menaces

Les moyens de stockage sont protégés contre tout accès non autorisé et des mesures sont prises visant à réduire au minimum les menaces physiques et environnementales potentielles.

Il est interdit de manger, boire et fumer en salle serveur.

Un contrôle permanent est effectué en salle serveur sur les conditions ambiantes (température et humidité).

La salle serveur est protégée contre les risques d'agression électromagnétiques.

3.2.2 Services généraux

Le matériel doit être protégé des coupures de courant et autres perturbations dues à une défaillance des services généraux.

3.2.2.1 Contrôles des services généraux

Le fonctionnement des services généraux tels que l'électricité, les télécommunications, l'alimentation en eau, le gaz, l'évacuation des eaux usées, la ventilation, la climatisation et la lutte contre l'incendie et les voies d'eau :

- ❑ Est conforme aux spécifications du fabricant du matériel et aux exigences légales locales ;
- ❑ Fait l'objet d'un contrôle régulier vérifiant sa capacité à répondre à la croissance de l'entité et aux interactions avec les autres fournisseurs de services généraux ;
- ❑ Est examiné et testé de manière régulière pour s'assurer du correct service rendu ;
- ❑ Est équipé, si nécessaire, d'alarmes de détection ;

- Dispose, si nécessaire, d'alimentations multiples sur les réseaux physiques d'acheminement.

3.2.2.2 Résilience des services généraux

Des systèmes d'éclairage et de communication d'urgence sont prévus en cas d'incident.

Des interrupteurs et des robinets de secours destinés à couper le courant, l'eau, le gaz ou autres services sont placés près des sorties de secours ou des salles contenant le matériel.

3.2.3 Sécurité du câblage

Les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information doivent être protégés contre toute interception, interférence ou dommage.

3.2.3.1 Emplacement des câblages

Il convient d'enterrer, dans la mesure du possible, les lignes électriques et les lignes de télécommunication branchées aux moyens de traitement de l'information ou de les soumettre à toute autre forme de protection physique adéquate.

Les câbles électriques doivent être séparés des câbles de télécommunication pour éviter toute interférence.

3.2.3.2 Mesures complémentaires pour les systèmes et données sensibles

Les mesures suivantes peuvent être mises en place pour les systèmes nécessitant une protection spécifique :

- L'installation d'un conduit de câbles blindé et de chambres ou de boîtes verrouillées aux points d'inspection et aux extrémités ;
- L'utilisation d'un blindage électromagnétique pour assurer la protection des câbles ;
- Le déclenchement d'inspections physiques techniques pour détecter le branchement d'appareils non autorisés sur les câbles ;
- Un accès contrôlé aux panneaux de répartition et aux chambres de câblage ;

- Des contrôles anti-piégeages réguliers, effectués par du personnel formé. Il peut être fait appel à des services spécialisés (opérations dites de « dépoussiérage »).

3.2.4 Maintenance du matériel

Le matériel doit être convenablement entretenu pour garantir sa disponibilité permanente et son intégrité.

3.2.4.1 Maintien en condition de fonctionnement

Il convient d'entretenir et de réparer le matériel selon les spécifications et la périodicité recommandées par le fournisseur, par du personnel de maintenance autorisé, tout en respectant les exigences imposées par les polices d'assurance.

Un dossier de toutes les pannes et de toutes les tâches de maintenance préventives ou correctives est conservé.

3.2.4.2 Maintenance externe

Lorsque la maintenance d'un matériel est planifiée, des mesures appropriées sont mises en œuvre en prenant en compte le fait qu'elle soit effectuée par du personnel sur site ou extérieur à l'organisation.

Lorsque cela est nécessaire, l'information sensible contenue dans le matériel est effacée ou bien, le personnel de maintenance reçoit les autorisations nécessaires à l'intervention.

3.2.4.3 Remise en service

Avant de remettre le matériel en service, il doit être inspecté afin de s'assurer qu'il n'a pas subi d'altérations et qu'il fonctionne correctement.

3.2.5 Sortie des actifs

Une autorisation préalable est obtenue avant toute sortie de matériels, d'informations ou de logiciels des locaux.

3.2.5.1 Sortie des actifs

Les salariés et les tiers ayant autorité pour extraire des actifs du site sont identifiés.

Une fiche de suivi des actifs est complétée à chaque mouvement afin d'en assurer le suivi. Elle comprend les informations suivantes :

- La description de l'actif ;
- L'identité, la fonction et l'affiliation du détenteur ;
- La date de sortie de l'actif ;
- La date de restitution de l'actif.

Une revue est effectuée périodiquement afin de vérifier la date des retours des actifs sortis.

3.2.6 Sécurité du matériel et des actifs hors des locaux

Le travail à distance fait l'objet d'un chapitre spécifique au sein de la directive « 02. Mobilité ».

3.2.6.1 Utilisation d'actifs hors locaux

L'utilisation des matériels de traitement et de stockage de l'information détenus par l'entité hors des locaux après validation formelle, est autorisée.

3.2.6.2 Mesures de sécurité pour les actifs hors locaux

Il est interdit de laisser le matériel et les supports de données extraits des locaux prévus pour leur hébergement sans surveillance dans des lieux publics.

Les instructions du fabricant visant à protéger le matériel doivent être respectées.

Des mesures pour les emplacements de travail hors site, comme le travail à domicile, le télétravail et les sites temporaires, doivent respecter les règles en vigueur conformément à la directive « 02. Mobilité ».

3.2.6.3 Traçabilité

Lorsque du matériel circule hors des locaux de l'entité entre différentes personnes ou entre des tiers, un journal détaillant la chaîne de traçabilité du matériel, mentionnant au minimum les noms des personnes responsables du matériel, ainsi que les entités dont elles relèvent doit être établi.

3.2.7 Mise au rebut ou recyclage sécurisé du matériel

Avant la mise au rebut ou réutilisation de matériel contenant des supports de stockage, les données sensibles et les logiciels sous licence doivent avoir été effacés de manière sécurisée.

3.2.7.1 Mise au rebut ou recyclage sécurisé du matériel

Avant la mise au rebut ou la réutilisation du matériel, il convient de vérifier s'il contient ou non un support de stockage et le retirer (serveur principalement).

Lorsque cela n'est pas possible (par exemple les postes de travail, terminaux mobiles), les données non chiffrées doivent être effacées de manière sécurisée avant mise au rebut, réutilisation ou maintenance.

L'effacement des données sensibles doit s'appuyer sur des produits qualifiés[1] ou respecter des procédures établies en concertation avec les RSSI des entités.

3.2.7.2 Destruction sécurisée du matériel

Les supports de stockage internes au matériel contenant de l'information sensible ou protégée par le droit d'auteur (logiciel) doivent être détruits physiquement.

Si cela n'est pas possible, l'information doit être détruite, supprimée ou écrasée en privilégiant les techniques la rendant irrécupérable.

3.2.8 Matériel utilisateur laissé sans surveillance

Les utilisateurs s'assurent que le matériel sans surveillance est doté d'une protection appropriée.

3.2.8.1 Responsabilité et sensibilisation des utilisateurs

Les utilisateurs sont sensibilisés aux exigences et aux procédures de sécurité destinées à protéger les matériels laissés sans surveillance et

[1] La qualification de produits de sécurité fait l'objet du chapitre III du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les autorités administratives et les usagers. Elle permet d'attester de la conformité d'un produit de sécurité au RGS (dont la première version en entrée en vigueur le 6 mai 2010 par arrêté du Premier ministre). Elle prévoit trois niveaux de qualification, un niveau élémentaire, un niveau standard et un niveau renforcé.

aux responsabilités qui leur incombent pour assurer la mise en œuvre de cette protection.

Il est notamment recommandé aux utilisateurs :

- De fermer les sessions actives lorsqu'ils ont terminé ;
- De se déconnecter des applications ou des services en réseau lorsqu'ils n'en ont plus besoin ;
- Lorsqu'ils ne s'en servent pas, de protéger les ordinateurs ou les appareils mobiles contre toute utilisation non autorisée par un dispositif équivalent tel qu'un mot de passe ;
- De protéger leur poste portable en utilisant le câble de sécurité fourni ;
- De protéger des indiscrétions visuelles (filtre écran) les postes de travail.

3.2.9 Politique du bureau propre et de l'écran vide

Pour les documents papier et les supports de stockage amovibles, la politique du « bureau propre » est adoptée et, pour les moyens de traitement de l'information une politique de l'écran vide.

3.2.9.1 Politique de bureau propre

Une politique du « bureau propre » et de l'écran vide est mise en place. Elle tient compte des classes d'information, des exigences légales et contractuelles, des risques associés et de la culture de l'organisation.

3.2.9.2 Protection des informations et des actifs sensibles

Lorsque l'information sensible liée à l'activité de l'entité n'est pas utilisée, qu'elle soit sous format papier ou sur un support de stockage électronique, il convient de la mettre sous clé (de préférence dans un coffre-fort, une armoire ou tout autre meuble de sécurité), notamment lorsque les locaux sont vides.

Les ordinateurs et les terminaux laissés sans surveillance doivent être déconnectés ou protégés par un verrouillage de l'écran ou du clavier contrôlé par un mot de passe, un jeton ou un autre mécanisme d'authentification de l'utilisateur. Lorsque cela est possible les sessions inactives pendant plus de 5 minutes doivent être verrouillées sur tous les postes.

Ils doivent également être protégés par des clés, des mots de passe ou d'autres mesures de sécurité lorsqu'ils ne servent pas.

3.2.9.3 Sécurité des imprimantes et des photocopieurs

L'utilisation des photocopieurs et autres appareils de reproduction est encadrée. Leur utilisation est soumise à l'authentification des utilisateurs.

Les documents contenant de l'information sensible doivent immédiatement être retirés des imprimantes et photocopieurs.

3.3 Manipulation des supports

3.3.1 Gestion des supports amovibles

Une procédure de gestion des supports amovibles est mise en place conformément au plan de classification défini.

3.3.1.1 Procédure de gestion des supports amovibles

Une procédure de gestion des supports amovibles est rédigée et appliquée conformément à la directive « 04. Gestion des actifs et classification ». Elle prend en compte toutes les règles ci-dessous.

3.3.1.2 Protection

Toute récupération du contenu d'un support réutilisable est proscrite et doit être rendue impossible avant sa réattribution ou sa destruction.

Les supports amovibles sont stockés dans un environnement sûr, sécurisé et conforme aux spécifications du fabricant.

Des techniques cryptographiques pour protéger les données sensibles figurant sur le support amovible doivent être utilisées (cf. directive « 06. Cryptographie »).

3.3.1.3 Gestion des supports au long du cycle de vie

Pour limiter les risques liés à la dégradation du support lorsque les données stockées sont encore nécessaires (sauvegardes), ces données doivent être transférées sur un support neuf, avant qu'elles ne soient corrompues.

Des copies de données de valeur doivent être réalisées sur des supports séparés pour réduire les risques concomitants d'endommagement ou de perte de données.

Un registre des supports amovibles doit être tenu à jour pour limiter les risques de perte de données et garantir le bon contrôle des règles ci-dessus.

3.3.2 Mise au rebut des supports

Des procédures formelles assurent une mise au rebut sécurisée des supports inutilisés.

3.3.2.1 Formalisation des procédures

Des procédures formelles de mise au rebut sécurisée des supports réduisent au minimum le risque de fuites d'information sensible.

3.3.2.2 Mise au rebut sécurisée

Les supports contenant de l'information sensible sont stockés et mis au rebut de façon sûre et sécurisée, par incinération ou déchiquetage. Les données utilisées dans d'autres applications de l'entité sont effacées. La mise au rebut des éléments sensibles pour en assurer la traçabilité est journalisée.

3.3.2.3 Externalisation de la mise au rebut sécurisée

En cas d'externalisation du processus de mise au rebut, (collecte et enlèvement des supports) le prestataire doit être choisi avec soin conformément à la directive « 12. Relation avec les fournisseurs ».

3.3.3 Transfert physique des supports

Les supports contenant de l'information doivent faire l'objet d'une protection lors de leur transport contre les accès non autorisés, l'utilisation frauduleuse ou l'altération. Cette protection est proportionnelle au niveau de classification des données contenues.

3.3.3.1 Gestion des coursiers et des transporteurs

La liste des coursiers et transporteurs autorisés est établie et validée par la hiérarchie opérationnelle en charge de la destruction des supports.

Des procédures de contrôle de l'identification des coursiers et des transporteurs sont mises en œuvre.

3.3.3.2 Protection des supports lors du transport

L'emballage choisi pour le transport doit être suffisant pour protéger le contenu contre tout dommage physique. L'accès au support durant le transport doit être rendu impossible.

Il est conforme aux spécifications du fabricant contre tout facteur environnemental pouvant diminuer l'efficacité de la restauration du support, comme l'exposition à de fortes températures, à une forte humidité ou à des champs électromagnétiques.

Les journaux identifiant le contenu du support, la protection appliquée, ainsi que les dates et heures de remise aux responsables du transport et de réception par le destinataire sont conservés.