DIRECTIVE STRATEGIQUE

05. CONTROLE D'ACCES

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 au contrôle des accès.

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
Accédant	L'accédant peut être une personne physique, un équipement ou un traitement informatique (système, application, etc.) qui cherche à établir une communication ou une connexion à un système ou à une application
Approbateur	L'approbateur approuve formellement la demande d'habilitation du Demandeur. Cette approbation a un double objectif : ▸ Garantir l'identité du futur accédant ; ▸ Confirmer la fonction et la mission du futur accédant auprès du responsable des habilitations. Il s'assure que les besoins exprimés par le Demandeur sont cohérents avec l'activité de l'accédant. Il signale au Responsable des Habilitations toute évolution relative au statut de l'accédant (mutation ou départ de l'utilisateur, application retirée de la production, etc.) Il est le plus souvent il s'agit du supérieur hiérarchique du demandeur accédant
Authentification	L'authentification est l'opération par laquelle un équipement ou un traitement informatique (système, application) vérifie que l'accédant qui souhaite se connecter est bien celui qu'il prétend être. S'authentifier = apporter la preuve de son identité Cette opération peut s'appuyer sur : ▸ Une information que l'accédant connaît : un secret, un mot de passe, etc. ; ▸ Une information que l'accédant possède : une carte à puce, un « token », etc. ; ▸ Une information qui lui est propre : une empreinte digitale, le son de sa voix, etc. Dans le processus de connexion à un SI et à ses ressources, l'authentification est le premier point de contrôle logique. L'authentification est à ce titre un mécanisme incontournable permettant de maîtriser les accès aux ressources du SI. De sa qualité et de sa robustesse dépendent la sûreté de l'information et sa protection contre des accès illicites
Bénéficiaire	Le "bénéficiaire" est la personne qui de fait, dispose d'une situation déterminée dont il tire un intérêt. Le mot est ici synonyme de "titulaire"
Compte à privilèges	Les comptes à privilèges sont des comptes bénéficiant de droits étendus (appelés privilèges), par rapport aux utilisateurs normaux ou réguliers. Ces privilèges

Terme	Description
	permettent de réaliser des actions sur le système, l'application, etc. Les comptes privilégiés sont par exemple des comptes d'administrateurs ou des comptes d'utilisateurs disposant de droits à fort impact métier dans une application
Compte d'administration	Les comptes d'administration sont des comptes à privilèges utilisés afin de permettre le maintien en condition opérationnelle et de sécurité du SI, et à gérer des changements mineurs ou des évolutions majeures
Contrôleur	Le contrôleur veille au respect des règles de sécurité, sous la forme d'un contrôle permanent ou de contrôles périodiques
Demandeur	Le demandeur renseigne la demande d'habilitation en précisant les besoins d'accès du futur accédant. Il peut être un utilisateur, un exploitant, un acteur d'un projet, etc. Lorsque le besoin concerne un équipement ou un traitement informatique, le demandeur est le responsable désigné de l'équipement ou du traitement informatique
Droits d'accès	Les droits d'accès sont des privilèges attribués à un utilisateur pour accéder à des ressources (systèmes, informations, etc.)
Habilitation / Accréditation	L'habilitation est l'action d'attribuer à un accédant des droits d'accès à une application, un système ou des informations. Il peut aussi être utilisé le terme d'accréditation
Identification	L'identification est l'opération par laquelle un équipement ou un traitement informatique (système, application) s'assure qu'il connaît l'accédant qui cherche à se connecter. S'identifier = communiquer son identité = obtenir un identifiant unique C'est par l'identification que l'on peut faire un lien entre une action et une personne ou une application. Toutes les possibilités d'audit reposent sur ce lien. Des règles doivent donc être définies pour que ce lien existe réellement et soit utilisable et opposable en cas de contrôle
Propriétaire d'Information / Responsable Métier	Le propriétaire d'information classifie les informations dont il a la charge conformément à la directive « 04. Gestion des actifs et classification » selon les critères de sécurité, disponibilité, intégrité, confidentialité et preuve et en déduit les exigences fonctionnelles sur les accès logiques à ces informations.

Terme	Description
	Il définit notamment les types de droits et les règles de gestion des droits d'accès à ces informations. Il les communique aux administrateurs et aux responsables des habilitations et les révise à l'occasion des évolutions des applications supportant ces informations. Le propriétaire d'information dispose des prérogatives nécessaires pour contrôler la bonne mise en application des règles qu'il a définies. Dans le cadre de ces contrôles, il peut disposer des listes des droits d'accès attribués et plus généralement des comptes rendus des activités liées à la gestion des droits d'accès
Responsable des Habilitations	Le responsable des habilitations est chargé de la validation de la demande et de l'identification des droits à donner à l'accédant en s'appuyant sur les règles définies par les propriétaires d'information et sa connaissance des métiers. Il réalise par ailleurs le suivi des droits d'accès et remonte aux propriétaires d'information et aux approbateurs : ▸ Toute information nécessaire au suivi des droits d'accès (comptes rendus, tableaux de bord, etc.) ; ▸ Tout incident relatif à la gestion des droits d'accès qui les concerne ; ▸ Toute demande non couverte par les règles de gestion des droits d'accès

3 Règles de sécurité applicables

Le contrôle des accès logiques est exercé lorsqu'un accédant cherche à établir une communication ou une connexion à un système ou une application.

L'accédant peut être une personne physique, un équipement ou un traitement informatique (système, application, etc.).

Le contrôle des accès logiques comprend obligatoirement :

- Une identification ;
- Une authentification ;
- Un contrôle des droits de l'accédant.

3.1 Exigences métiers en matière de contrôle d'accès

Objectif : Limiter l'accès à l'information et aux moyens de traitement de l'information.

Les accès aux SI sont tracés, historicisé et analysés dans le but de détecter toute tentative d'accès non autorisé, en fonction de la criticité du SI concerné.

L'accès à toute ressource du SI de l'entreprise fait l'objet de contrôles. Ils reposent sur les principes d'identification, d'authentification et d'autorisation individuelle et systématique du bénéficiaire de cet accès.

En cas d'externalisation ou de sous-traitance, le Groupe La Poste doit conserver en interne la maîtrise du processus de création et d'attribution des droits d'accès.

3.1.1 Procédure de contrôle d'accès

Chaque entité doit définir, appliquer et contrôler les accès à ses SI au regard des besoins Métiers et des risques (profils, rôles, respect de la séparation des tâches, niveau d'exposition depuis l'interne ou l'externe, arrivées et départs d'utilisateurs du SI, etc.) conformément aux règles décrites dans la directive.

3.1.1.1 Formalisation des processus de gestion des droits d'accès

Les processus de gestion des droits d'accès au réseau et aux applications sont définis en matière d'exigences de sécurité applicables au métier,

documentés et auditables selon l'organisation de chaque activité, en s'appuyant sur la directive « 04. Gestion des actifs et classification ».

Ils s'imposent à tous les Propriétaires des actifs, avec l'appui des Maîtrises d'Ouvrage des SI.

Ces documents sont diffusés auprès des entités en charge des processus d'habilitation et mis à jour dès que nécessaire.

Le processus inclut au minimum :

- La prise en compte de la législation et les obligations contractuelles applicables relatives à la limitation de l'accès aux données ou aux services ;
- Le cloisonnement des rôles en vue d'assurer la juste ségrégation des tâches. Par exemple la demande d'accès, l'autorisation d'accès et l'administration des accès doit être réalisée par des personnes différentes ;
- L'archivage des enregistrements de tous les événements significatifs relatifs à l'utilisation et à la gestion des identités des utilisateurs et des informations d'authentification secrètes.

Le processus de contrôle d'accès est régi selon les principes suivants :

- Le besoin d'en connaître : on n'a accès qu'à l'information dont on a besoin pour réaliser ses tâches (différentes tâches/fonctions impliquent des besoins d'en connaître différents, d'où des profils d'accès différents) ;
- Le besoin d'utiliser : on n'a accès qu'aux moyens de traitement de l'information (matériel informatique, applications, procédures, salles) dont on a besoin pour accomplir sa tâche/son travail/son rôle.

3.1.1.2 Classification des actifs

Le Propriétaire d'actif classifie les informations dont il a la charge conformément à la directive « 04. Gestion des actifs et classification » selon les critères de sécurité de Disponibilité, Intégrité, Confidentialité, Traçabilité (D, I, C, T). Il en déduit les exigences fonctionnelles sur les accès logiques à ces informations. Lorsque des données à caractère personnel sont traitées, ces exigences sont conformes aux recommandations de la CNIL.

Il définit notamment les droits et règles de gestion des droits d'accès à ces informations.

3.1.2 Accès aux réseaux et aux services en réseau

Les utilisateurs n'accèdent qu'aux seuls services pour lesquels ils sont autorisés.

3.1.2.1 Procédure d'accès

Les procédures relatives à l'accès aux réseaux et des services en réseau sont définies en cohérence avec la présente directive et couvre :

- ❑ Les réseaux et les services en réseau pour lesquels l'accès a été accordé ;
- ❑ Les procédures d'autorisation désignant les personnes autorisées ;
- ❑ Les procédures et mesures de gestion destinées à protéger l'accès aux connexions ;
- ❑ Les moyens utilisés pour y accéder ;
- ❑ Les exigences d'authentification de l'utilisateur ;
- ❑ La surveillance de l'utilisation faite de ces services en réseau.

Ces procédures s'inscrivent dans un processus RH de circuit d'arrivée / départ / mobilité.

3.2 Gestion de l'accès utilisateur

Objectif : maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information.

Tout bénéficiaire d'un accès au SI de l'entreprise est considéré comme un utilisateur du SI de l'entreprise.

Tout accès logique à une ressource non publique des SI du Groupe La Poste nécessite :

- ❑ Une identification et une authentification préalables de l'accédant ;
- ❑ Une vérification des droits d'accès de l'accédant sur la ressource.

Les accès anonymes aux ressources internes sont strictement interdits.

3.2.1 Enregistrement des utilisateurs

Une procédure d'enregistrement et de sortie des utilisateurs est formalisée afin de permettre l'attribution de droits d'accès.

3.2.1.1 Processus de gestion des identifiants

Un processus de gestion des identifiants doit être formalisé et validé.

Il doit prendre en compte au minimum les étapes suivantes :

- ❑ Demande d'un identifiant, en garantissant sa validation par une fonction habilitée ;
- ❑ Attribution d'un identifiant à un accédant ;
- ❑ Suppression d'un identifiant lorsque celui-ci ne doit plus accéder aux SI.

Le processus doit préciser les éléments de traces concernant sa réalisation, qui doivent être conservés.

3.2.1.2 Caractère Individuel et confidentiel du couple Identifiant/Authentifiant

Le couple identifiant / authentifiant est obligatoire. Il est personnel, confidentiel et incessible. Il est interdit de modifier le processus d'authentification notamment de supprimer l'authentifiant.

Par conséquent les identifiants personnels génériques ou partagés sont proscrits.

3.2.1.3 Caractère personnel / unique de l'identifiant

Tout accédant doit disposer d'un identifiant individuel qui l'identifie de manière unique au sein du SI, par un dispositif qui permet d'établir le lien entre cet identifiant et la personne physique (référentiel d'identité) ou la ressource (référentiel des biens).

3.2.1.4 Construction des identifiants

Les identifiants doivent être construits selon des règles établies et doivent être basés sur une convention de nommage.

3.2.2 Maîtrise de la gestion des accès utilisateurs

Un processus formel est mis en place pour la gestion des accès de l'ensemble des utilisateurs des SI de l'entité (attribution et révocation de droits).

3.2.2.1 Approbation des demandes d'accès

La demande d'habilitation est vérifiée et validée selon les règles définies dans la procédure et dans le respect de la séparation des tâches.

Les accès aux réseaux sont soumis à validation du responsable hiérarchique.

Les accès aux données applicatives sont soumis à validation du propriétaire des données.

3.2.2.2 Suivi des demandes d'accès

Chaque demande d'accès formalisée est enregistrée et conservée dans un outil de gestion centralisé permettant le suivi des demandes.

Tout besoin de modification de droits d'accès doit faire l'objet d'une nouvelle demande d'habilitation afin d'en respecter le cycle de validation.

Une revue périodique des droits est réalisée, la périodicité est déterminée par la sensibilité des actifs et ne peut dépasser un an.

3.2.2.3 Droits d'accès temporaires

Des droits d'accès temporaires peuvent être mis en place pour des acteurs ayant besoin d'un accès limité dans le temps (par exemple : expertise ponctuelle, intervention sur incident, audit, etc.).

La période d'accès temporaire est définie dès le départ et doit être techniquement limitée dans l'outil (date de fin).

3.2.3 Gestion des privilèges d'accès

Les accès privilégiés doivent être restreint et leur utilisation contrôlée.

3.2.3.1 Spécificité des comptes d'accès privilégiés

Les comptes à privilèges ne sont utilisés que pour les activités et besoins liés aux tâches d'administration ou d'exploitation.

Ces tâches sont réalisées via un identifiant nominatif spécifique (administrateur).

Toute autre opération doit être effectuée depuis un compte standard.

En conséquence, dans le cas où l'administrateur est également utilisateur du système, deux comptes distincts doivent être créés.

Les comptes d'accès privilégiés doivent être identifiés dans chaque système, applicatif ou base de données. Les identifiants génériques sont proscrits dans les limitations techniques des systèmes.

Tous les comptes d'administration doivent être rattachés à une personne physique.

3.2.3.2 Principe du moindre privilège

Le principe du moindre privilège consiste à ne pas attribuer plus de droits que ne l'exigent les activités professionnelles de l'accédant. Ce principe s'applique à deux niveaux :

- Lors de la définition des droits, en s'assurant qu'ils sont bien adaptés aux activités ;
- Lors de l'attribution des droits à l'accédant, en lui octroyant une liste minimale de droits mais suffisante pour l'exercice de son activité.

3.2.3.3 Droits d'accès aux fonctions privilégiées

L'accès aux fonctions privilégiées (fonctions Métiers sensibles, fonction d'administration technique) doit être restreint :

- L'autorisation d'accès à ces fonctions privilégiées relève d'une procédure d'habilitation spécifique ;
- Des mesures de sécurité spécifiques (type d'authentification, délai de validité du compte, traçabilité, contrôle, etc.) doivent être mises en place ;
- Les droits sont listés dans un outil dédié et sont revus périodiquement au minimum, semestriel ;
- Chaque responsable applicatif doit s'assurer du besoin d'en connaître des accédants à son système en procédant à une revue au minimum annuelle.

3.2.3.4 Restriction des droits

Sauf exception dûment motivée et validée par le RSSI de l'entité, les utilisateurs n'ont pas de droits d'administration.

3.2.3.5 Gestion des actions d'administration

Les opérations d'administration doivent être tracées de manière à pouvoir gérer au niveau individuel l'imputabilité des actions d'administration.

Les modifications aux comptes à privilèges doivent être journalisées et font l'objet d'une revue périodique.

3.2.3.6 Sécurisation des outils de prise de main à distance

La prise de main à distance d'une ressource informatique locale ne peut être effectuée que par les exploitants autorisés, après s'être authentifiés selon les règles en vigueur sur les ressources informatiques de leur périmètre.

Des mesures de sécurité spécifiques doivent être définies et respectées.

3.2.4 Gestion des informations secrètes d'authentification des utilisateurs

Un processus formel de gestion des attributions des informations secrètes d'authentification doit être défini et mis en œuvre.

3.2.4.1 Gestion sécurisée du mot de passe initial

Le processus d'attribution de l'authentifiant initial (« mot de passe par défaut ») doit être sécurisé :

- ❑ L'authentifiant doit être généré aléatoirement ;
- ❑ L'authentifiant doit être remis à l'utilisateur via un moyen garantissant sa confidentialité ;
- ❑ L'authentifiant ne doit jamais être communiqué dans le même échange et par le même canal que l'identifiant ;
- ❑ La modification de cet authentifiant doit être obligatoirement forcée à la première utilisation ;
- ❑ L'authentifiant doit avoir une durée de vie limitée.

3.2.4.2 Renouvellement des mots de passe

Les mots de passe doivent respecter les règles suivantes dans la mesure des limitations techniques des SI :

- ❑ Nombre minimum de caractère définis (au moins huit) ;
- ❑ Plusieurs types de caractères différents ;

- Renouvellement imposé plusieurs fois par an (au moins tous les quatre-vingt-dix jours).

Le changement du mot de passe doit être imposé par le système d'authentification. Pour les cas où cela ne serait pas possible, les utilisateurs s'engagent à procéder à leur révision.

Par ailleurs, en cas de suspicion de compromission, les utilisateurs doivent pouvoir procéder sans délai au changement de leur mot de passe. Les administrateurs peuvent forcer le changement des mots de passe si nécessaire.

3.2.4.3 Protection des sessions

Les sessions inactives doivent être suspendues (mise en veille) automatiquement. Une authentification est requise pour réactiver la session.

Le nombre de tentatives d'accès infructueuses doit être limité.

3.2.4.4 Stockage et sauvegarde sécurisés des couples identifiants / authentifiants

Les couples identifiants / authentifiants pour la connexion aux équipements et applications doivent être stockés et sauvegardés de manière sécurisée par les équipes opérationnelles.

3.2.4.5 Vérification de la validité des certificats électroniques

Pour assurer le contrôle d'accès aux ressources des SI, l'usage de clés cryptographiques peut être adopté, sur la base d'une Public Key Infrastructure (PKI) :

- Interne ou externe dans le cadre d'accès à des ressources internes au Groupe La Poste ;
- Externe dans le cadre d'accès à des ressources extérieures au Groupe La Poste.

Les mécanismes d'authentification forte par certificats doivent s'assurer de la validité des certificats électroniques :

- Date de validité ;
- Etat non révoqué ou non suspendu ;
- Chaîne de certification de confiance ;
- Types d'utilisation autorisés.

3.2.5 Revue des droits d'accès utilisateur

Les propriétaires d'actifs doivent revoir les droits d'accès accordés aux utilisateurs à intervalles réguliers.

3.2.5.1 Revue des comptes inactifs

Une revue régulière des identifiants réseaux et applicatifs inutilisés doit être effectuée afin de statuer sur leur état. Cette revue doit être programmée avec une fréquence d'au moins une fois par an.

3.2.5.2 Revue des droits d'accès

Les Responsables des Habilitations et les Propriétaires d'actifs procèdent de manière régulière à la vérification des droits d'accès attribués.

Le Propriétaire de l'actif s'assure notamment de l'adéquation de la nature des droits aux besoins des Métiers.

Il convient que cette fréquence soit d'au moins une fois par an pour tous les droits d'accès octroyés, et d'au moins une fois par semestre pour les accès privilégiés.

La revue doit être effectuée après tout changement d'affectation d'un salarié ou contractant tiers.

3.2.6 Suppression ou adaptation des droits d'accès

Les droits d'accès des accédants aux informations et aux moyens de traitement de l'information de l'entité doivent être supprimés à la fin de leur période d'emploi ou adaptés en cas de modification du contrat ou de l'accord.

3.2.6.1 Mise à jour des droits d'accès

En coordination avec l'ensemble des acteurs du processus d'habilitation, les Approbateurs veillent à la mise à jour des droits d'accès en tenant compte des modifications (d'affectation, de responsabilité, de mission, etc.) des accédants.

De manière similaire, les Responsables des Habilitations veillent à la mise à jour des droits d'accès, en tenant compte de la définition même des droits par rapport à leurs évolutions dans le temps (par exemple, modification des types de droits d'accès à une application).

En cas de changement d'affectation d'un salarié ou d'un contractant tiers, tous les comptes génériques auxquels ce dernier avait accès doivent être modifiés sans délais.

3.2.6.2 Suppression des droits d'accès

En cas de départ définitif d'un utilisateur du Groupe La Poste (retraite, licenciement ou démission pour un collaborateur, fin de prestation pour un prestataire, etc.), tous ses droits d'accès doivent être supprimés rapidement.

Les règles de gestion des droits d'accès doivent préciser la fonction ou l'identité de la personne en charge des demandes formelles de suppression et de leur suivi.

Des mécanismes de révocation doivent être mis en place.

Pour les authentifications réalisées au moyen d'objet physique de sécurité (« token », carte à puce, etc.), le Responsable de l'utilisateur doit s'assurer que ce dernier a bien restitué les objets physiques en sa possession.

De manière similaire, lorsqu'un traitement informatique ou équipement est retiré de la production, les règles de gestion des droits d'accès doivent identifier la personne en charge de la demande de suppression des droits d'accès.

3.2.6.3 Délégation de droit

La délégation peut porter sur tout ou partie des droits.

La délégation de droits doit obtenir l'accord formalisé du déléguant et du délégué pour une période donnée et avoir une date de début et une date de fin de validité.

Les délégations de droits doivent être journalisées et revues annuellement.

3.3 Responsabilités des utilisateurs

Objectif : rendre les utilisateurs responsables de la protection de leurs informations d'authentification.

3.3.1 Utilisation d'informations secrètes d'authentification

Les utilisateurs d'informations secrètes d'authentification doivent appliquer les règles existantes au sein de l'entité.

3.3.1.1 Information de l'utilisateur

Tout nouvel accédant doit être informé des responsabilités qui lui incombent au travers d'une charte utilisateur et / ou administrateur notamment en matière de protection des identifiants / authentifiants et de ses droits d'accès aux SI.

Il doit notamment veiller à la préservation de la confidentialité de ses authentifiants et des informations auxquelles il accède.

3.3.1.2 Protection des authentifiants utilisateurs

Il est recommandé aux utilisateurs :

- ❑ De ne pas divulguer ni partager son authentifiant ;
- ❑ De ne pas le conserver en clair ;
- ❑ De modifier son authentifiant en cas de risque de compromission ;
- ❑ De choisir un mot de passe facile à retenir mais difficile à deviner (ex : JMl@p1zza, « j'aime la pizza ») ;
- ❑ Utiliser un coffre-fort de mot de passe pour en assurer la confidentialité (ex : liste de mot de passe pour les connexions automatiques) ;
- ❑ De ne pas utiliser les mêmes authentifiants pour les activités professionnelles et les activités personnelles.

3.3.1.3 Contrôles d'accès renforcés

La force de l'authentification doit être adaptée à la sensibilité des informations accédées et des opérations, sensibilité définie par leur propriétaire (DICT).

Les applications et activités sensibles contiennent des informations dont la modification entraînerait le détournement ou la perte d'une quantité importante de biens financiers ou d'informations. Elles doivent donc faire l'objet de mesures spécifiques de protection pour empêcher leur utilisation.

La conception des authentifiants des administrateurs doit bénéficier de mesures renforcées.

3.4 Contrôle de l'accès aux systèmes et aux applications

Objectif : empêcher les accès non autorisés aux systèmes et aux applications.

3.4.1 Restriction d'accès à l'information

Les accès à l'information et aux fonctions d'application système doivent être restreints.

3.4.1.1 Procédure de restriction

Les restrictions d'accès sont décrites dans des procédures par l'entité en fonction des exigences de chaque application métier et conformes à la directive de contrôle d'accès définie.

L'application doit pouvoir gérer les contraintes suivantes :

- Gestion des mots de passe ;
- Implémentation d'une matrice de séparation des tâches ;
- Restrictions des actions (lecture, écriture, suppression et exécution) ;
- Limiter les informations contenues dans les éléments de sortie.

3.4.2 Sécuriser les procédures de connexion

Les accès aux systèmes et aux applications sont contrôlés par une procédure de connexion sécurisée d'accès au SI.

3.4.2.1 Règles d'authentification

Une technique d'authentification permet de vérifier l'identité de l'utilisateur.

Dans le cadre de la protection d'information sensible, il est préconisé d'utiliser des méthodes d'authentification forte, autres qu'un mot de passe : par exemple un procédé cryptographique, une carte à puce, des jetons d'authentification.

Les procédures de connexion doivent prendre en compte au minimum les règles suivantes :

- Affiche un avertissement précisant que l'accès de l'ordinateur est limité aux seuls utilisateurs autorisés ;
- Ne propose pas, pendant la procédure de connexion, de messages d'aide qui pourraient faciliter un accès non autorisé ;

- Valide l'information de connexion seulement lorsque toutes les données d'entrée ont été saisies. Si une condition d'erreur survient, il convient que le système n'indique pas laquelle est incorrecte ;
- Assure une protection contre les tentatives de connexion par force brute ;
- Enregistre les tentatives réussies et avortées ;
- Lance une alerte de sécurité en cas de détection d'une brèche possible, réussie ou avortée, dans les contrôles de connexion ;
- Affiche les informations suivantes après une connexion réussie :
  - la date et l'heure de la dernière connexion réussie,
  - les détails relatifs à toute tentative de connexion avortée depuis la dernière tentative réussie.
- N'affiche pas le mot de passe qui est entré ;
- Ne transmet pas les mots de passe au sein d'un réseau sous la forme d'un texte en clair ;
- Met fin aux sessions inactives au bout d'une période définie d'inactivité ;
- Restreint les temps de connexion pour apporter une sécurité supplémentaire aux applications sensibles et réduire les risques de tentatives d'accès non autorisé.

3.4.2.2 Modification des authentifiants par défaut

Les authentifiants par défaut des équipements, systèmes ou applications informatiques doivent être modifiés par les équipes opérationnelles avant la mise en production.

Les équipes opérationnelles doivent obligatoirement éviter de choisir un même couple identifiant / authentifiant pour un ensemble d'équipements / applications similaires, afin de limiter les risques de compromission généralisée.

3.4.2.3 Activation de processus de connexion « sûrs »

Les options de sécurisation des processus de connexion (par exemple chiffrement de l'authentifiant) doivent être activées sur tous les équipements et applications le permettant.

Une double authentification ou une authentification mutuelle sont préconisées.

3.4.2.4 Stockage et sauvegarde sécurisés des couples identifiants / authentifiants

Les couples identifiants / authentifiants pour la connexion aux équipements et applications doivent être stockés et sauvegardés de manière sécurisée par les équipes opérationnelles.

La protection des authentifiants est assurée par des moyens organisationnels et techniques adaptés au niveau de risque (restriction d'accès au lieu de stockage des authentifiants, limitation du nombre de personnes autorisées à y accéder, processus d'auto-contrôle des personnes habilitées, chiffrement des authentifiants, doubles enveloppes stockées dans un coffre sécurisé, etc.).

3.4.3 Système de gestion des mots de passe

Les systèmes générant les mots de passe doivent être interactifs et fournir des mots de passe de qualité.

3.4.3.1 Règles de gestion

Le système de gestion des mots de passe répond aux exigences suivantes :

- ❑ Impose l'utilisation d'identifiants et de mots de passe utilisateurs individuels afin de garantir l'imputabilité ;
- ❑ Autorise l'utilisateur à choisir et à modifier ses mots de passe, et prévoie une procédure de confirmation afin de tenir compte des erreurs de saisie ;
- ❑ Impose le choix de mots de passe complexes ;
- ❑ Impose aux utilisateurs de changer leur mot de passe à la première connexion du compte au SI ;
- ❑ Impose des changements réguliers de mot de passe ;
- ❑ Tient à jour un enregistrement des anciens mots de passe et empêche leur réutilisation ;
- ❑ N'affiche pas les mots de passe à l'écran lors de leur saisie ;
- ❑ Stocke les fichiers de mots de passe à d'autres emplacements que les données d'application système ;
- ❑ Stocke et transmette les mots de passe sous une forme protégée.

3.4.3.2Révision des authentifiants mots de passe

Le changement de l'authentifiant doit être imposé par le système d'authentification.

Pour les cas où cela ne serait pas possible, les utilisateurs s'engagent à procéder à leur modification manuellement.

3.4.4 Utilisation de programmes utilitaires à privilèges

L'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un SI ou d'une application doit être limitée et contrôlée.

3.4.4.1 Mesures d'utilisation

La plupart des installations informatiques comportent un ou plusieurs programmes utilitaires susceptibles de contourner les mesures de sécurité d'un système ou d'une application.

Les mesures suivantes doivent être prises en compte en matière d'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application :

- Utiliser des procédures d'identification, d'authentification et d'autorisation spécifiques ;
- Séparer les programmes utilitaires des logiciels d'application ;
- Limiter le nombre d'utilisateurs à privilèges pour l'emploi des programmes utilitaires ;
- N'autoriser qu'une utilisation spécifique des programmes utilitaires ;
- Poser des limites à la disponibilité des programmes utilitaires, par exemple limiter la durée d'une autorisation de modification ;
- Journaliser toutes les utilisations de programmes utilitaires ;
- Définir et documenter les niveaux d'autorisation relatifs aux programmes utilitaires ;
- Désinstaller ou désactiver tous les programmes utilitaires inutiles ;
- Ne pas mettre de programmes utilitaires à la disposition des utilisateurs concernés par la ségrégation des tâches.

3.4.5 Contrôle d'accès au code source des programmes

Les accès au code sources des programmes doivent être limités aux seules personnes ayant le besoin d'en connaître.

3.4.5.1 Accès aux codes source

Le personnel chargé de l'assistance technique dispose d'un accès restreint et contrôlé aux bibliothèques de programmes sources.

Un contrôle strict de l'accès au code source des programmes et aux éléments associés doit être exercé (tels que les exigences de conception, les spécifications, les programmes de vérification et de validation).

Les bibliothèques de code source ne sont pas stockées sur les systèmes d'exploitation mais dans un environnement sécurisé.

3.4.5.2Intégrité des codes sources

Les codes source du programme et les bibliothèques de programmes sources doivent être gérés conformément aux procédures établies afin de :

- Empêcher l'introduction d'une fonctionnalité non autorisée ;
- Eviter toute modification involontaire ;
- Préserver la confidentialité en matière de propriété intellectuelle de valeur.

La mise à jour et la recopie des bibliothèques de programmes sources et des éléments associés, ainsi que la délivrance des programmes sources aux programmeurs doivent être soumises aux procédures strictes de contrôle des modifications. Toute modification est réalisée après attribution d'une autorisation appropriée et formalisée.

3.4.5.3Traçabilité des codes sources

Un journal d'audit de tous les accès aux bibliothèques de programmes sources est tenu à jour.

Une revue des accès est effectuée périodiquement.