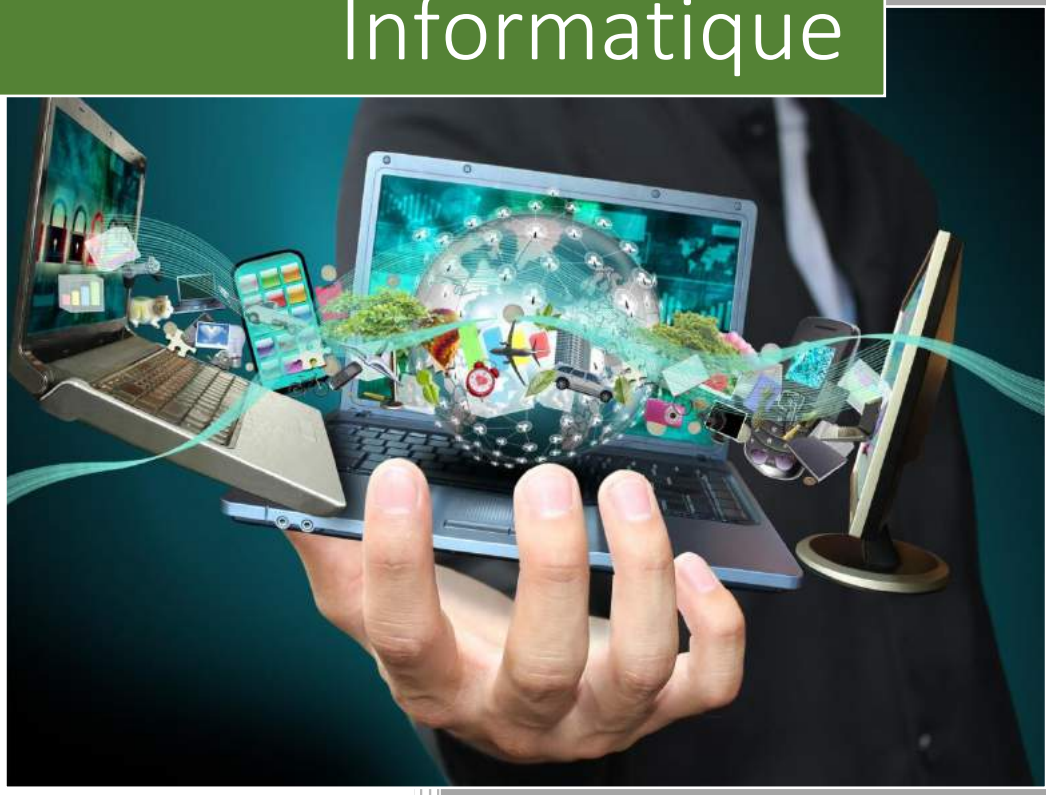
2016

Référentiel de Sécurité Informatique



Ministère de la Poste et des Technologies de l'Information et de la communication

Juin 2016

Table des matières

Préambule

Les systèmes d'information font désormais partie intégrante de nos vies quotidiennes, personnelles et professionnelles, et deviennent indispensables au fonctionnement des entreprises, des administrations et plus généralement de l'économie. Ces systèmes, cible au quotidien d'attaques et intrusions multiples, véhiculent des téraoctets de données numériques, notamment des informations personnelles, économiques, industrielles, administratives et sécuritaires, et sont de ce fait porteurs de risques nouveaux pesant lourdement sur les utilisateurs.

Afin de préserver les données numériques, il est nécessaire de prévoir les règles, les mécanismes et les bonnes pratiques à même de permettre et de garantir un seuil minimal de sécurité.

C'est dans ce contexte, qu'a été élaboré le présent référentiel de sécurité qui vise d'une part à favoriser une meilleure protection des systèmes d'information au sein des organismes utilisateurs, et d'autre part à sensibiliser les usagers de la toile aux risques encourus et leur expliquer les bonnes pratiques en matière de prévention et de sécurité informatique.

Chapitre 1 : Gestion des actifs

1.1. Responsabilités relatives aux actifs

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

- **Inventaire des actifs :**
  - Les actifs ayant accès à des informations ou manipulant des moyens de traitement des informations au sein de l'organisme doivent être identifiés et inventoriés ;
  - L'inventaire doit être précis, documenté, cohérent et à jour.
- **Propriétaire de l'actif :**
  - Les actifs identifiés et inventoriés au sein de l'organisme doivent être affectés à des entités ;
  - Les individus ou toutes autres entités ayant des capacités de gestion des actifs peuvent être désignés comme responsables d'actifs. Cette affectation doit être désignée lors de la création de l'actif ou de son transfert vers l'organisme ;
  - Le responsable d'actifs doit remplir les fonctions suivantes :
    - S'assurer et confirmer que l'actif est inventorié ;
    - S'assurer que les actifs sont proprement classifiés et protégés ;
    - Vérifier et revoir périodiquement les restrictions d'accès et la classification des actifs, en se basant sur les politiques de classification et de contrôle d'accès validées.
- **Utilisation adéquate des actifs :**
  - Des règles d'utilisation adéquate des informations, des actifs qui y sont associés et des moyens de traitement des informations doivent être élaborées, validées, documentées et mises en œuvre ;
  - Les employés et les partenaires (fournisseurs, clients, …) manipulant ou ayant accès aux actifs de l'organisme, doivent être informés et sensibilisés des exigences de sécurité des informations, des actifs et des moyens de traitement des informations de l'organisme. Ils doivent être responsables de l'utilisation de ces actifs.
- **Restitution des actifs :**
  - l'employé ou le partenaire doit restituer les actifs qui lui ont été affectés à la fin de la mission ayant justifiée leur attribution ;
  - Une procédure de restitution des actifs doit être formalisée ;
  - Dans le cas où un partenaire utilise son propre équipement pour le traitement des informations de l'organisme, des procédures doivent être mises en place afin de s'assurer que toutes les informations soient transférées, en toute sécurité, à l'organisme.

En outre, en cas de réforme de tout équipement disposant d'un support de stockage, des procédures de destruction définitive des données doivent être élaborées.

Lorsque les impératifs de sécurité l'imposent, les supports de stockage doivent être détruits.

1.2. Classification de l'information

Objectif : Déterminer le niveau de protection qui devrait être appliqué aux informations.

- **Classification de l'information :**
  - Les informations de l'organisme doivent être classifiées. Cette classification doit prendre en considération les exigences juridiques, la valeur, la criticité et la sensibilité à la divulgation ou à la modification non autorisée de cette information. Chaque niveau de classification doit être associé à des procédures de gestion et de traitement des actifs qui lui sont propres ;
  - Les actifs autres que des informations peuvent également être classifiés, et ce, en conformité avec la classification des informations qui sont stockées, traitées ou manipulées par ces actifs ;
  - La classification doit être inclue dans les processus de gestion de l'organisme. Elle doit être unique dans l'organisme ;
  - Les résultats de classification devraient indiquer la valeur des actifs en fonction de leur sensibilité et leur criticité au sein de l'organisme, notamment en termes de confidentialité, d'intégrité et de disponibilité. De même, ils devraient être mis à jour en fonction des changements de leur valeur, de la sensibilité et de la criticité liés à leur cycle de vie.

    A titre d'exemple, un plan de classification des actifs peut s'appuyer sur quatre niveaux :

    - Niveau 1 : la divulgation ne cause aucun préjudice ;
    - Niveau 2 : la divulgation cause une gêne mineure ou un léger désagrément de fonctionnement ;
    - Niveau 3 : la divulgation a, sur le court terme, des répercussions importantes sur les opérations ou les objectifs tactiques ;
    - Niveau 4 : la divulgation a, sur le long terme, des répercussions graves sur les objectifs stratégiques ou compromet la pérennité de l'organisation.
  - Les employés doivent être informés du plan de classification des actifs et des procédures y afférentes.
- **Etiquetage des informations :**
  - Un ensemble approprié de procédures pour l'étiquetage de l'information devrait être élaboré et mis en œuvre conformément au système de classification de l'information adopté par l'organisme ;
  - Les procédures d'étiquetage de l'information doivent couvrir l'information et les actifs annexes ;

- L'étiquetage devrait refléter le système de classification établi précédemment, et les étiquettes doivent être facilement reconnaissables ;
- Les procédures devraient donner des indications notamment sur l'endroit et la manière de fixation des étiquettes ;
- Les procédures peuvent définir les niveaux pour lesquels l'étiquetage n'est pas obligatoire ;
- Les employés doivent être informés des procédures d'étiquetage.

- **Manipulation des actifs :** Des procédures destinées pour les actifs de manutention devraient être élaborées, mises en œuvre et communiquées, et ce, conformément au système de classification de l'information adoptée par l'organisme.

  A cet effet, des procédures devraient être établies pour la manipulation, le traitement, le stockage et la communication des informations conformément à leur classification, en prenant en considération les éléments suivants :

  - La tenue à jour d'un enregistrement des destinataires autorisés des actifs ;
  - La protection des actifs informatiques contenant l'information ;
  - La protection des copies temporaires ou permanentes d'information à un niveau compatible avec le niveau de protection de l'information originale.

Chapitre 2 : Sécurité de l'utilisateur final

2.1 . Gestion et contrôle des accès aux systèmes et aux informations

Objectif : Veiller à ce que seules les personnes autorisées ont accès au système, et que la responsabilité individuelle est assurée.

2.1.1. **Politique de contrôle d'accès**

Pour limiter l'accès à l'information et aux moyens de traitement de l'information en fonction des habilitations, Il est nécessaire :

1. D'établir, de documenter et de tenir à jour une politique de contrôle d'accès sur la base des exigences métier et de sécurité de l'information ;
2. l'organisme détermine les règles de contrôle d'accès, des droits d'accès et des restrictions d'accès appropriés aux fonctions spécifiques de l'utilisateur de ces actifs conformément à la politique de sécurité approuvée ;
3. Les contrôles d'accès sont à la fois logiques et physiques et il convient de les envisager conjointement ;
4. La politique de contrôle d'accès doit tenir compte des impératifs suivants :
   a) Les exigences en matière de sécurité des applications métier ;
   b) La cohérence entre la politique des droits d'accès et la politique de classification de l'information ;
   c) Le respect de la législation et les obligations contractuelles applicables, relatives à la limitation de l'accès aux données ou aux services ;
   d) La séparation des rôles pour le contrôle d'accès : la demande d'accès, l'autorisation d'accès et l'administration des accès doivent être effectuées par des rôles distincts ;
   e) L'attribution formelle des autorisations d'accès ;
   f) La revue régulière des droits d'accès ;
   g) Les modalités d'archivage des journaux d'accès ;
   h) L'établissement des règles fondées sur le principe que tout est interdit sauf autorisation expresse, plutôt que sur celui que tout est autorisé sauf interdiction expresse ».

2.1.2. **Gestion des accès d'utilisateur**

Pour maîtriser l'accès utilisateur par le biais des autorisations et empêcher les accès non autorisés aux systèmes et aux services d'information, il est nécessaire de mettre en œuvre une procédure formelle de gestion des accès utilisateur pour attribuer ou révoquer des droits d'accès à tous les types d'utilisateurs de tous les systèmes et de tous les services d'information.

1) La procédure de gestion des identifiants utilisateurs doit inclure :
   a) L'obligation d'attribuer à chaque utilisateur un identifiant qui lui est propre ;
   b) Les identifiants doivent permettre de relier chaque action effectuée sur le système à un utilisateur unique ;
   c) L'utilisation des identifiants communs peut être autorisée à titre exceptionnel lorsque les aspects opérationnels liés à l'activité de l'organisme l'exigent ;
   d) L'obligation de suppression ou de blocage immédiat des identifiants des utilisateurs qui ont quitté l'organisme d'une façon temporaire ou définitive.

2) La procédure de gestion des accès utilisateur doit inclure :

a) Un processus formel de la gestion des accès utilisateur permettant la maitrise des opérations d'attribution ou de révocation des droits d'accès aux systèmes et aux services d'information ;
b) La séparation des rôles en charge de l'approbation des droits d'accès et de leur gestion ;
c) La vérification que les droits d'accès accordés sont adaptés à la politique d'accès et qu'ils sont cohérents avec les autres exigences telles que la séparation des rôles ;
d) La tenue à jour d'un enregistrement centralisé de tous les droits d'accès accordés aux identifiants utilisateurs ;
e) L'adaptation des droits d'accès des utilisateurs qui ont changés de fonction ou de poste ;
f) La revue régulière des droits d'accès des systèmes ou des services d'information.

2.1.3. **Gestion des contrôles d'accès au réseau**

Pour que les utilisateurs ne puissent avoir accès qu'aux ressources réseau pour lesquels ils ont reçu une autorisation formelle, il est nécessaire de définir une politique relative à l'utilisation des réseaux et des services y afférents, cette politique de gestion des contrôles d'accès au réseau doit définir :

1) Un descriptif des ressources réseaux existantes ;
2) Les moyens utilisés pour accéder aux réseaux ;
3) Les exigences d'authentification de l'utilisateur pour l'accès aux différentes ressources réseaux ;
4) Les procédures d'autorisation désignant les personnes autorisées à accéder aux ressources réseaux ;
5) Les procédures et mesures de gestion destinées à protéger l'accès aux ressources réseaux.

2.1.4. **Contrôle de l'accès au système et aux applications**

Pour empêcher les accès non autorisés au système et aux applications, il est nécessaire de restreindre l'accès aux informations et aux fonctions d'applications système conformément à la politique de contrôle d'accès, et cela par la mise en œuvre d'un dispositif permettant le contrôle des droits d'accès aux fonctions des différents systèmes et applications déployés.

2.2. Responsabilité liée à la sécurité des informations personnelles

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

2.2.1. **Utilisation d'informations secrètes d'authentification**

Pour préserver la confidentialité de l'authentification secrète :

1) Il est interdit de conserver les informations secrètes d'authentification (mot de passe, code PIN,… sur support papier, fichier électronique…) ;
2) Il est impératif de changer les informations secrètes d'authentification périodiquement et à chaque fois qu'il y a suspicion de compromission ;
3) L'organisme doit établir une politique de définition des mots de passe respectant notamment les mesures suivantes :
    a) la taille du mot de passe doit être supérieure à huit (08) caractères ;

b) le mot de passe doit être composé de caractères alphanumériques (minuscules et majuscules) et de caractères spéciaux ;
c) le mot de passe ne doit pas être facile à deviner (noms, prénoms, numéros de téléphone, dates d'anniversaire,….) ;
d) ne pas utiliser des mots usuels (azerty, qwerty…) ;
e) doivent être changés à la première connexion s'ils sont fournis par autrui.

4) Ne pas partager les informations secrètes d'authentification ;
5) Ne pas utiliser les mêmes informations secrètes d'authentification sur plusieurs comptes.

2.2.2. **Système de gestion des mots de passe**

L'organisme peut disposer d'un ou de plusieurs systèmes de gestion des mots de passe qui doivent garantir que ceux utilisés pour les accès aux applications, aux systèmes d'exploitation et aux ressources réseau sont robustes, en veillant à :

1) Imposer l'utilisation de mots de passe respectant la politique adoptée ;
2) Autoriser l'utilisateur à choisir et à modifier ses mots de passe, et prévoir une procédure de confirmation afin de tenir compte des erreurs de saisie ;
3) Imposer aux utilisateurs de changer leur mot de passe à la première connexion ;
4) Imposer un changement régulier de mot de passe et l'autoriser au besoin ;
5) Tenir à jour un enregistrement des derniers mots de passe afin d'empêcher leur réutilisation. Le nombre des derniers mots de passe enregistrés étant fixé par la politique de mot de passe ;
6) Ne pas afficher les mots de passe à l'écran lors de leur saisie ;
7) Stocker et transmettre les mots de passe sous une forme protégée.

2.2.3. **Préservation de l'intégrité des systèmes informatiques**

Afin de préserver l'intégrité des systèmes informatiques, il est nécessaire de :

1) Interdire la perturbation volontaire du fonctionnement des systèmes informatiques et des réseaux (internes ou externes) que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels malveillants ;
2) Interdire l'exécution des travaux de recherche ou d'expérimentation sur les environnements de production. Ils peuvent être exécutés sur des environnements de simulation après autorisation de la hiérarchie.

2.3. Formation et sensibilisation

Objectif : sensibiliser les utilisateurs aux risques liés à l'usage des TIC et améliorer leurs compétences.

2.3.1. **Programme de sensibilisation des utilisateurs et des partenaires**

1) Informer les utilisateurs du système d'information de l'organisme des politiques de sécurité ;
2) Sensibiliser les employés sur la sécurité informatique, notamment le risque lié au téléchargement et l'installation de logiciels non autorisés et les menaces liées au social-engineering ;
3) Sensibiliser les utilisateurs sur le risque relatif à la sortie et à la transmission des données professionnelles hors des postes de travail ;
4) Etablir et diffuser des chartes d'utilisation des ressources informatiques ;
5) Sensibiliser les utilisateurs sur les sanctions prévues en cas de tentative d'accès non autorisé ;
6) Sensibiliser les utilisateurs sur les actions qui peuvent mettre en péril la sécurité ou le bon fonctionnement des ressources qu'ils utilisent.

2.3.2. **Formation sur la cyber-sécurité**

1) Former les utilisateurs sur les risques provenant de l'Internet et sur la législation y afférente ;
2) Former le personnel en charge des systèmes d'information sur la gestion des incidents liés à la sécurité de l'information ;
3) Informer les utilisateurs des procédures à suivre en cas d'incident de sécurité ;
4) Former les utilisateurs sur la classification interne des informations et les procédures de traitement y afférentes.

2.4. Mesures de sécurité informatique à respecter en cas de déplacement à l'étranger

Objectif : prémunir les missionnaires contre les risques de sécurité encourus lors des déplacements à l'étranger.

1) Il est interdit d'utiliser des terminaux (ordinateurs, tablettes..) publics ou partagés pour accéder au compte de messagerie professionnelle ou aux applications métiers ;
2) Le missionnaire doit garder sur lui, en permanence, son terminal professionnel ainsi que les supports de stockage ;
3) Le missionnaire doit désactiver les fonctions de communication sans fil tel que le Wi-Fi et le Bluetooth des appareils lorsque celle-ci ne sont pas nécessaires ;
4) Supprimer toutes les données professionnelles sensibles, non nécessaire à la mission, de tous les supports amovibles avant tout déplacement à l'étranger ;
5) Informer l'hiérarchie et la représentation diplomatique algérienne en cas d'inspection ou de saisie des équipements informatiques par des autorités étrangères lors des missions à l'étranger ;
6) Interdire l'utilisation des équipements offerts lors d'un déplacement à l'étranger à des fins professionnelles ;

7) Exiger des missionnaires de mentionner dans leurs comptes rendus la liste des objets connectés offerts lors de leur déplacement ;
8) Interdire formellement le transfert par un étranger de documents via des supports de stockage amovibles. Tout échange de document doit se faire exclusivement par courriel ;
9) Le missionnaire doit changer les mots de passe utilisés pendant la mission.

Chapitre 3 : Sécurisation des réseaux

3.1. Les réseaux

Objectif : mettre en œuvre une architecture sécurisée afin de protéger le réseau des accès non autorisés.

3.1.1. **Conception et Gestion des réseaux**

L'organisme doit mettre en place des mécanismes de gestion de l'infrastructure réseau, lesquels doivent comprendre, notamment :

1) Les définitions des tâches / rôles / responsabilités des acteurs impliqués dans la gestion et la configuration des ressources réseau de l'organisme ;
2) La documentation du réseau qui inclure au minimum :
    a) Un diagramme déterminant la topologie du réseau, les équipements réseau, et toutes les connexions autorisées ;
    b) Un diagramme logique qui détaille les services et les serveurs critiques ;
    c) La configuration de tous les équipements réseau.

   La documentation, citée supra, doit être datée et mise à jour à chaque nouvelle configuration. L'accès à la documentation doit être restreint aux personnes habilitées ;
3) Des locaux sécurisés pour l'installation des équipements réseau actifs (routeurs, pare-feu, Switch, etc.), de manière à interdire tout accès physique non autorisé à l'équipement et d'en garantir l'intégrité ;
4) Les mécanismes d'authentification, d'autorisation et de traçabilité lors de l'administration des périphériques réseau ;
5) La journalisation (Logs) et la surveillance du trafic réseaux ;
6) Des accès exclusifs pour les systèmes, les processus, et les utilisateurs aux ressources réseau nécessaires à l'exécution de leurs tâches.

3.1.2. **Configuration des équipements réseaux**

1) Tous les mécanismes de protection du périmètre réseau notamment les routeurs et les pare-feu, et tous les équipements de connectivité tel que les commutateurs, points d'accès sans fil, etc. doivent être reconfigurés et personnalisés lors de leur installation ;
2) Les comptes par défaut doivent êtres désactivés ou renommés, et leurs mots de passe changés avant toute mise en service ;
3) Les procédures de gestion des configurations et des correctifs doivent être appliquées à tous les équipements réseaux ;
4) Toute modification de la topologie du réseau notamment à travers l'installation de points d'accès sans fil ou de clé de connexion sur le réseau mobile doit faire l'objet d'une autorisation formelle ;
5) Pour maintenir la précision temporelle des données et des journaux d'audit sur les systèmes d'information et équipements réseaux, les horloges de tous les systèmes et l'ensemble des terminaux doivent être synchronisées ;
6) Tous les équipements critiques du réseau doivent être reliés à une source d'alimentation sans coupure (Onduleur), qui doit être régulièrement testée et entretenue ;

7) Tous les ports physiques des équipements réseaux qui ne sont pas utilisés, doivent être désactivés ;

3.1.3. **Segmentation du réseau**

1) Le réseau interne de l'organisme doit être séparé en zones pour protéger les serveurs des utilisateurs réseau ;
2) L'organisme doit évaluer les risques liés à la sécurité réseau afin de déterminer le nombre de zones à délimiter et les exigences de sécurité applicables ;
3) Chaque zone établie doit être documentée : ses composantes, les risques, les mesures de sécurité mises en œuvre, etc ;
4) A titre d'exemple, la classification des zones réseaux peut être établie comme suit :

Zone	**Contenu**
Zone sécurisée	- Services base de données, - Services applicatifs, - Serveurs et stations contenant des données confidentielles,
Zone démilitarisé (DMZ)	- Interface utilisateur / Web,
Zone spécifique	- Développement, - Equipement de protection physique (onduleurs, caméras, etc.)
Zone utilisateur	- Les postes utilisateurs

5) Dans le cas où l'organisme met en place un réseau sans fil destiné aux visiteurs ou aux utilisateurs externes, il doit l'isoler du réseau interne ;
6) Dans le cas où l'organisme utilise un réseau sans fil dans son réseau interne, il doit appliquer de manière très stricte les recommandations de sécurité citées à la section 6 ;
7) L'organisme doit mettre en place les exigences de sécurité applicables à chaque zone. A titre d'exemple, les exigences de sécurité peuvent être modélisées comme suit :

Zone		Zone sécurisée		Zone démilitarisé (DMZ)
Niveau des risques		Standard	élevé	/
Utilisateur	Accès	Option	Non	Oui
	authentification	Obligatoire	/	Option
	Cryptage de connexion	Obligatoire	/	Option
Administrateur	Accès	Oui	Oui	Oui
	authentification	Obligatoire	Obligatoire	Obligatoire
	Cryptage de connexion	Obligatoire	Obligatoire	Obligatoire
	Accès	Oui	Oui	Oui

Application à Application / Serveur à Serveur	authentification	Obligatoire	Obligatoire	Option
	Cryptage de connexion	Obligatoire	Obligatoire	Option
Pare-feu		Obligatoire	Obligatoire	Obligatoire
Système de Détection et de Prévention d'Intrusion		Option	Obligatoire	Option

8) Il est nécessaire de séparer les serveurs d'applications des serveurs de base de données via des mécanismes et des dispositifs éprouvés (pare-feu ou VLANs) ;
9) Les organismes ne disposant pas, actuellement, des moyens permettant la mise en œuvre de la segmentation du réseau et / ou autres exigences de sécurité doivent identifier les zones réseaux et documenter les raisons ayant empêché leur mise en œuvre. Ces zones doivent être mise en œuvre dès la levée des raisons ayant empêché leur concrétisation ;
10) Les environnements virtuels doivent implémenter une communication sécurisée entre les machines virtuelles, et doivent utiliser une séparation de réseau équivalent à l'environnement physique.

3.1.4. **Authentification des équipements réseaux**

1) Les mesures d'authentification des équipements connectés aux réseaux doivent être testées périodiquement ;
2) Les équipements réseau de l'organisme ne doivent autoriser que la connexion des équipements préalablement identifiés à partir de chemins spécifiques

3.1.5. **Routage et configuration des pare-feux**

1) Le réseau doit être configuré pour surveiller et contrôler les communications aux limites externes du réseau, et à des points internes stratégiques ;
2) Dans ces limites, les contrôles de protection doivent au minimum inclure les éléments suivants :
    a) Vérification des adresses sources et destination ;
    b) L'authentification des administrateurs des équipements ;
    c) La mise en œuvre d'un mécanisme permettant de masquer les adresses du réseau interne de la vue externe ;
3) Installation et configuration du pare-feu, au minimum, comme suit :
    a) La configuration par défaut des pare-feux consiste à interdire tout trafic à l'exception des services autorisés et documentés par l'organisme ;
    b) L'organisme doit désigner un ou plusieurs administrateurs de pare-feu, et s'assurer qu'il a la formation nécessaire pour les tâches d'administration ;
    c) Toute demande d'ouverture exceptionnelle d'un port doit être dûment autorisée et limitée dans le temps. L'administrateur doit systématiquement refermer le port dès écoulement du délai ;
    d) Les administrateurs doivent configurer les pare-feux de sorte qu'ils ne peuvent pas être identifiables en tant que tel ;

e) Les pare-feux doivent être installés dans des lieux physiquement sécurisés contre toute altération. Ils ne doivent pas être déplacés sans l'approbation préalable de l'organisme ;
f) Les pare-feux doivent obligatoirement intégrer les règles suivantes :
   - Interdire le trafic réseau entrant émanant d'une source non-authentifiée ;
   - Interdire le trafic réseau entrant d'un réseau externe et utilisant une adresse source locale ;
   - Interdire tout trafic entrant émanant d'une source non autorisée contenant des paquets ICMP ;
   - Interdire le trafic réseau entrant contenant des informations de source de routage ;
   - Interdire tout trafic réseau (entrant ou sortant) contenant une adresse IP 0.0.0.0 ;
   - Interdire le trafic réseau entrant ou sortant contenant les adresses de diffusion.
g) Les pare-feux doivent être configurés pour enregistrer tous les paquets rejetés. Les journaux doivent être régulièrement examinés ;
h) La configuration et l'intégrité des fichiers de configuration des pare-feux doivent être examinées et vérifiées périodiquement.

3.1.6. **Utilisation des Systèmes de Détection et de Prévention d'Intrusion IDS/IPS**

1) L'organisme doit élaborer, appliquer et maintenir une stratégie de détection d'intrusion et de prévention, qui comprend :
   a) L'identification des systèmes de détection et de prévention des intrusions installés sur le réseau.
   b) les procédures et les ressources utilisées pour la gestion des mécanismes et des bases de connaissance utilisées lors de la détection.
   c) les procédures et les ressources utilisées pour l'analyse des journaux d'événements et des alertes en temps réel.

3.2. Transmission des données

Objectif : protéger les données qui transitent dans le réseau afin de garantir leur intégrité et leur confidentialité

3.2.1. **Contrôle de la distribution et transmission des données**

1) Les organismes doivent gérer l'échange ou le transfert de données électroniques afin de s'assurer que les exigences de sécurité (confidentialités, intégrités,…) relatives au niveau de classification sont maintenues durant le processus de transfert.
2) Les organismes doivent mettre en œuvre des contrôles ou des procédures techniques permettant de garantir que les données et les informations ne peuvent être échangées qu'avec autorisation.
3) L'utilisation de protocoles sécurisés doit être privilégiée.

3.2.2. **Contrôle des Transactions en ligne**

1) Lorsque les organismes acceptent ou initient des transactions en ligne, ils doivent mettre en œuvre des contrôles, et vérifier que les contrôles existent pour :

a) Valider l'identité des parties impliquées dans la transaction.
b) Si nécessaire, obtenir l'approbation appropriée pour la transaction.
c) Protéger les données confidentielles utilisées lors de la transaction.
d) Assurer l'intégrité de la transaction.
e) Obtenir la preuve que la transaction s'est achevée correctement.
f) Empêcher la relecture non autorisée ou accidentelle d'une transaction, de sorte qu'elle ne puisse être reproduite.

2) Les méthodes pour mettre en œuvre les contrôles ci-dessus dépendent de la nature de la transaction et du niveau du risque identifié. Elles peuvent inclure sans s'y limiter :
   a) L'utilisation des signatures électroniques issues d'un tiers de confiance où d'un prestataire de services de signature électronique conformément à la législation et la réglementation en vigueur.
   b) L'utilisation des techniques d'authentification fortes, telles que l'authentification multi-facteurs.
   c) Chiffrement des données échangées par le biais de protocoles sécurisés ;
   d) Journalisation des transactions dans un lieu sécurisé.

3.3. Courriel et Communication sur Internet

Objectif : contrôler l'utilisation d'internet dans l'organisme, et protéger les systèmes d'information contre les attaques.

3.3.1. **Envoi et réception de courrier électronique (e-mail)**

1) Chaque organisme doit mettre en place une messagerie électronique, hébergée sur le territoire national, destinée aux usages professionnels ;
2) L'organisme doit élaborer sa politique d'utilisation de la messagerie électronique professionnelle. Elle doit traiter notamment des :
   a) Règles liées au transfert automatique des emails ;
   b) Cas d'usage autorisés ou interdits de cette messagerie (envoi de canular,….) ;
   c) Moyens de protection des données confidentielles transmises ;
3) La messagerie professionnelle ne peut être utilisée qu'à des fins professionnelles. A cet effet, il est strictement interdit :
   a) L'envoi de message de nature privée ou personnelle ;
   b) L'utilisation de l'adresse électronique pour l'enregistrement sur les réseaux sociaux, les forums et les sites web ;
4) Il est strictement interdit d'utiliser les adresses mail personnelles pour la transmission des documents professionnels
5) Le personnel de l'organisme doit faire preuve de vigilance lors de l'utilisation des courriers électroniques et ceci en s'assurant que :
   a. l'adresse du destinataire est bien formulée ;
   b. le destinataire est habilité à accéder au contenu transmis ;
   c. les bonnes pièces jointes ont été rattachée au document.
6) Il est interdit d'ouvrir les pièces jointes et/ou les liens hypertexte transmis à partir d'adresses mail inconnues ;
7) Il est strictement interdit d'ouvrir sa boite mail professionnelle à partir des espaces communautaires d'accès à internet notamment les cybers café ;

8) L'organisme doit sensibiliser les utilisateurs sur les risques liés à l'usage de la messagerie électronique ;

3.3.2. **Utilisation de l'Internet à des fins de travail**

1) Le personnel ayant accès à l'Internet doit s'engager à :
   a) Ne pas utiliser intentionnellement ce service à des fins malveillantes, obscènes, frauduleuses, haineuses, diffamatoires, pornographiques ou illégales ;
   b) Respecter tous les droits d'auteur de logiciels et de licences ;
   c) Ne pas surcharger le réseau de l'organisme ;
   d) Ne pas accéder ou tenter d'accéder à un compte, ordinateur ou réseau pour lequel il ne dispose pas d'autorisation d'accès.
   e) Faire preuve de prudence lors du téléchargement des fichiers, et s'assurer de les scanner par un antivirus.

3.3.3. **Utilisation des médias sociaux**

1) Lorsque les médias sociaux sont adoptés pour une utilisation professionnelle, l'organisme doit veiller à :
   a) Élaborer des guides de travail destinés aux personnes autorisées à administrer et à modérer les sites de médias sociaux exploités par l'organisme dans un cadre professionnel.
   b) Aider à prévenir le piratage et l'accès non autorisé aux comptes médias sociaux de l'organisme. Aussi, le personnel en charge de ces comptes doit :
      - Utiliser des comptes et mots de passes différents pour chaque réseau social, ces mot de passe doivent respecter la politique de mot de passe arrêtée par l'organisme ;
      - Utiliser la double authentification, quand le service est fourni.
2) Pour l'utilisation à titre privé des média sociaux, l'organisme doit :
   a) Interdire l'utilisation de l'adresse électronique professionnelle pour l'ouverture de comptes médias sociaux ;
   b) Interdire aux employés de fournir des informations liées à leur fonction, grade ou responsabilité sur les réseaux sociaux ;
   c) Interdire la divulgation de toute information liée à la vie professionnelle sur les réseaux sociaux ;
   d) Sensibiliser les employés aux risques liés à la divulgation des données à caractère privé ou personnel sur les réseaux sociaux ;

3.3.4. **Filtrage des contenus inappropriés sur Internet**

1) L'organisme doit mettre en place un dispositif permettant de filtrer le contenu et l'accès à Internet ;
2) L'organisme doit indiquer clairement à son personnel la présence de ce dispositif.
3) Ce dispositif doit maintenir l'historique des sites web visités et les fichiers téléchargés ;
4) Les informations sauvegardées sur l'utilisation de l'Internet et la durée de leurs conservations doivent être documentées ;

3.4. Sécurisation des communications

Objectif : sécuriser les communications à caractère confidentiel

1) La transmission des informations confidentielles par ligne téléphonique non sécurisées doit être strictement interdite ;
2) Lors des échanges de données confidentielles par voie IP, les mesures de sécurité appropriées doivent être mises en place ;
3) L'échange de données confidentielles sur les plateformes de voix IP, hébergées en dehors du territoire national, est interdit ;
4) Toutes les données confidentielles doivent être chiffrées lors de la transmission à travers les réseaux sans fil ou publics ;

3.5. Réseaux sans fil

Objectif : Sécuriser le réseau sans fil afin de protéger les systèmes d'information contre l'écoute et les accès non autorisés.

Les points d'accès du réseau sans fil de l'organisme, destiné à un usage interne, doivent répondre aux exigences minimales suivantes :

1) L'accès physique
   a) Tous les points d'accès au réseau et les équipements connexes, supportant des réseaux sans fil doivent être sécurisés avec des mécanismes de verrouillage, ou placement dans une zone où l'accès est limité au personnel autorisé ;
   b) Les points d'accès doivent être disposés de manière à minimiser la propagation du signal en dehors du périmètre de l'organisme.
2) Accès réseau
   a) Lorsque les points d'accès sont connectés au réseau local (LAN), ils doivent l'être via un dispositif « passerelle ».
   b) La valeur par défaut du Service Set Identifier (SSID) doit être personnalisée.
   c) Le nom SSID ne doit pas contenir des indicateurs sur l'organisme, sur le lieu d'installation ou les fonctions du point d'accès.
3) Système d'accès
   a) Tous les points d'accès doivent exiger un mot de passe pour accéder à ses fonctions administratives. Ce mot de passe doit être stocké et transmis dans un format crypté.
   b) Il est strictement interdit de communiquer ce mot de passe aux personnes non autorisées ;
4) Authentification
   a) Tous les accès au réseau par l'intermédiaire d'un réseau sans fil doivent être authentifiés.

Chapitre 4 : Sécurité des systèmes

4.1. L'acquisition et l'installation des logiciels

Objectif : Limiter les risques liés à la sécurité des systèmes d'information lors de l'acquisition des solutions et leur implémentation.

4.1.1. **Acquisition :**

1) Il doit être strictement interdit d'acquérir et/ou utiliser des logiciels piratés. Tout logiciel ou système acquis doit disposer d'une License officielle.
2) Le téléchargement des logiciels via internet ne doit intervenir qu'à travers le site officiel de l'éditeur ;
3) Il doit être interdit d'acquérir des logiciels et/ou des applications dont l'éditeur a annoncé la fin de support ;
4) Il est recommandé d'acquérir les versions les plus récentes des systèmes et des logiciels ;

4.1.2. **Installation :**

1) Il doit être interdit d'installer ou d'exécuter tout logiciel et/ou application n'ayant pas une licence valide ;
2) L'utilisateur final n'est pas autorisé à installer des logiciels et/ou application sur son poste de travail sans l'accord préalable des structures concernées ;
3) Ne doivent être installés sur les postes de travail et les serveurs que les logiciels et les systèmes nécessaires à l'accomplissement des missions de l'organisme ;
4) Tous les mots de passe par défaut doivent être personnalisés conformément à la politique arrêtée à cet effet.

4.2. Inspection et contrôle du code source des logiciels

Objectif : protéger les systèmes contre toute tentative de détournement ou d'utilisation illicite.

1) Lorsqu'ils sont disponibles, les codes sources des applications critiques acquises ou développées doivent être inspectés.
2) Seul le personnel autorisé peut avoir accès aux codes sources ;
3) Les codes sources doivent être stockés dans un environnement garantissant leur intégrité et leur confidentialité.

4.3. Maintenance et mise à jour des logiciels

Objectif : Protéger les systèmes d'information des nouvelles vulnérabilités découvertes

4.3.1. **Mise à jour des logiciels :**

1) Les systèmes et les logiciels doivent être mis à jour ;
2) Les mises à jour de sécurité doivent être appliquées dès leur publication ;
3) Les mises à jour système et logiciels doivent être testées dans un environnement de test préalablement à un déploiement de masse.
4) Un point de restauration doit être mis en place, préalablement à l'installation des mises à jour critiques ;

5) Seul le personnel technique qualifié doit être autorisé à déployer les mises à jour ;
6) Toutes les opérations de mises à jour doivent être journalisées ;

4.3.2. **Maintenance des logiciels**

1) Les erreurs et les bugs doivent être signalés au service concerné dès leur occurrence ;
2) Les recommandations publiées par des organismes officiels habilités concernant les vulnérabilités n'ayant pas de patch doivent être appliquées après avoir été testées dans un environnement restreint ;

4.4. Opérations effectuées sur les systèmes et logiciels

Objectif : Contrôler les systèmes d'information et les protéger contre les utilisations non autorisées

4.4.1. **Opérations d'administration**

1) Les systèmes et les applications doivent être audités périodiquement ;
2) Le système d'information doit faire l'objet d'une cartographie basée sur les actifs identifiés dans le chapitre 1 ;
3) Les administrateurs doivent utiliser des outils d'administration centralisés lorsque le nombre d'actifs informationnels est important ;
4) Les procédures d'administration doivent être documentées ;
5) La configuration des ressources informatiques doit être documentée et mise à jour à chaque changement.
6) L'organisme doit mettre en œuvre un système de surveillance et d'audit du système pour détecter toute activité non autorisée où à défaut activer cette fonctionnalité au niveau des systèmes d'exploitations déployés ;
7) L'organisme doit mettre en œuvre des contrôles destinés à empêcher ou à détecter l'utilisation de logiciels non autorisés (par exemple, listes blanches d'applications) ;
8) Veiller à la mise en place d'un antivirus et à sa tenue à jour
9) Les événements de sécurité de l'antivirus des systèmes connectés doivent être remontés sur un serveur pour analyse statistique et gestion des problèmes.
10) Les systèmes déployés doivent être synchronisés via une référence de temps commune (service NTP, Network Time Protocol).
11) L'administrateur système doit désactiver ou désinstaller les services non utilisés ;
12) Les administrateurs doivent signer une charte d'éthique
13) Veillez à la gestion et à la sécurisation des données partagées par le système ou les applications ;
14) Désactivez l'exécution automatique des supports amovibles depuis les postes utilisateurs ;
15) Seuls les administrateurs habilités sont autorisés à avoir un accès distant aux serveurs de l'organisme ;
16) L'option accès bureau distant aux postes utilisateurs doit être désactivée ;
17) le BIOS des serveurs, des postes de travail (fixe ou mobile) doit être verrouillé avec un mot de passe et le démarrage à partir de supports amovibles, CD et/ou DVD doit être désactivé.

4.4.2. **Opérations effectuées par l'utilisateur :**

1) Verrouiller l'accès au poste de travail en cas d'absence, même temporaire ;
2) Alerter les services techniques en cas de découverte d'un nouvel équipement connecté au poste de travail ;
3) S'assurer que son poste de travail dispose d'un antivirus, et informer la structure concernée dans l'organisme de toute alerte de sécurité survenue ;
4) Il est interdit de connecter des équipements personnels au poste de travail ;
5) Scanner tous les supports amovibles connectés au poste de travail avant de les utiliser ;
6) Eteindre l'ordinateur pendant les périodes d'inactivité prolongée (nuit, weekend, vacances,) ;

4.4.3. **Journalisation**

1) L'organisme doit définir et mettre en œuvre une politique de gestion et d'analyse des journaux.
2) L'organisme doit journaliser et conserver une trace des événements de sécurité de tous les systèmes déployés.
3) Les journaux des événements de sécurité doivent être conservés conformément à la politique de gestion et d'analyse des journaux de l'organisme.
4) L'organisme est tenu de conserver de manière fiable les journaux d'évènement en les protégeant contre les risques d'altération ou d'accès non autorisé.
5) Les journaux d'évènement doivent être analysés régulièrement.

4.5. Tests

Objectif : Tester les nouveaux systèmes et logiciels afin de garantir l'intégrité et la confidentialité des données

1) Les environnements de développement et de test doivent être séparés des environnements de production.
2) L'utilisation de données réelles dans l'environnement de test doit respecter les règles de confidentialité définies par le propriétaire des données.
3) Les nouveaux systèmes développés doivent être testés pour démontrer qu'ils répondent aux exigences de sécurité ;

4.6. Développement et maintenance des sites web

Objectif : veiller à ce que les risques accrus associés aux applications web sont minimisés.

1) Le développement des sites web doit être fait par un personnel qualifié utilisant des méthodes de développement sécurisées et éprouvées ;
2) Les modules d'authentification utilisés dans les sites web ne doivent pas stocker les mots de passe en clair mais sous une forme transformée par une fonction cryptographique non réversible ;
3) L'administration d'un site web doit se faire via des protocoles sécurisés à partir de postes de travail réputés fiables ;
4) Les systèmes et applicatifs utilisés par le site web doivent être régulièrement tenus à jour ;
5) Sauf nécessité de service, bloquer les transferts de zone DNS ;

6) empêcher la fourniture de renseignements relatifs à la configuration technique du site web (Système d'exploitation utilisé, serveur d'application utilisé…).
7) Les sites web doivent être régulièrement audités ;

4.7. Utilisation des appareils mobiles et des supports de stockage

Objectif : se prémunir contre la perte ou le vol des données stockées sur des appareils mobiles et des supports de stockage.

1) L'organisme doit identifier les données pouvant être stockées sur les appareils mobiles et les supports de stockage, et définir les mesures de protection devant être mises en place.
2) Chiffrer les données confidentielles contenues dans des appareils mobiles et des supports de stockage ;
3) Lors des déplacements professionnels, l'utilisateur doit garder ses appareils mobiles et supports de stockage amovible sur soi ;

4.7.1. **Utilisation des appareils mobiles**

1) Toute perte ou vol d'un appareil mobile doit être signalée à l'hiérarchie dans l'immédiat ;
2) Consigner les numéros de série de tous les appareils mobiles utilisés par l'organisme.
3) Sauf exception dûment motivée et validée par l'hiérarchie, les utilisateurs n'ont pas de droits d'administration ;
4) Verrouiller toujours les appareils mobiles lorsqu'ils ne sont pas utilisés ;
5) L'utilisateur doit désactiver les fonctions Wi-Fi et Bluetooth des appareils lorsque celles-ci ne sont pas nécessaires ;

4.7.2. **Utilisation des supports de stockage**

1) L'organisme doit mettre en œuvre des procédures de gestion des supports de stockage conformément au plan de classification adopté.
2) Interdiction formelle pour toute personne étrangère à l'organisme de transférer des documents par support amovible, tout échange de document doit se faire par courriel. Dans le cas où le volume de données exige le recours à un support amovible, ce dernière doit être analysé par les services compétents avant toute utilisation ;

4.8. Gestion des données

Objectif : Assurer la confidentialité et l'intégrité des données.

1) La confidentialité et l'intégrité des données sensibles doit être garantie par les moyens techniques appropriés notamment le chiffrement.
2) L'intégrité des données stockées doit être garantie notamment par des contrôles applicatifs.
3) Le stockage des données professionnelles sur des plateformes hébergées en dehors du territoire national doit être strictement interdit.
4) Avant toute opération de maintenance externe, les supports de stockage des données doivent être retirés des équipements.

4.9. Sauvegarde, restauration et archivage

Objectif : Assurer une sauvegarde des données dans le but de les récupérés en cas de perte.

1) L'organisme doit mettre en œuvre des processus de sauvegarde et de recouvrement et effectuer périodiquement des sauvegardes de systèmes ;
2) La sauvegarde se fait sur un support externe dédié ;
3) L'organisme doit interdire la sauvegarde des données professionnelles sur des sites de stockage « Cloud» hébergeant les données en dehors du territoire national ;
4) L'organisme doit conserver des copies des sauvegardes dans un site distant ;
5) L'organisme doit inclure les configurations des systèmes et des logiciels dans les sauvegardes ;
6) Le réseau de stockage/sauvegarde des centres informatiques doit reposer sur une architecture dédiée à cet effet ;
7) Les sauvegardes doivent être réalisées selon les règles édictées par le plan de continuité de l'activité ;
8) L'exécution de la sauvegarde doit être compatible avec le niveau de disponibilité des applications ;
9) L'organisme doit prendre en compte la durée de vie des supports de sauvegarde ;
10) Chaque média de sauvegarde d'un composant du système d'information doit être identifié. Il doit être étiqueté avec au minimum le nom de la machine sauvegardée et un numéro de série unique ;
11) Les sauvegardes doivent être testées régulièrement afin de garantir la capacité de restituer l'environnement complet d'un composant du système d'information, particulièrement les applications estimées comme critiques ;
12) L'organisme doit chiffrer les informations confidentielles sauvegardées ;
13) Avant la mise en production d'un nouveau système, le processus de sauvegarde doit être testé sur le nouveau composant afin de garantir la reprise des données suite à un incident potentiel.
14) Toute procédure de sauvegarde doit être revue et le cas échéant mise à jour à chaque changement de contexte d'exploitation, à chaque création ou modification d'une fonctionnalité sur l'un des composants techniques ou applicatif du système d'information.

4.10. Les partenaires

Objectif : Veiller à ce que les partenaires ne représentent pas un vecteur de risque

1) Un contrat de confidentialité doit être signé avec les fournisseurs des équipements liés au centre de traitement de données.
2) L'organisme doit s'assurer que les partenaires respectent les politiques, les normes et les procédures ;
3) Les contrats doivent être mis à jour pour indiquer tout changement éventuel ;
4) L'accès au système d'information de l'organisme de la part de personnels d'entreprises extérieures doit être conforme à la politique générale d'accès aux moyens informatiques.

Chapitre 5 : Sécurité physique

5.1. Zones sécurisées

Objectif : empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisme.

5.1.1. **Périmètre de sécurité physique :**

1) Définir clairement les périmètres de sécurité et décider de l'emplacement et du niveau de résistance de chacun d'eux en fonction des risques identifiés et des exigences de sécurité des actifs situés à l'intérieur ;
2) Les bâtiments ou les sites abritant des moyens de traitement de l'information sensible doivent être construit en dur et toutes les portes extérieures et les fenêtres doivent être adéquatement protégées contre les accès non autorisés ;
3) Equiper d'une alarme, dotée d'une sécurité intégrée, l'ensemble des portes coupe-feu du périmètre de sécurité des zones sensibles. Surveiller ces portes et les soumettre à essai régulièrement ;
4) Séparer physiquement les moyens de traitement de l'information gérés par l'organisme de ceux gérés par des tiers.

5.1.2. **Contrôles physiques des accès :**

1) Exiger de l'ensemble des salariés, contractants et utilisateurs tiers et de tous les visiteurs, le port d'un moyen d'identification visible.
2) Contrôler l'accès en le limitant aux seules personnes habilitées,
3) Mettre en œuvre des contrôles additionnels d'authentification pour l'accès aux zones de traitement ou de stockage des informations sensibles ;
4) Journaliser les accès conformément à la politique de journalisation ;
5) L'accès du personnel externe doit être motivé et autorisé ;
6) Accompagner le personnel externe et l'instruire des exigences de sécurité à respecter.
7) Mettre à jour régulièrement les droits d'accès aux zones sécurisées.

5.1.3. **Sécurisation des bureaux, des salles et des équipements :**

1) Choisir un emplacement non accessible au public pour les équipements-clés ;
2) Ne pas divulguer les lieux abritant des activités de traitement de l'information sensible.

5.1.4. **Protection contre les menaces extérieures et environnementales :**

1) Prendre en considération toute les menaces contre la sécurité que pourraient présenter les locaux voisins, tel que l'incendie d'un bâtiment, une fuite d'eau au plafond, une inondation dans les étages, lors de l'élaboration de la politique de sécurité physique ;
2) Stocker les matières dangereuses ou combustibles à une distance suffisamment éloignée de la zone sécurisée ;
3) Placer le matériel de secours dans un site distant afin d'éviter tout dommage engendré par un sinistre touchant le site principal ;
4) Prévoir et placer à un endroit approprié le matériel de lutte contre l'incendie.

5.1.5. **Travail dans les zones sécurisées :**

1) Le personnel ne doit être informé de l'existence de zones sécurisées ou des activités qui s'y pratiquent qu'en cas de nécessité de service ;
2) Toute intervention dans une zone sécurisée doit être encadrée et documentée ;
3) Les zones sécurisées inoccupées doivent être verrouillées physiquement et contrôlées ;
4) Interdire tout équipement photographique, vidéo, audio ou autres dispositifs d'enregistrement, tels que les appareils photos intégrés à des appareils mobiles, sauf autorisation ;

5.1.6. **Zones de livraison et de chargement :**

1) Isoler les points d'accès, des moyens de traitement de l'information, de façon à éviter les accès non autorisés.
2) L'accès à la zone de livraison/chargement depuis l'extérieur du bâtiment doit être limité au personnel identifié et autorisé ;
3) Concevoir la zone de livraison/chargement de sorte que les marchandises reçues puissent être déchargées sans que le personnel de livraison n'ait accès aux autres parties du site ;
4) Contrôler les matières entrantes, pour vérifier l'absence de menaces potentielles avant le transfert de ces matières de la zone de livraison/chargement à leur point d'utilisation ;

5.2. Matériel

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

5.2.1. **Emplacement et protection du matériel :**

1) L'emplacement du matériel doit permettre de réduire le plus possible les accès inutiles aux zones de travail et de réduire le risque d'accès non autorisé à l'information ;
2) Sécuriser les moyens de stockage contre tout accès non autorisé ;
3) Isoler les éléments nécessitant une protection particulière ;
4) Adopter des mesures visant à réduire le plus possible les risques de menaces physiques potentielles, comme le vol, l'incendie, les explosifs, la fumée, les fuites d'eau (ou une rupture de l'alimentation en eau, surtout pour le refroidissement des équipements, le cas échéant), la poussière, les vibrations, les effets engendrés par les produits chimiques, les interférences sur le secteur électrique, les interférences sur les lignes de télécommunication, les rayonnements électromagnétiques et le vandalisme ;
5) Interdire au personnel de manger, de boire ou de fumer à proximité des moyens de traitement de l'information ;
6) Surveiller les conditions ambiantes, telles que la température et l'humidité, qui pourraient nuire au fonctionnement des moyens de traitement de l'information ;
7) Protéger l'ensemble des bâtiments et des installations contre les risques liés à la foudre et au tonnerre ;
8) Prévoir l'application des mesures spéciales de protection pour le matériel en environnement industriel et protéger les moyens de traitement de l'information sensibles des risques de fuites d'informations.

5.2.2. **Services généraux**

1) Les services généraux, tels que l'électricité, l'alimentation en eau et la climatisation doivent être correctement dimensionnés pour répondre aux besoins de l'organisme ;
2) Inspecter régulièrement et soumettre à essai les services généraux pour s'assurer de leur bon fonctionnement ;
3) Installer une alimentation électrique adaptée, conforme aux spécifications du fabricant du matériel et prévoir un éclairage de secours ;
4) Utiliser un/des onduleur(s) et un/des générateur(s) de secours pour le matériel prenant en charge des opérations critiques pour l'organisme avec une quantité de carburant suffisante ;
5) Placer les interrupteurs et les robinets de secours destinés à couper le courant, l'eau, le gaz ou autres services près des sorties de secours et/ou des salles contenant le matériel.
6) L'alimentation en eau doit être régulière et suffisante pour alimenter les systèmes de l'organisme ;
7) Maintenir en état de fonctionnement au moins deux voies de communication vers l'extérieur ;

5.2.3. **Sécurité du câblage :**

1) Enterrer, dans la mesure du possible, les lignes électriques et les lignes de télécommunication branchées aux moyens de traitement de l'information ou les soumettre à toute autre forme de protection adéquate ;
2) Séparer les câbles électriques des câbles de télécommunication pour éviter toute interférence ;
3) Prévoir les mesures supplémentaires suivantes pour les systèmes sensibles ou critiques :
    a) l'installation d'un conduit de câbles blindé et de chambres ou de boîtes verrouillées aux points d'inspection et aux extrémités ;
    b) le balayage technique et l'inspections physiques pour détecter le branchement d'appareils non autorisés ;

5.2.4. **Maintenance du matériel :**

1) Entretenir le matériel conformément aux spécifications et périodicité recommandées par le fournisseur ;
2) Assurer la maintenance du matériel par le personnel habilité ;
3) Conserver un dossier de toutes les pannes suspectées ou avérées et de toutes les tâches de maintenance préventives ou correctives ;
4) Mettre en œuvre des mesures appropriées lorsque la maintenance d'un matériel est Planifiée en prenant en compte la nature de l'information contenue dans le matériel, et le fait qu'elle soit effectuée par du personnel sur site ou extérieur à l'organisme ;
5) Inspecter le matériel à l'issue de sa maintenance avant de le remettre en service, pour s'assurer qu'il n'a pas subi d'altérations et qu'il fonctionne correctement.

5.2.5. **Sortie des actifs :**

1) Ne pas sortir un actif des locaux de l'organisme sans autorisation préalable ;

2) Identifier clairement les salariés, contractants et utilisateurs tiers qui ont autorité pour permettre le retrait des actifs du site.
3) Fixer des délais pour la sortie de matériels et veiller à leur respect ;
4) Enregistrer la sortie du matériel et son retour dans les locaux de l'organisme et documenter toute manipulation ou utilisation des actifs.
5) Effectuer des contrôles ponctuels, destinés à détecter une sortie d'actif non autorisée.

5.2.6. **Sécurité du matériel et des actifs hors site :**

1) L'utilisation de matériels de traitement de l'information hors site doit être dument autorisée par l'organisme ;
2) Observer les instructions du fabricant visant à protéger le matériel ;
3) Définir des mesures de sécurité liés aux emplacements de travail hors site ;
4) Tenir à jour un journal détaillant la chaîne de traçabilité du matériel, lorsque le matériel circule hors des locaux de l'organisme ;

5.2.7. **Mise au rebut ou recyclage sécurisés du matériel :**

Préalablement au recyclage ou à la mise au rebut des équipements de traitement de données, les supports de stockage contenant de l'information confidentielle ou protégée par les droits d'auteur, doivent être détruits, ou bien l'information contenue doit être détruite en utilisant les techniques rendant l'information d'origine irrécupérable.

5.2.8. **Politique du bureau propre et de l'écran vide :**

1) Il convient de mettre sous clé les informations sensibles ou critiques liées à l'activité de l'organisme ;
2) Protéger les points d'entrée/sortie des courriers postaux ainsi que les télécopieurs ;
3) Retirer immédiatement des imprimantes les documents contenant des informations sensibles ou classées et empêcher l'utilisation non autorisée des photocopieurs et autres appareils de reproduction.

Chapitre 6 : Gestion des Incidents liés à la Sécurité de l'Information :

6.1. Contrôle des Systèmes

Objectif : Identifier les menaces qui peuvent conduire à un incident de sécurité de l'information.

1) L'organisme doit mettre en place un système de journalisation permettant notamment, d'enregistrer les événements liés à la sécurité de l'information.
2) Les journaux d'évènements doivent être conservés durant une période préalablement définie afin de faciliter les opérations d'audit.
3) Sauf autorisation explicite de l'organisme, Il est interdit aux administrateurs du système d'effacer les journaux d'évènement ou de désactiver la journalisation des évènements.
4) L'organisme doit mettre en place des procédures d'audit périodique des systèmes de traitement de l'information.

6.2. Protection des Informations Journalisées

Objectif : Maintenir l'intégrité et la confidentialité des informations importantes liées à la sécurité.

1) L'organisme doit protéger la confidentialité et l'intégrité des journaux d'évènement et veiller à leur disponibilité.
2) L'organisme doit veiller à ce que le système de journalisation ne soit accessible que par les personnes autorisées et que toute modification de ses paramètres soit subordonnées à l'autorisation de qui de droit.
3) L'organisme doit conserver les rapports d'audit conformément à sa politique de sécurité.

6.3. Signalement et gestion des incidents de sécurité informatique

Objectif : Identifier les risques importants et les maintenir dans des limites acceptables.

1) L'organisme doit mettre en place des procédures formelles de signalement des évènements ayant un impact sur la sécurité. Cette procédure définit notamment l'interlocuteur, la méthode et les délais de signalement ;
2) L'organisme doit sensibiliser tous les utilisateurs aux procédures de signalement des différents types d'événements et de failles susceptibles d'avoir une incidence sur la sécurité ;
3) L'organisme doit établir des procédures de réponse en cas de détection d'un incident lié à la sécurité de l'information ;
4) L'organisme doit identifier les responsables et les procédures de gestion des incidents de sécurité ;
5) L'organisme doit veiller à la mise à jour et à l'amélioration des procédures arrêtées ;
6) L'organisme doit informer sa tutelle en cas d'incident de sécurité informatique ;
7) L'organisme doit mettre en place une cellule de veille en matière de sécurité informatique.

Chapitre 7 : Gestion des risques et reprise après incident

Objectif : neutraliser les interruptions des activités de l'organisme, protéger les processus métier cruciaux des effets causés par les principales défaillances des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.

1) L'organisme doit mettre en œuvre des plans de continuité de l'activité visant à garantir une reprise des opérations essentielles dans les meilleurs délais ;
2) L'organisme doit mettre en œuvre un processus de gestion du plan de continuité de l'activité avec des mesures préventives et correctives visant à réduire le plus possible l'impact sur l'organisme et à récupérer les actifs informationnels perdus (notamment à la suite de catastrophes naturelles, d'accidents, de pannes de matériel et d'actes délibérés) ;
3) La mise en place d'un plan de continuité de l'activité qui doit suivre les étapes suivantes :
    a) Identifier les actifs concernés par les processus métier cruciaux ;
    b) Identifier les risques auxquels pourra être exposé l'organisme et en définir la probabilité d'occurrence et l'impact ;
    c) Identifier le temps maximum toléré pour l'arrêt des services critiques de l'organisme ;
    d) Définir les solutions projetées pour le traitement de chaque incident identifié ;
    e) Identifier les ressources financières, d'organisation, techniques et environnementales suffisantes pour satisfaire aux exigences de la reprise d'activité ;
    f) Elaborer et documenter les plans de continuité de l'activité ;
    g) Soumettre à essai et mettre à jour de façon régulière les plans et processus mis en place ;
    h) Identifier, informer et former les intervenants chargés de la mise œuvre du plan de continuité ;