ODOS

Office de Développement et des Œuvres Sociales

POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION DE ODOS

Rédigée en 2017

Révisée en 2024

Introduction

Le système d'information de ODOS permet de collecter, de stocker, de traiter et de diffuser les informations sur les activités au sein de l'organisation. Il constitue donc un atout précieux qu'il convient de protéger avec la plus grande rigueur, car il participe à valoriser la confiance et la crédibilité auprès des bailleurs.

Dans ce contexte, le Conseil d'Administration et le Bureau de Coordination de ODOS sont résolument convaincus que la sécurisation du matériel informatique et des données informationnelles que traite le système d'information doit être un axe d'effort constant. La Coordination de ODOS est également engagée à mobiliser les moyens nécessaires à la mise en place et au fonctionnement de l'organisation de la sécurité du système d'information.

I- Inventaire des biens à protéger

Cette partie vise à déterminer les catégories homogènes de biens (matériels, immatériels, organisationnels) à intégrer dans la démarche d'analyse et de mitigation des risques.

1- **Les locaux**
   - Le bâtiment administratif,
   - Les bureaux.

2- **Logiciels**
   - Logiciel bureautique,
   - Logiciel antivirus,
   - Logiciels de gestion de la comptabilité.

3- **Infrastructure réseau et télécom**
   - L'autocommutateur,
   - Les routeurs et switches,
   - Le réseau informatique,
   - Le réseau téléphonique,
   - Le Téléphone de bureau.

4- **Terminaux utilisateurs**
   - Les ordinateurs de bureau,
   - Les ordinateurs portables,
   - Les appareils photographiques,
   - Les tablettes,
   - Les imprimantes,
   - Les scanners,
   - Les photocopieurs,

- Les stockages amovibles : les clés USB, les disques durs externes, les CD ROM,
- Un disque dur NAS mis en réseau pour tout le personnel.

5- Organisation

- Le personnel travaillant au bureau pour ODOS,
- Les données des activités,
- Le personnel d'appui sur le terrain,
- Les rapports d'audit, les rapports d'évaluation,
- Les documents de procédures, de politique, de convention.

II- Les principaux risques

Cette section synthétise les différents risques ou menaces qui pèsent sur ODOS et leurs sources. Ces menaces peuvent être d'origine humaine ou non humaine :

- Le personnel interne,
- Des criminels auteurs de vandalisme ou de vol,
- Des hackeurs,
- Des catastrophes naturelles.

EVENEMENTS REDOUTES (risques)	SOURCES	PROBABILITE (faible, moyenne, forte)	GRAVITE (mineure, modérée, majeure)	IMPACT (faible, moyen, fort)
Perte ou vol de matériel informatique	Sortie d'équipement non autorisée ni contrôlée	Forte	Modérée	Fort
	Accès non autorisé au bâtiment suivi de vol de matériel	Forte	Majeure	Fort
	Du matériel confié aux prestataires pour réparation	Moyenne	Modérée	Fort
Altération d'information (modification ou suppression)	Intrusion informatique	Faible	Majeure	Fort
	Code malveillant, virus	Moyenne	Modérée	Moyen
	Erreurs de saisie	Forte	Mineure	Moyen
	Détournement de logiciel	Faible	Majeure	Fort
	Hameçonnage	Faible	Majeure	Fort
Indisponibilité de service	Panne ou coupure électrique	Forte	Majeure	Fort

	Indisponibilité de la connexion internet	Forte	Majeure	Fort
	Catastrophe naturelles	Forte	Majeure	Fort
	Panne généralisée des équipements	Forte	Majeure	Fort
	Incendie ou inondation des locaux	Forte	Majeure	Fort
	Intrusion informatique ou physique	Forte	Majeure	Fort
Vol et/ou perte d'information	Les impressions et photocopies gâtées mises dans les poubelles	Faible	Majeure	Fort
	L'utilisation des disques amovibles personnels au bureau	Forte	Majeure	Moyen
	Non sauvegarde ni archivage des données	Forte	Majeure	Fort
	Accès non protégé des postes de travail	Forte	Majeure	Fort
	Mot de passe faible	Forte	Majeure	Fort
	Les ordinateurs remis pour réparation	Forte	Majeure	Fort

III- Les règles de sécurité à implémenter

Après avoir identifié les enjeux de sécurité, inventorié les biens à protéger et analysé les principaux risques, il ne reste qu'à définir les règles de sécurité concrètes à mettre en œuvre par les utilisateurs afin de réduire la probabilité de survenance de ces risques.

1. Engagement du personnel de ODOS aux enjeux de sécurité

1.1 Sensibilisation

La première mesure de sécurité du système d'information de ODOS est son personnel, donc chaque acteur du système d'information doit être formé au bon usage des outils informatique et télécom et des systèmes afin d'instaurer une culture de sécurité informatique.

1.2 Engagement

Une charte d'utilisation du système informatique sera remise contre émargement à chaque personnel.

2. Sécurité des locaux

2.1 Contrôle **d'accès aux locaux**

- matérialiser l'accès du personnel aux locaux les jours de service
- disposer des caméras de surveillance aux entrées des bureaux ou bâtiments si possible.

2.2. **Sécurité contre le dégât des eaux**

- disposer les ordinateurs sur des socles et non en contact direct avec le sol ;
- éviter de déposer les bouteilles d'eau et les tasses de café sur les machines ou à proximité des équipements ;
- prévoir le mécanisme d'évacuation de l'eau dans les locaux.

2.3. **Sécurité incendie**

- éviter les rallonges électriques en bois ;
- utiliser les rallonges équipées de fusibles ;
- réaliser les installations électriques avec des prises de terre ;
- disposer au moins d'un extincteur dans le bâtiment.

2.4. Services techniques

- climatiser les bureaux contenant du matériel informatique ;
- disposer des sources d'énergie électrique continue pour le bâtiment ;
- enfouillir les câbles réseau ou télécom dans des goulottes ou les encastrer.

3. Protection des postes de travail

3.1. Protection des accès aux postes

- il est interdit de laisser sa station de travail à une personne étrangère à l'institution c'est-à-dire une connaissance, un membre de famille, un(e) ami(e) ;
- l'accès aux sessions de poste de travail est conditionné par la détention d'un mot de passe. Chaque session est protégée par mot de passe (confère 4.1) ;
- il est interdit d'utiliser les équipements personnels (n'appartenant pas à ODOS) au service.

3.2. Protection des données des postes de travail

- éviter d'imprimer les documents confidentiels sur les imprimantes partagées ;
- programmer la mise en veille automatique des postes de travail après 5 min d'inactivité ;
- éviter de stocker directement les fichiers sur le bureau. Il est conseillé de créer un dossier sur une partition pour les sauvegardes ;
- installer un antivirus sur chaque poste de travail. Les antivirus gratuits ne sont pas conseillés ;
- il est interdit d'amener ou d'utiliser les supports amovibles du service à la maison ;

- brancher tous les postes sur onduleur et les batteries des ordinateurs portatifs doivent disposer d'autonomie en énergie électrique ;

4. Sécurité applicative

4.1 Contrôle d'accès applicatif

- définir les profils des accès aux données applicatives

- authentifier les utilisateurs par un login et un mot de passe : mot de passe alphanumérique de 8 caractères au moins.

4.2 Sauvegarde des données

Sauvegarder et archiver chaque jour les données sensibles de ODOS comme les courriers, les fichiers comptables, les rapports, les politiques sur les disques durs externes, sur le disque dur NAS mis en réseau et sur un espace en ligne.

5. Sécurité Réseau local et internet

5.1 Réseau sans fil (wifi)

- le code d'accès à ce réseau ne doit pas être communiqué à une personne externe, ni connecté aux équipements externes ;

- modifier régulièrement (au moins trimestriellement) le code d'accès wifi

5.2 Réseau filaire

- les câbles réseaux ne doivent pas joncher à même le sol, il faut les faire passer dans des goulottes ;

- les équipements terminaux du réseau comme les switches et les routeurs doivent être arrangés dans un coffret.

5.3 Internet

- Disposer d'une connexion internet secours (soit des clés nomades 4G ou 3G pour pallier l'indisponibilité de la connexion internet ordinaire).

- Il est interdit aux utilisateurs d'internet de stocker ou d'enregistrer les mots de passe dans les cookies pour l'authentification automatique aux pages web.

- Traiter avec précaution tout courrier électronique non sollicité et dont la provenance est inconnue.

- Chaque membre du personnel doit disposer d'une boite de messagerie professionnelle avec le nom de domaine « odoseadt.org » qu'il utilisera systématiquement pour tout échange professionnel par mail.

- Toutes les activités organisées par ODOS ou par un partenaire et auxquelles ODOS participe font l'objet d'une communication sur toutes les plateformes professionnelles de ODOS (LinkedIn, facebook, site internet…).

- Les échanges de mail d'un département à un autre doivent mettre en copie le responsable du département expéditeur.

- Tous les mails adressés à une personne externe à la coordination de ODOS ou à une institution partenaire doivent mettre en copie le secrétariat et le Coordonnateur National.

IV- La mise en œuvre et la mise à jour de la politique

1. La mise en œuvre efficace de la politique

La politique de sécurité du système d'information (PSSI) de ODOS est un document de référence, validé et appuyé par la Coordination, qui doit être pris en compte par l'ensemble des acteurs et utilisateurs du SI (Système d'Information). Le Coordonnateur National de ODOS doit adopter une démarche itérative et échelonnée dans le temps pour la mise en œuvre du contenu de ce document.

2. La démarche d'amélioration continue de la PSSI

La Politique de Sécurité du Système d'Information (PSSI) n'est pas un document figé. Elle suit l'évolution du contexte d'ODOS à laquelle elle s'applique, de manière à toujours être en phase avec l'activité de la structure. Une mise à jour s'impose à chaque fois que l'on constate une modification du SI (Système d'Information) ou l'entrée d'un équipement majeur dans le système.

Fait à Lomé, le 13 septembre 2024

Le Coordonnateur National

Dr. FLEVI Kossi Mensah