ONG
Femmes & Développement
FEDE

Site : www.fede-mali.com ; Facebook: Femmes et Développement

01/01/2019

LA POLITIQUE DE SECURISATION DES DONNEES

ONG Femmes et Développement ''FEDE''

Route de Kati 150 m du centre émetteur de l'ORTM à droite carrefour des médecins et 50 m droite du château vert
NIF n° 081113579X Accord cadre n° 0524 / 1582, Tel : 62 22 55 69/76 07 73 49
Adresse mail : fedev2000@yahoo.fr, fedevbko@gmail.com.

Table des matières

POLITIQUE DE SECURISATION DES DONNEES

La **protection des données** se traduit aussi dans le règlement par un renforcement du droit des personnes. Il s'agit notamment du droit à la portabilité de ses **données**, du droit à l'oubli et du droit de demander la suppression de ses **données**.

1. Respecter une politique rigoureuse de mot de passe

En premier lieu, il faut adopter **une politique rigoureuse de mot de passe**, étant donné qu'il est le premier levier de sécurisation d'un poste informatique. La première des protections est donc de restreindre l'accès à un poste de travail ou à un fichier, via un identifiant et un mot de passe. Ce mot de passe doit impérativement être individuel, difficile à deviner et bien sûr demeurer confidentiel. En outre, il ne doit être inscrit sur aucun support. Le responsable informatique doit déployer une politique de gestion des mots de passe particulièrement rigoureuse. Ainsi, un mot de passe devrait être constitué d'au moins 8 caractères, mêlant lettres, chiffres et caractères spéciaux. De même, il convient de le **renouveler environ tous les trois mois**, tout du moins de manière fréquente. S'il est attribué par l'administrateur d'un système, le mot de passe doit pouvoir être changé par l'utilisateur dès la première utilisation. Ces recommandations s'appliquent également aux administrateurs des systèmes et du réseau, en ce qui concerne les mots de passe qu'ils utilisent eux-mêmes.

2. Déployer une procédure de création et de suppression des comptes utilisateurs

De manière à **responsabiliser l'ensemble des intervenants** et éventuellement, être capable de retracer les actions effectuées sur un fichier, l'accès aux postes de travail et aux applications doit se faire uniquement via des comptes nominatifs. Ces comptes ne doivent pas être génériques, mais réellement personnalisés. Évitez ainsi les comptes du type "compta1, compta2, service-client, etc), qui ne permettent pas d'identifier précisément une personne, mais juste un service dans son ensemble.

3. Sécuriser au maximum les postes de travail

La première des recommandations à appliquer est de paramétrer les postes de travail de chaque agent, afin qu'ils se verrouillent automatiquement au-delà d'un certain temps d'inactivité (tout au plus 10 minutes). Dès qu'ils s'absentent de leur bureau, les agents doivent également être incités à verrouiller leur poste. Ces dispositions sont destinées à restreindre les risques d'une utilisation frauduleuse d'un poste de travail ou d'une application lors de l'absence momentanée d'un salarié. Il est par ailleurs fortement recommandé de contrôler l'usage des ports USB sur les postes dits "sensibles", en interdisant, entre autres, la copie de l'ensemble des données d'un fichier.

4. Identifier de manière précise qui peut avoir accès aux données à protéger

L'accès aux fichiers regroupant les données personnelles doit être limité aux seules personnes qui en ont légitimement besoin dans l'exécution de leurs missions. Lors de chaque mouvement de salarié ou affectation d'un agent à un poste, le supérieur hiérarchique alors concerné doit identifier les fichiers auxquels ce dernier a besoin d'accéder, afin de lui en accorder les droits. Il doit également penser à faire la mise à jour de ces mêmes droits, régulièrement, afin d'en interdire l'accès aux salariés dont les activités ne le justifient plus.

5. Assurer la confidentialité des données vis-à-vis des prestataires

En ce qui concerne **les contrats de sous-traitance**, il faut qu'une **clause de confidentialité** soit établie au sujet des données auxquels les prestataires peuvent avoir accès. Ainsi, les interventions des divers sous-traitants du système d'information doivent faire l'objet de garanties suffisantes, en termes de sécurité comme de confidentialité. De ce fait, la présence d'un salarié du système informatique est obligatoire lors d'éventuelles interventions de prestataires sur les bases de données de l'ONG.

6. Sécuriser le réseau local vis-à-vis des attaques extérieures

Des dispositifs de sécurité logiques et spécifiques, tels qu'une sonde anti-intrusions, des routeurs filtrants, un pare-feu, etc., doivent permettre d'assurer **un premier niveau de protection du réseau local** de l'ONG. Ces outils doivent être constamment mis à jour, afin d'assurer une protection fiable contre les logiciels espions et les virus. Ces outils doivent être renouvelés aussi bien au niveau du serveur que sur les postes de l'ensemble des salariés.

La messagerie électronique des salariés doit également faire l'objet d'une vigilance toute particulière, étant donné qu'elle est bien souvent la porte d'entrée à de possibles actes malveillants.

7. Assurer la sécurité de l'accès physique aux locaux

Il serait vain de sécuriser l'accès virtuel aux données détenues de l'ONG, si les locaux sensibles de cette dernière le sont insuffisamment. Ainsi, **l'accès aux salles hébergeant les serveurs informatiques** et autres éléments du réseau doit être strictement limité aux salariés habilités. Tout doit être mis en œuvre pour assurer leur sécurité : gardiennage, vérification des habilitations, portes fermées à clefs, accès par badge nominatif, etc.

8. Anticiper la perte ou la divulgation de données

Malheureuse erreur d'un salarié ou acte malveillant, vol d'un ordinateur portable, incendie, dégâts des eaux ou panne matérielle doivent être anticipés. Les données de l'ONG doivent ainsi être **stockées sur des espaces serveurs** prévus à cet effet, lesquels font l'objet de sauvegardes régulières. Par ailleurs, les supports de sauvegarde doivent impérativement se trouver dans un local distinct de celui hébergeant les serveurs ; l'idéal étant qu'ils se trouvent dans un coffre ignifugé.

Autre élément important à prendre en compte, **les supports nomades** (ordinateurs portables, clés USB, assistants personnels, etc.), qui doivent faire l'objet d'une attention particulière au

regard des données qu'ils peuvent stocker. Les matériels en fin de vie doivent ainsi être impérativement détruits ou bien expurgés de leurs disques durs avant d'être recyclés.

9. Consigner dans un document la politique de sécurité du système d'information

L'ensemble des règles portant sur la sécurité informatique doit être formalisé dans un document qui sera accessible par l'ensemble des salariés de l'ONG. Sa rédaction doit être anticipée en réalisant un inventaire **des potentielles menaces et vulnérabilité** pesant sur le réseau informatique. Ce document doit évoluer de manière régulière, à chaque modification des systèmes ou outils informatiques.

10. Sensibiliser les salariés à la loi Informatiques et Libertés et aux risques informatiques

En matière de sécurité informatique, le principal risque demeure l'erreur humaine. C'est pourquoi l'ensemble des utilisateurs du système d'information de l'ONG **doivent être sensibilisés aux différents risques** inhérents à l'utilisation d'une base de données.

Une charte informatique doit également être formalisée, laquelle regroupe, à destination de l'ensemble des salariés, les bonnes pratiques à adopter dans le cadre de l'utilisation de son poste de travail.

Fait à Bamako, Janvier 2019

La Directrice Exécutive