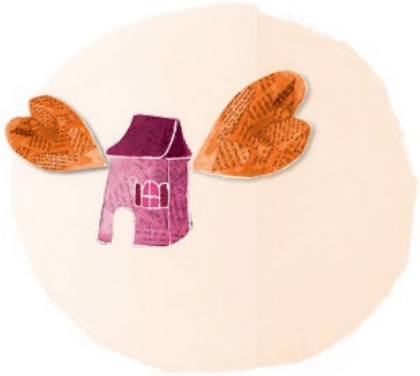
PROTOCOLE DE LA GESTION DE LA SÉCURITÉ DES INFORMATIONS

« La Méridienne 1990 »

Adopté le 14 septembre 2023



HISTORIQUE DES CHANGEMENTS AU DOCUMENT

Date de création	Août 2023
Version	Date de modification

OBJECTIF

Ce document clarifie les pratiques que l'équipe de travail de La Méridienne 1990 doit mettre en place et respecter afin de protéger la sécurité des documents, actifs informationnels et informations confidentielles avec lesquelles elles transigent dans le cours de leur travail.

CHAMP D'APPLICATION

Ce protocole vise principalement les travailleuses mais peut également s'appliquer aux administratrices, contractuelles et bénévoles qui partages des dossiers.

MODALITÉ D'APPLICATION

La direction de La Méridienne 1990 est responsable de la mise en œuvre et de l'application de ce protocole.

Les administratrices, la direction, les employées, les stagiaires et les bénévoles doivent remplir, dès l'entrée en vigueur de ce protocole, un formulaire d'engagement à respecter celui-ci.

Le protocole entre en vigueur le 14 septembre 2023.

PROTOCOLE

1. DOCUMENTS PAPIERS : CONSULTATION ET CONSERVATION

1.1. Ne consigner des renseignements personnels que dans les documents et les dossiers prévus à cet effet.

1.2. Conserver dans un lieu barré, tel un classeur, tous documents contenant des renseignements personnels.

1.3. Dans la mesure du possible, éviter de sortir de La Maison des documents contenant des renseignements personnels. Lorsque cela s'avère nécessaire, s'assurer que l'accès à ces documents demeurent protégé en tout temps, dans la voiture, les transports en commun, les endroits publics, votre domicile et tout autre espace de travail.

1.4. Les documents utilisés en contexte de télétravail doivent être rapportés et archivés à La Maison une fois leur consultation terminée.

2. Documents papiers : destruction

2.1. Ne jeter aucun document contenant des informations confidentielles dans les poubelles ou bacs de recyclage. Utiliser la déchiqueteuse.

2.2. A la fin de la période de conservation des dossiers, utiliser le protocole de destruction sécuritaire adopté par La maison.

3. Documents électroniques : consultation et conservation

3.1. Ne consigner des renseignements personnels que dans les documents et les dossiers prévus à cet effet.

3.2. Si vous utiliser TEAMS, option pour l'envoi du lien du document plutôt que d'une copie entre les membres de votre équipe. De cette façon, seules les personnes autorisées à consulter un dossier pourra le voir.

3.3. N'archiver ou ne copier aucun document contenant des renseignements confidentiels sur le disque dur de l'ordinateur.

4. Utilisation des ordinateurs, portables et tablettes.

4.1. Munir chaque ordinateur d'un mot de passe robuste et unique. Informer la responsable de la sécurité lors du changement de mot de passe.

4.2. Activer la fonction de mise en veille lorsque l'ordinateur n'est pas utilisé pour une courte période.

4.3. Fermer systématiquement son poste de travail à la fin de son quart de travail.

5. Utilisation d'un cellulaire personnel

5.1. Munir le cellulaire d'un mot de passe robuste et utiliser la reconnaissance faciale ou l'empreinte digitale lorsque possible.

5.2. S'assurer que le téléphone se verrouille automatiquement lors que vous ne l'utiliser pas.

5.3. Dans la mesure du possible, configurer l'option Traçage du mobile pour localiser votre appareil en cas de perte ou de vol.

5.4. Ne conserver pas de renseignements personnels des femmes ou enfants sur votre cellulaire personnel (nom, prénom, photos, documents, vidéos, etc).

6. Utilisation d'un cellulaire professionnel

6.1. Munir le cellulaire d'un mot de passe robuste et unique et informer la responsable de la sécurité lors de changements du mot de passe.

6.2. L'utilisation de la reconnaissance faciale ou l'empreinte digitale est encouragée.

6.3. Faire une sauvegarde de son téléphone régulièrement.

6.4. Aviser immédiatement sa coordonnatrice lors de la perte ou vol du cellulaire.

6.5. Utiliser la localisation géographique pour récupérer l'appareil.

6.6. Effacer les données à distance lors d'un vol ou d'une perte.

7. Gestion des clés d'accès

7.1. Garder les clés d'accès de la maison avec vous en tout temps lorsque vous êtes sur les lieux d'hébergement.

7.2. Informer immédiatement l'équipe lors de la perte de clés.

8. Télétravail

8.1. Utiliser le portable ou ordinateur mis à votre disposition par l'organisme employeur. Si vous devez utiliser votre propre ordinateur, s'assurer que :

- L'ordinateur est muni d'un logiciel antivirus reconnut et à jour.
- L'accès aux données confidentielles est protégé par un mot de passe unique qui n'est pas partagé par la famille ou les collègues.
- Les documents créés et consultés sont sauvegardés dans les dossiers de l'organisme et non sur le disque dur de l'ordinateur privé.

8.2. Porter des écouteurs pendant les vidéoconférences, lorsque vous n'êtes pas seule dans la maison.

8.3. Ranger les portables, téléphones et documents dans un tiroir barré à la fin de la journée.

8.4. Retourner tous les documents consultés au bureau.

9. Communication par courriel

9.1. Utiliser l'adresse courriel professionnelle remise par l'organisme employeur pour toutes les communications impliquant des renseignements personnels obtenus dans le cadre de l'emploi.

9.2. Ajouter un texte de mise en garde de confidentialité après la signature électronique tel que : Le présent courriel peut contenir des renseignements confidentiels. Si ce courriel vous est parvenu par mégarde, veuillez le supprimer et nous en aviser. Merci.

9.3. Éviter de conserver de courriels contenant des informations confidentiels et personnels. Les détruire une fois l'information entreposer dans le dossier légitime.

10. En cas d'incident de confidentialité

10.1. Aviser la responsable de la protection des renseignements personnels secteur intervention ou la responsable de la protection des renseignements personnels secteur administratif de tout incident de confidentialité.