Liste de contrôle de la sécurité des données pour améliorer la sécurité et la confidentialité des survivantes

L'ère de l'électronique a exacerbé nos besoins en matière de confidentialité. Cependant, les survivantes de violence conjugale, de violence à caractère sexuel et de harcèlement ont encore davantage de préoccupations en matière de sécurité. Toute initiative de collecte de données doit être soigneusement planifiée à partir de son déploiement et évaluée régulièrement, car la sécurité et la confidentialité des survivantes en dépendent.

La sécurité des données englobe toute une série d'enjeux, allant de la prévention des accès non autorisés à la minimisation des informations collectées et partagées. Compte tenu de la complexité des risques, ces bases de données pourraient devoir être stockées sur des serveurs distincts avec une sécurité accrue, confirmée par les différents fournisseurs de services, afin de préserver les privilèges et la confidentialité.

Cette liste de contrôle se veut un point de départ pour discuter de la sécurité de la clientèle et de celle des données; elle n'est pas destinée à remplacer une formation intensive sur la confidentialité.

Avant de commencer votre collecte de données

Minimiser les données récoltées	Minimiser les informations collectées auprès des survivantes vous permettra de réduire la responsabilité de votre organisation en cas de problème. Passez en revue les objectifs de votre organisation et évaluez votre processus de collecte de données • Existe-t-il des solutions moins intrusives pour mesurer les résultats au cours du processus d'admission? • Comment les données que vous allez collecter pourraient-elles être utilisées à mauvais escient si on y accédait par des moyens légitimes ou illégitimes?

	• Quelle est la quantité minimale d'informations que votre organisation doit collecter pour fournir des services?
Élaborer et mettre en œuvre des politiques claires	• Il est essentiel d'élaborer des politiques et des procédures qui décrivent les pratiques en matière de confidentialité pour le traitement des données sensibles. • Examinez la législation relative à la protection de la vie privée pour vous assurer que vos politiques sont conformes à la loi. • Communiquez régulièrement ces politiques lors des séances d'orientation et des réunions.
	Les politiques de sécurité des données doivent porter sur les points suivants: • Le contenu du dossier, sa durée de conservation et les personnes qui peuvent y accéder • Procédures permettant aux survivantes d'examiner, de retirer ou de corriger leurs données ou leurs dossiers, ou d'empêcher toute information d'être recueillie • Collecte, modification, utilisation et divulgation de données identifiantes • Procédures d'élimination sécurisée des ordinateurs ou autres supports électroniques contenant des données identifiantes • Procédures de sélection, de formation et de vérification des antécédents des personnes ayant accès à des informations sensibles • Procédures de protection contre l'utilisation et l'accès non autorisés

Évaluations de l'impact sur la confidentialité	Les agences gouvernementales réalisent des évaluations de l'impact sur la vie privée (EIVP) pour répondre aux questions suivantes: • Types d'informations collectées • Objectifs de la collecte • Utilisations prévues de l'information • Partage d'informations • Notification à la clientèle • Sécurité de l'information Vérifiez auprès du fournisseur de la base de données si une évaluation des incidences sur la performance a été réalisée pour son produit et si elle est disponible.
Séparer les données	Les bases de données contenant des notes de cas et d'autres informations sensibles doivent être soigneusement protégées. Conservez les notes de cas séparément pour éviter toute mention d'autres survivantes en cas de citation à comparaître. Par exemple, des auteurs de violence peuvent assigner les organisations à comparaître pour obtenir les dossiers de leurs enfants. Envisagez de séparer les données relatives aux enfants et aux mères afin d'éviter de fournir des informations sur les survivantes par inadvertance.
Limiter les niveaux d'accès	Limitez le nombre de personnes autorisées à consulter les informations les plus sensibles. Pour déterminer les niveaux d'accès, vous devez tenir compte des risques de sécurité si les données sont partagées de manière interne ou entre organisations. Il est essentiel d'examiner les lois sur la protection de la vie privée qui stipulent qui peut accéder aux données.

Éléments essentiels à prendre en compte lorsque vous concevez un système de gestion des données

Testez votre sécurité	Embauchez une société de consultation ou de sécurité compétente et digne de confiance pour tester votre réseau et vos procédures de protection des données. Un contrôle de sécurité externe peut fournir une analyse

	approfondie des points faibles ou des éléments manquants.
Tenir les données des survivantes à l'écart de l'Internet	Le moyen le plus sûr de protéger les informations sensibles est de disposer d'ordinateurs distincts: un pour Internet et les courriels et un autre pour toutes les données sensibles si vous optez pour une base de données interne située sur vos serveurs (plutôt qu'un service infonuagique). Ces ordinateurs désignés ne doivent pas être connectés entre eux. Les pare-feu et les antivirus sont utiles (voir ci-dessous), mais peuvent être compromis. Lorsque des vies sont en jeu, protégez vos données.
Utiliser des antivirus et des pare-feu	Si vous disposez d'un réseau professionnel, utilisez des antivirus ou des pare-feu. Les antivirus ou les pare-feu matériels sont des mesures de sécurité importantes et vont de pair avec un accès Internet.
Utiliser le cryptage	Le cryptage est la conversion de données sous une forme qui ne peut pas être facilement déchiffrée par des comptes non autorisés. Le cryptage n'est pas la solution à tous les problèmes de sécurité; c'est un élément dans une stratégie beaucoup plus complexe. Envisagez l'acquisition d'une base de données dotée d'un cryptage de bout en bout ou d'un cryptage à connaissance nulle.

Maintenance, contrôles et formations

Mise à jour des systèmes d'exploitation	Téléchargez régulièrement les mises à jour de vos systèmes d'exploitation.
Utilisez des mots de passe forts, à modifier fréquemment	La gestion des mots de passe est un élément essentiel de la sécurité des données. L'utilisation de noms d'animaux, dates d'anniversaires ou de mots du dictionnaire devrait être interdite. Les mots de passe doivent être changés fréquemment et conservés en lieu sûr; ne les gardez pas sous le clavier ou sur l'écran! Un écran de veille activé par le personnel à l'aide d'un mot de passe peut protéger des informations sensibles et assurer la sécurité des données.

Contrôle de qualité des données	Il s'agit d'un processus d'évaluation des données collectées et de suppression de toute information incorrecte. Au minimum, le personnel chargé de la saisie quotidienne des données ne devrait pas être responsable de ce contrôle. Il s'agit d'un processus qui devrait inclure des échantillons aléatoires d'informations collectées sur les survivantes afin d'évaluer leur qualité et exactitude, et d'identifier si des données inappropriées sont collectées ou partagées.
Faire appel à des professionnels qualifiés	La plupart des OSBL ne disposent pas d'un personnel informatique à temps plein. Il est cependant impératif que les organisations qui collectent des données sensibles bénéficient d'une assistance technique professionnelle qualifiée. Pour limiter les coûts, renseignez-vous auprès d'autres organisations antiviolence sur la possibilité de passer un contrat pour utiliser leur base de données comme point de départ.
Formation permanente	Participez à des formations ou invitez des spécialistes pour parler de la sécurité des données pour le bien des survivantes. La formation continue sur la sécurité des données est d'autant plus importante lorsque le roulement du personnel est élevé.

Pour soutenir le développement de politiques sécuritaires, HFC a rédigé le document Use of Technology Policy Template Guide for Women's Shelters and Transition Houses (PDF, en anglais).

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter *hebergementfemmes.ca* pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un *plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.*

Adapté pour le Canada avec l'autorisation du projet Safety Net du NNEDV, d'après leur ressource Data Security Checklist to Increase Service User Safety & Privacy.

Ce projet est rendu possible grâce au financement du ministère Femmes et Égalité des genres Canada (FEGC).

Women and Gender Equality Canada | Femmes et Égalité des genres Canada