

 <b>Hôpital St-Boniface Hospital</b> <small>FONDATION • FOUNDATION</small>	<b>Titre de la politique</b> Politique de protection des renseignements névralgiques contenus dans les systèmes de TI
	<b>Approuvée par :</b> Conseil d'administration de la Fondation de l'Hôpital Saint-Boniface <b>Entrée en vigueur :</b> Le 11 décembre 2015  <b>Demandée par :</b> Comité des finances de la Fondation de l'Hôpital Saint-Boniface <b>Date de la prochaine révision :</b> Mars 2017

## **POLITIQUE – Politique de protection des renseignements névralgiques contenus dans les systèmes de TI**

La Fondation de l'Hôpital Saint-Boniface s'engage à protéger la confidentialité des renseignements concernant la Fondation et ses donateurs, et à les protéger contre les cyberattaques. De plus en plus de renseignements sont stockés électroniquement et sont hébergés dans les locaux de la Fondation ou chez des fournisseurs indépendants dignes de confiance. L'objectif ultime consiste à s'assurer que toutes les données sont protégées à l'intérieur d'une infrastructure sûre.

Afin de réduire les risques et de maintenir la confiance des donateurs et de la population, la Fondation engagera une tierce partie pour procéder annuellement à des vérifications de sécurité dans le but d'évaluer la vulnérabilité des systèmes. Aucun système n'est impénétrable, mais la présente politique permet à la Fondation de gérer le risque en mettant en œuvre des recommandations formulées par des experts indépendants.

### **Mesures de surveillance précises**

Voici certains aspects de l'infrastructure qui doivent être surveillés. Il ne s'agit toutefois pas d'une liste exhaustive :

- Évaluation de la sécurité du réseau
  - Vue d'ensemble de la situation en matière de sécurité d'une perspective interne.
  - Évaluation des menaces internes.
  - Déterminer si les vulnérabilités techniques cernées pourraient être exploitées.
  - Déterminer dans quelle mesure les usagers internes peuvent représenter une vulnérabilité exploitable sur le plan de la sécurité de l'organisation.
- Test d'intrusion des applications Web
  - Sécurité des applications.
  - Systèmes de surveillance et d'alarme de détection d'intrusion.
  - Coupe-feu.
  - Fiabilité des mots de passe et gestion des séances.
  - Configuration et sécurité de l'hôte.
- Test d'intrusion externe
  - Fournir une vue d'ensemble de la situation de l'organisme en matière de sécurité externe.
  - Identification et évaluation des menaces externes.
  - Déterminer si des vulnérabilités techniques pourraient être exploitées.

- Déterminer dans quelle mesure les usagers internes peuvent représenter une vulnérabilité exploitable sur le plan de la sécurité de l'organisation par des techniques d'ingénierie sociale.
- Présenter un rapport détaillé des conclusions et une liste des priorités en matière de mesures correctives à mettre en place.

### **Fréquence**

- La Fondation engagera une tierce partie pour procéder annuellement à une vérification des systèmes de TI. Cette vérification consistera en une vérification de la sécurité du réseau en alternance à des tests d'intrusion des applications Web et d'intrusion externe. Le calendrier permettra de procéder à une budgétisation efficace et de répondre à toute préoccupation soulevée dans les rapports.
- Le calendrier suivant servira de guide. Les évaluations ou les tests d'intrusion peuvent être faits à tout moment, si le personnel de la Fondation ou les membres de son conseil d'administration estiment qu'un risque existant justifie une évaluation additionnelle.
  - Les années paires : Évaluation de la sécurité du réseau.
  - Les années impaires : Tests d'intrusion des applications Web et d'intrusion externe.

### **Marche à suivre**

- Le directeur de la Technologie ou son représentant engagera annuellement des consultants externes spécialisés en sécurité de réseau.
- Au besoin, plusieurs fournisseurs pourraient être invités à présenter un devis pour les services demandés.
- Le directeur de la Technologie ou son représentant recommandera au vice-président des Finances le fournisseur de son choix pour l'évaluation ou les tests d'intrusion.

### **Reddition de comptes**

- Le vice-président des Finances présentera annuellement au comité des finances des recommandations formulées par des spécialistes externes, ainsi que le plan d'action élaboré par la Fondation.