| | |
|---|---|
| Hôpital St-Boniface Hospital<br>FONDATION · FOUNDATION<br><br>**POLICIES & PROCEDURES** | **Policy Name**<br>IT Systems Critical Information Safeguarding Policy |
| | **Approved By:**<br>St. Boniface Hospital Foundation Board of Directors<br>**Effective Date:** December 11, 2015<br><br>**Originated by**:<br>St. Boniface Hospital Foundation Finance Committee<br>**Date of Next Review**: March 2017 |

## POLICY – IT Systems Critical Information Safeguarding Policy

St-Boniface Hospital Foundation is committed to ensuring that Foundation and donor data are kept confidential and secure from cyber-attacks. More and more information is stored electronically and hosted locally within the Foundation or hosted externally with reputable third party vendors. Ensuring that all data is kept secure within a protective infrastructure is the ultimate goal.

In order to reduce the risk and maintain the trust and confidence of our donors and public, the Foundation will annually engage an external party to conduct network security audits to determine if there are any vulnerabilities. No systems are impenetrable but this policy will allow the Foundation to address risk by implementing recommendations provided by external experts.

## Specific monitoring areas to be covered

The following are some areas within the infrastructure to be covered but not necessarily an exhaustive list:

- Network Security Assessment
  - Comprehensive view of security posture from an internal perspective
  - Evaluation of internal threats
  - Determines whether identified technical vulnerabilities may be exploited
  - Determines the extent to which internal users may represent an exploitable vulnerability to the organization's security
- Web Application Penetration Test
  - Application Security
  - Intrusion Detection Monitoring and Alerting
  - Firewall
  - Password Strength and Session Management
  - Host Configuration and Security
- External Penetration Test
  - Provides a comprehensive view of the organization's external security posture
  - Identification and risk evaluation of external threats
  - Determines whether technical vulnerabilities may be exploited
  - Determines the extent to which internal users may represent an exploitable vulnerability to the organization's security through social engineering techniques
  - Provides a detailed account of findings and a prioritized list of remediation actions to be taken

## Frequency

- The Foundation will annually hire an external party to review key IT systems. This review will alternate between a Network Security Assessment and Web/External Penetration Tests. This schedule will allow for effective budgeting and the ability to implement and address any concerns noted in the reports.
- The following schedule will be used as a guide. Assessments and or penetration tests can be conducted at any point if the Foundation staff or Board deems there to be a relevant risk that warrants additional assessing.
    - Even Years Network Security Assessment
    - Odd Years Web Application Penetration and External Penetration Test

## Procedure

- The Director of Technology or delegate will annually engage external consultants whose expertise is network security.
- As required, quotes may be requested from several vendors who offer the required service.
- The Director of Technology or delegate will recommend to the Vice President of Finance the vendor of choice for the assessment and/or penetration tests.

## Reporting

- The Vice President of Finance will annually provide the Finance Committee with recommendations from the external experts and the corresponding Foundation action plan.