**Blind River District Health Centre – Testing Strategy**

Team #3

By: Marki, Ryan, Reshma, Krunal, Jagsir

Fifteen features will be tested in the Blind River District Health Centre redesign. In the following paragraphs we will briefly describe the procedures and testing to reduce the chances of security issues and increase confidence in the quality of the product delivered.

For users to interact dynamically with the BRDHC website, they will be required to submit information through input fields and textboxes. The features that will be utilizing these user inputs include, forms (careers page, volunteers page, contact us, events calendar, etc) and search fields (find a doctor). Furthermore, the submission and uploading of files to the database for review will also be required in key areas of the website. Although these features provide a service to our users, it creates an entry point for malicious attacks which may include and are not limited to SQL injections, and malevolent scripts.

Textboxes across all pages will be sanitized to prevent any UTF-8 entrees that are either invalid, or entities that may be malicious. By sanitizing, we can prevent input data from running or inserting scripts, as well as anything that can harm the integrity of the database.

As a user submits and uploads data to the database the content will be screened for correct formatting and character types. Career and Volunteer pages create a greater risk for security, as uploaded data can potentially be dangerous. Therefore additional precautions will be made to verify and determine correct file formats as users upload files to the database, ensuring that for instance only PDF’s and Word documents will be uploaded to the careers and volunteers page.

We will also ensure that non-public data will only be accessible upon the successful login and authentication of unique users, and only relevant and necessary information will be made available to them. On each dashboard page associated with user’s and their roles, private information will only be shared with those appropriate users, and attempts to access, modify and delete this data will fall within the scope and privileges of that user as determined by the administrator.

The donation page and bill payment page create another security risk access point. Dealing with money is a highly delicate undertaking; therefor to ensure the completion and authentication of these transactions we will utilize security protocols involving non-repudiation (PayPal). This will safeguard monetary transactions, as this third party service will provide proof of integrity and origin of data, preventing bots and related malicious programs from exploiting our website.

Confidential data that is stored within our database will also be encrypted, such as passwords and user medical information. As an added precaution, user created passwords will be strength tested, ensuring the creation of sufficiently secure passwords. Moreover, all activity on the website will be monitored in order to identify malicious intent or actions. Under the circumstances that breaches of security are detected the appropriate counter measures will be triggered. In the most severe of cases the website will be placed offline, thus preventing any and all compromises of confidential data.