Board of Health Manual
Public Health Sudbury & Districts

Procedure

Category

Board of Health Administration

Section

Technology

Subject

Board of Health Mobile Device Use

Number

I-V-10

Approved By

Board of Health

Original Date

February 2015

Revised Date

September 19, 2024

Review Date

September 19, 2024

Process

1. All devices will be registered with Information Technology and will be managed by its Mobile Device Management software (MDM).

2. Devices must be configured with a password.

3. A secure/strong password is required in order to access the device and the Board of Health application. The password for the Board of Health application and the device should be different. The device/application passwords must follow these rules:

   - A minimum of 8 characters and must use at least one Uppercase, one number and one special character (!@#$%^&*(){}[]);
   - These passwords will not expire unless there is reason to believe there has been unauthorized access;
   - Device and application passwords allowing access to Agency resources must never be stored on the mobile device in unencrypted format, be written down

in any form or shared with anyone that would allow users to gain access to resources.

- The Board of Health application password will be managed by the Executive Assistant to the MOH/Secretary to the Board of Health.

4. Users should always maintain physical control of the device in order to protect against theft or loss and natural/environmental hazards.

5. Board members must report lost, stolen or damaged devices to Information Technology immediately by calling 705.522.9200 ext. 300. Outside of normal business hours please leave a message. Information Technology can remotely wipe the device or lock the device to prevent access. If the device is recovered, it can be submitted to IT for re-provisioning.

6. The addition of hardware or software and/or related components to provide additional mobile connectivity will be managed at the discretion of Information Technology. Information Technology reserves the right to monitor, audit and restrict access to features on the device in order to protect the safety and security of the device.

7. Devices are to be returned to Executive Assistant to the Medical Officer of Health and Secretary to the Board of Health at the end of the Board member’s term. All device passwords must also be provided to the Board Secretary at that time.