Technical Controls and Physical Work Space Checklist for Foundry Service Providers who may be working from home

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Foundry Centre: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PURPOSE:

As we are in the current state of emergency, we know that many service providers are working from home. As part of this, some of your team members may be accessing Toolbox from home and they may be using their personal computer for this work. The purpose of this document is to outline the technical and physical requirements they should meet in order to utilize Toolbox for entering client information from home.

Client confidentiality is a large consideration when arranging an at-home workspace to ensure that no other person in the household can view information and the information is maintained securely. Service Providers are responsible for protecting the security and privacy of the information they handle and the technology they use. The checklist below will help them determine if they have a home working environment that provides the security and privacy for carrying out their roles.

Please note that this checklist will help ensure all other systems they are accessing from home (e.g. your EMR, video conferencing/chat technology, etc.) are as secure as possible.

Please fill out this document and submit it to datamanager@foundrybc.ca

# Technical & Physical Assessment – please complete this checklist

NOTE: The following technical and physical controls must be in place

|  |  |  |
| --- | --- | --- |
| **Technical Considerations** | **Yes** | **No** |
| 1. Are all service providers using a computer provided by a health authority?

If YES, skip to number 10 |  |  |
| **Home computer** |  |  |
| 1. If any staff are using a shared home computer, are there separate user profiles and access passwords set up for their work-related activities?
 |  |  |
| 1. Are screen savers set to time out after 15 minutes of inactivity?
 |  |  |
| 1. Does the screen saver require a password for re‐activation?
 |  |  |
| **Home computer – Virus Protection / Firewall** |  |  |
| 1. Is there active anti‐virus software installed on all computers being used at home? E.g. Norton, Bitdefender, Kaspersky
 |  |  |
| 1. Is the anti‐virus software configured to receive updates regularly?
 |  |  |
| 1. Is a full computer virus scan set to run on a weekly basis on all computers?
 |  |  |
| **Home computer – Operating System, Internet browser, Application Software** |  |  |
| 1. Is the Operating System (OS) on computers being use at home up‐to‐date (Windows update, Mac OS updates)?
 |  |  |
| 1. Are the applications (e.g. Microsoft Office, Adobe Reader) kept up‐to‐date with security patches?
 |  |  |
| **Wireless Network**  |  |  |
| 1. Do their home wireless networks have a secure password?
 |  |  |
| 1. Do their home wireless networks have encryption enabled?

*To find out if your wireless network has encryption enabled you can:** *Google the model number of your router and look for the manual online*
* *Call your Internet Service Provider (e.g. Telus, Shaw) for support*
 |  |  |

|  |  |  |
| --- | --- | --- |
| **Physical Environment** |  |  |
| 1. Are computer monitors positioned so that unauthorized individuals cannot see the screen?

In addition to ensuring they have the appropriate technical controls and a secure physical workspace, please note the following requirements:* They will log out of Toolbox when leaving the computer unattended and at the end of their shifts.
* They will not enable any passwords to be saved by a shared home computer web browser. The password must be entered each time.
 |  |  |

|  |
| --- |
| Form completed by:  Name: |
| Signature: |
| Date: |