Securely working from Home

Northern Health's Information Security team would like to provide you with security focused guidance for working from home (WFH).

Physical Security

The first so-obvious-it's-not-obvious tip is to make sure your work devices are physically safe, and that you avoid offering unauthorized views of confidential information. Here are a few ways to shore up physical security while WFH:

- If you need to leave your home for supplies or other reasons, make sure your work devices are either shut down or locked—including any mobile phones you might use to check email or make work phone calls.
- If you live with a roommate or young children, be sure to lock your computer even when you step away for just a bit. Don't tempt your roommates or family members by leaving your work open. This is true even for the workplace, so it is imperative for WFH.
- If you can't create a separate work space in your home, be sure to collect your devices at the end of your workday and store them someplace out of sight. This will not only keep them from being accidentally opened or stolen, but will also help separate your work life from your home life.

NH System access

If you think cybercriminals (and regular criminals) will be sensitive to global events and refrain from attacking remote workers, sadly, you'd be mistaken.

- Make sure you've read NH's Remote Access policy and standard.
- Ensure you're able to access NH's remote access systems prior to leaving the office to commence WFH. Requesting remote access is done via the User Access Portal.
- Access to your computer is password protected, ensure the password is a strong one. If the system is stolen, this will keep the thief from easily accessing sensitive information.
- Data encryption is active on your work machine, leave it that way! Encryption helps protect information on stolen or compromised computers.
- Speaking of stolen, if you misplace your system or know that it's been stolen, contact the ITS Service Desk ASAP at its.servicedesk@northernhealth.ca or 1-888-558-4357.

Separate work and personal tasks

Easier said than done, we know. Still, just as it's important to establish boundaries between work life and home life while WFH, the same is true of devices. Do you have a child being homeschooled now and turning in digital assignments? Are you ordering groceries and food online to avoid stores? Best not to cross those hairs with work.

While it may seem cumbersome to constantly switch back and forth between the two, do your best to at least keep your main work computer and your main home computer separate (if you have more than one such device). If you can do the same for your mobile devices—even better. The more programs and software you install, the more potential security risks you introduce.

- Don't use your work computer for personal entertainment, doing so could violate company policy.
- Don't pay your home bills on the same computer you compile work spreadsheets.
- Don't send work-related emails from your personal email address and vice versa. Not only does it look unprofessional, but you could be violating company policy.

Secure your home network!

- Secure your home Wi-Fi with a strong unique password.
- Keep your Internet router software up to date (often completed by your Internet service provider).
- Access to the settings on your home Internet router should be password protected. Be sure to change the default password it came with—no 12345, people!
- Consider adding a secure DNS provider to your home router. The Canadian Internet Registry Authority (CIRA) provides a great free service. Details located on their website here: https://www.cira.ca/cybersecurity-services/canadian-shield

For more Cybersecurity best practices please visit our InfoSec page on OurNH. Feel free to contact us anytime at INFO-SECURITY@NORTHERNHEALTH.CA