Business Resource Committee (OBRC)

Working From Home

April Papineau – Community Living Haldimand

OBRC Webinar April 23,2020

Covid 19 Telecommuting/Work From Home Policy

Granting of Telecommuting privileges

Conditions under Arrangements

- Internet connections- private, password protected
- Documents & email- safeguarded as confidential
- Remain available and contactable throughout the day

Health, Safety & Liability

- Employees responsibility to keep a safe and fit for work environment at home and outlines employees obligation to identify and remove and potential hazards

Covid 19 Telecommuting/Work From Home Policy

Privacy, Confidentiality and Data Security

- All Agency owned equipment and data remain the property of the employer
- Back up practices are followed
- No third-party technicians other than those pre- approved in writing
- Data breach -report to HR

Duration Amendment and Revocation

- Employer can amend or withdraw arrangement at any time.
- In the event of termination of employment employee agrees Employer may immediately revoke access to accounts and equipment and documentation without notice. Employee agrees to return all issued equipment and documents within 3 calendar days.

Covid19 Telecommuting/Work From Home Policy

General

- Payroll will continue to be administered in the ordinary course
- Employer will not involve itself with tax affairs of the employee
- This policy does not detract from any existing Policies and procedures

Signatures & Acknowledgment

Link to Policy:

- Telecommuting-Working From Home Policy

Cyber/Digital Best Practices: Working from Home during COVID 19

Rapidly emerging security threats

Know what you are dealing with

Malware	Spam	Phishing	Spear Phishing	Spoofing	Adware

Cyber/Digital Best Practices: Working from Home during COVID 19

Verify	Verify information – phone call to colleague you are receiving request from
Verify	Verify authenticity from request from outside, financial information data or funds.
Don’t fall	Don’t fall for “rush” requests even if from ED or HR
Don’t open	Don’t open links, attachments or files from banks, CRA, or Public Health
Ensure	Ensure Wi-Fi connection is secure, and you are using a work-exclusive Wi-Fi Network.
Ensure	Ensure all anti virus is in place and updated
Ensure	Ensure all security software is up to date and lock your screen

Examples of Know Threats

Malware contained within email updates purporting to be sent by the World Health Organization, Centres for Disease Control and Prevention, Public Health Ontario, Health Canada, *etc*.

Phishing emails, robo-calls, text messages and other communications promising advanced access to COVID-19 vaccinations in exchange for credit card and other personal information.

Fraudulent emails from third parties purporting to be charitable organizations seeking donations in support of their efforts to respond to COVID-19.

Spoofing attempts from senior executives within organizations asking for funds to be directed to external third parties.

Spear Phishing attempts, often leading to account takeovers initiated after individuals have clicked on links found within fraudulent or malicious emails, text messages, *etc*.

What to do if you are experiencing issues

Include contact information during and outside of business hours

Link to: Cyber-Digital Best Practices

Resources & Acknowledgments

A special thank you to LeClair & Associates for sharing templates – they do not constitute legal advice.

Https://www.leclairandassociates.ca/about/

Pooran Law is another great resource sign up for their weekly webinars

https://pooranlaw.com/