Company Internet and Technology Policy
(last updated October 2017)

This internet usage policy outlines guidelines for using our Company's internet connection, network and technology equipment. This policy applies to all employees, consultants and contractors (herein referred to as "**workers**").

Summary
Voice mail, email, internet usage assigned to a worker's computer or telephone extensions are solely for the purpose of conducting Company business.

Software Access Procedure
Software needed, in addition to the Microsoft Office suite of products, must be authorized by your manager and downloaded by IT support. If you need access to software or websites not currently on the Company network, speak to your manager to explain what returns you expect to receive from the product. All reasonable requests, not considered a network risk, will be considered for you and other workers.

Company Owned Equipment
Any device or computer including, but not limited to, desk phones, smartphones, tablets, laptops, desktop computers, GPS devices, satellite phones, and iPads that the Company provides for your use, should only be used for Company business.

Keep in mind that the Company owns the devices and the information in these devices. If you leave the Company for any reason, the Company will require that you return the equipment on your last day of work.

You may use personal electronic devices that are not connected to the Company network to access any appropriate internet site during breaks and lunch.

Internet Usage
Internet use, using company-owned devices connected to the Company network, is only authorized to conduct Company business. Internet data usage is tracked by the Company for all devices.

We ask workers to limit internet use. Internet use brings the possibility of breaches of the security of confidential Company information. Internet use also creates the possibility of contamination to our network via viruses or spyware. Spyware allows unauthorized people, outside of the Company, potential access to Company passwords and other confidential information. Removing such programs from the Company network requires IT support to invest time and attention that is better devoted to making technological progress.

Additionally, under no circumstances may Company owned computers or other electronic equipment, including devices owned by the workers, be used on Company time at work to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-business-related internet sites.

Social Media

Workers are not permitted to use social media including but not limited Facebook, Twitter, Instagram, Snapchat etc. during work hours unless required under their job description and authorized in writing by their manager.

Confidential Information

You are prohibited from sharing any confidential or protected information that belongs to or is about the Company. You are strongly encouraged not to share disparaging information that places your Company or co-workers in an unfavorable light. The Company's and co-worker reputations should be protected by all workers.

Email Usage at the Company

Workers are to be cautious and diligent when opening any suspicious emails or downloading and opening/executing files and software. The Company is inundated with what appears to be emails from, for example, chartered banks such as CIBC or BMO, Microsoft Exchange, etc. Some helpful hints follow:

- check the sender's email address which sometimes provides clues with an unusual email address or domain;
- never open any winzip type files contained within or attached to a suspicious email;
- be aware that attachments contained within an email may also be dangerous;
- never click on "click here" pdf and other links within a suspicious email.

If in doubt, contact the email sender via the regular business telephone number (not the one included in the suspicious email). Also, consider contacting IT Support to scan the suspicious email prior to opening it.

Email is to be used for Company business only. Company confidential information must not be shared outside of the Company, without authorization, at any time.

Sending or forwarding non-business emails is not permitted. Please keep this in mind, also, as you consider forwarding non-business emails to associates, family or friends. Non-business related emails waste company time and attention.

No personal business is permitted using the Company's assets or email addresses.

Viewing pornography, or sending pornographic jokes or stories via email, is inappropriate. Immediate termination is the most frequent disciplinary action.

Any form of email content related to discrimination against any protected classification including age, race, color, religion, sex, national origin, disability, or genetic information is prohibited.

What is inappropriate internet usage?

- Download or upload obscene, offensive or illegal material;
- Send confidential information to unauthorized recipients;
- Invade another person's privacy and sensitive information;
- Download or upload movies, music and other copyrighted material and software;
- Visit social media sites at any time using Company equipment;
- Visit potentially dangerous websites that can compromise the safety of our network and computers;
- Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods and more.

Keep in mind that the Company owns any communication sent via email or that is stored on Company equipment. Management and other authorized staff have the right to access any material in your email or on your computer at any time. Please do not consider your electronic communication, storage or access to be private if it is created or stored on the Company's assets including but not limited to local computers, laptops or the network.

Company-issued equipment

We expect our workers to respect and protect our Company's assets. "Company equipment" includes company-issued phones, laptops, tablets, GPS devices, satellite phones, and any other electronic equipment, and is owned by the Company. Workers are responsible for their equipment at all times including when they take it out of the office.

The Company maintains anti-virus and disk encryption software on our computers and network servers. Workers may not deactivate or configure settings and firewalls.

Disciplinary Action

A worker who violates this policy will face disciplinary action. Serious violations will be cause for termination or legal action, as appropriate.

***

I have read and understand the above **Company Internet and Technology Policy.**

_____

Name:
Date: