Sample Employer Policy – Acceptable Use Policy

[This Sample is a draft only and is not intended to be legal advice. Employers must review and consider their legal obligations and appropriate rules. There may be good reason to take a different approach to various aspects of this policy. Further guidance may be appropriate in areas not covered in this sample. Highlights indicate areas which most likely require modification to the particular workplace.]

1. PURPOSE

Company Name (the "**Company**") provides technology for use in the furtherance of its business objectives. The purpose of this Acceptable Use Policy (the "**Policy**") is to outline acceptable use of technology at the Company and to ensure the risks associated with inappropriate or unauthorized use of computer technology are adequately managed to support business objectives.

For the purpose of this Policy, technology includes, but is not limited to, computers, laptops, mobile devices, internet, software, systems, email, telephones, voice mail and related equipment ("**Company Technology**"). Users of Company Technology must respect the rights of other users, respect the integrity of the Company Technology and observe all relevant laws and regulations.

2. SCOPE

This Policy applies to all employees (including temporary employees) who use the Company Technology ("**Users**"). This Policy applies to the Company's unionized and non-unionized workforce. With respect to the Company's unionized workforce, to the extent that there is any inconsistency between the provisions of this Policy and the applicable collective bargaining agreement, the provisions in the collective bargaining agreement will prevail.

3. RESPONSIBILITIES

(a) Acceptable Use

The Company provides Company Technology to Users for legitimate business purposes. Users are expected to exercise good judgment and professionalism in the use of all Company Technology.

Incidental and occasional personal use of Company Technology is permissible as long as it does not interfere with workplace productivity or the Company's systems or business operations, does not pre-empt any business activity, does not consume more than a trivial amount of the Company's resources and is lawful. Users should be aware that all use of Company Technology is subject to monitoring as described in this Policy and as such, Users have no right to, or

expectation of, privacy with respect to their use of Company Technology, subject to applicable laws.

Notwithstanding the above, any use of the Company Technology must be in accordance with the provisions set out within this Policy. If a User requires additional clarification about the appropriate use of Company Technology, they should contact their manager.

(b) Unacceptable Use

The relationship between the Company and its Users is based on trust. This trust must be maintained at all times as it is fundamental to the employment relationship. Users must, at all times, hold themselves to the highest standards of conduct so as to maintain the Company's reputation and the integrity of the Company's business.

Users shall not be permitted to use any of the Company Technology to:

- solicit or recruit for any non-job-related commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations;
- store, access, transfer, download, upload, communicate or create any fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, libelous, slanderous, threatening, abusive, defamatory, or otherwise unlawful or inappropriate materials;
- download entertainment software or games, or to play games over the Internet;
- access Internet sites for gambling or any illegal activity;
- embarrass Company executives, or to jeopardize the Company's reputation;
- download, store or transmit material that infringe any copyright, trademark or other proprietary right;
- post or transmit proprietary or confidential information related to clients, suppliers, vendors, allied parties, or other third parties;
- post or store Company business-related information on public storage sites;
- download or distribute pirated software or data;
- deliberately propagate a virus, malware, or any other malicious program code;
- send confidential Company information without prior authorization from the proper authoritative manager. Such confidential information includes, but is not limited to, Company copyrighted materials, trade secrets, intellectual property, proprietary financial information, employee information, customer information, or other similar materials that would be considered confidential in nature ("**Confidential Information**");
- access, use or disclose Confidential Information without authority;
- engage in activities for personal gain or a personal business, or for any commercial or business purposes other than Company purposes;
- perform any scanning or information gathering regarding Company Technology, including the following: port scanning, security scanning, network sniffing, keystroke

logging, or other information gathering techniques, when not part of the User's job function;
- violate any applicable laws;
- send unsolicited email;
- install or use peer-to-peer file-sharing programs or access those types of networks; or
- use Company resources in a manner that violates applicable laws, including without limitation, those laws relating to discrimination and harassment, privacy, financial disclosure, intellectual property and proprietary information, defamation and criminal laws.

Users shall also not be permitted to use the Company Technology to view, access, amend, update, change, collect, use or disclose: (i) any personal information in the Company's possession or control; or (ii) any Confidential Information without proper authorization.

Users should report any suspected unacceptable use of Company Technology to their manager.

Any User who uses Company Technology for any of these unacceptable uses will be subject to discipline in accordance with this Policy.

4. MONITORING

The Company maintains ownership over all Company Technology and all data created, sent, received or stored on or using Company Technology. Users should have no expectation of privacy with respect to their use of Company Technology.

Subject to compliance with applicable laws, the Company reserves the right to and may from time to time inspect, access, audit, monitor and/or record Users' use of and access to Company Technology and any information accessed, created, modified, stored, sent, received, copied, manipulated or otherwise handled in any way, by or through any Company Technology, at any time, in its sole discretion, without notice to any User.

These actions will be performed only as reasonably necessary to ensure compliance with this Policy and other Company policies, to detect and prevent loss or theft of Confidential Information, personal information or other misconduct, to conduct investigations into suspected inappropriate or unlawful activity, to meet legal disclosure and document production requirements, and other compliance requirements.

5. SECURITY AND CONFIDENTIALITY

The Company reserves the right to implement controls in respect of Company Technology at any time in its sole discretion where it is deemed necessary to protect the security of the Company Technology, Confidential Information, personal information or other assets. Users may not block, uninstall or otherwise interfere with such controls.

Users must maintain basic controls to prevent Company Technology assets being lost or stolen, potential security breaches, leaking of Confidential Information or personal information and breaches of software licensing agreements.

Users must maintain confidentiality and exclusive control of authentication credentials (passwords, tokens, certificates) used to access the Company Technology. Credentials must not be shared with others at any time or left in a place where an unauthorized person might find them. If a User has reason to believe that his/her password has been compromised or discovered by another person, the User must immediately inform his/her manager (if an employee) or [IT?] if any other type of User, and change his/her password immediately. Other basic controls include, but are not limited to:

- Ensuring that laptops, mobile devices and desktop computers are protected by lock screen passwords of at least 8 characters in length and that screens are set to lock within 10 minutes of inactivity;
- changing passwords not less than every 30 days. The same password cannot be used more than once every 24 passwords;
- keeping laptops, mobile devices and portable storage devices and media appropriately secured (e.g. not leaving these items unattended in a vehicle or public place);
- preventing unauthorized changes being made to the operating system software or configuration of personal computers or mobile devices used to access Company Technology; and
- not sharing mobile devices used to access Company Technology, or portable media containing Confidential Information or assets, with third parties (including family members);

Users must exercise caution when opening attachments or selecting links (these can be contained in electronic messages, blogs or social networks) from unknown sources as these may contain malicious software (also known as malware, examples include viruses, worms and trojans).

The Company reserves the right to revoke access to or use of any or all Company Technology any time in its sole discretion. Access to Company Technology will be revoked when a User leaves the Company.

All Company Technology resources must be returned to the Company at the end of a User's employment, or at any time Company deems it necessary.

6. BREACHES, INVESTIGATIONS AND DISCIPLINE

All Users must comply with this Policy at all times and take care to ensure that their use of Company Technology does not jeopardize the interests of the Company, personal information in its custody or control, or its Confidential Information.

Users must immediately notify the Company of any suspected breach of this Policy. The Company will investigate any reasonably suspected breach of this Policy promptly and impartially.

In the course of an investigation, the Company may require a written statement from the User involved in or with knowledge of the suspected breach, as well as an interview of any person with knowledge of the incident, and collect any and all relevant and material documents and other evidence. The Company may involve investigators and experts where appropriate to investigate and report to the Company.

A User may, in the Company's sole discretion, be suspended while an investigation is undertaken and completed.

Confidentiality will be maintained through the investigation process to the extent practicable and appropriate in the circumstances. Information obtained in connection with this Policy, including identifying information about any individuals involved, will not be disclosed unless the disclosure is necessary for the purposes of investigating or taking corrective action with respect to the incident, or as otherwise required by law. However, the Company may disclose certain information to the affected parties to gather pertinent facts or answer allegations.

All Users are expected to cooperate fully in any investigation pursuant to this Policy. If, after investigation, the Company finds that a violation of this Policy has occurred, the Company will determine what remedial action should be taken to avoid future incidents and to ensure compliance with this Policy in the future. Any such remedial action will be undertaken in accordance with this Policy.

Any and all breaches of this Policy will be treated with the utmost seriousness by the Company. Any breach of this Policy will result in discipline, up to and including termination of employment for just cause.

7. ADMINISTRATION

This Policy shall be administered in accordance with all applicable federal, provincial and local laws and regulations.

The Company may amend this Policy from time to time, at its sole discretion. Users are responsible for regularly reviewing this Policy.

8. QUESTIONS

Any questions regarding this Policy should be directed to a supervisor/[title of appropriate manager].

Acknowledgement and Agreement

I, _____, hereby acknowledge that I have received, read and understand the Company's Acceptable Use Policy and agree to comply with its terms. I understand that a violation of this Policy may subject me to discipline, up to and including termination of my employment for just cause.

Name: _____

Signature: _____

Date: _____