DGSI INFORMATION TECHNOLOGY

POLICY ON ACCEPTABLE USE OF COMPUTER RESOURCES

I. INTRODUCTION

DGSI's computer resources are dedicated to the support of the DGSI mission statement "To create business excellence and enrich the lives of people". In furtherance of this mission statement, the DGSI Information Technology department respects, upholds and endeavors to safeguard the principles of client confidentiality, employee privacy, and complete data security.

The DGSI Information Technology department recognizes there is a concern among all participants and consumers of our computer resources that because information created, used, transmitted or stored in electronic form is by its nature susceptible to disclosure, invasion, loss, and similar risks, that electronic communications and transactions will be particularly vulnerable to infringements of our mission statement.

Whenever possible, the DGSI Information Technology department will provide access to, and protect DGSI intellectual properties and electronic information. However, the use of DGSI computer resources, which includes use for professional and personal purposes, are subject to the requirements of legal and ethical behavior.

This policy is intended to provide guidelines for the access and use of internal and external IT resources securely, while recognizing the company responsibilities and limitations associated with such exchange.

II. APPLICABILITY

This policy applies to all users of DGSI computer resources, as defined in Article III below.

III. DEFINITIONS

1. "DGSI Computer Resources" refers to all computer and information technology hardware, software, data, access and other resources owned, operated, or contracted by DGSI. This includes, but is not limited to, desktop and laptop computers, handheld devices that allow or are capable of storing and transmitting information (e.g., cell phones, tablets), mainframes, minicomputers, servers, network facilities, databases, memory, memory sticks, and associated peripherals and software, and the applications they support, such as e-mail, cloud computing applications, and access to the internet.

2. "E-mail" includes point-to-point messages, postings to newsgroups, social media, and other electronic messages involving computers and computer networks.

3. "PIPEDA" is the Canadian Personal Information Protection and Electronic Documents Act.

4. "Non-Public DGSI Information" has the meaning set forth in DGSI's IT Security Policies and Procedures found at http://security.dgsi.ca, namely: personally identifiable information such as an individual's Social Insurance Number; driver's license number or non-driver identification card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; personal electronic mail address; Internet identification name or password; parent's surname prior to marriage; other information relating to the administrative or business activities and operations of the company (including employee evaluations, employee home addresses and telephone numbers, and other employee records that should be treated confidentially); and any other information available in DGSI files and systems that by its nature should be treated confidentially .

5. "User" means a user of DGSI computer resources, including all current and former users, whether affiliated with DGSI or not, and whether accessing those resources internally within DGSI or remotely from another computer.

IV. RULES FOR USE OF DGSI COMPUTER RESOURCES

1. Authorization.

a. Users may not access a DGSI computer resource without authorization or use it for purposes beyond the scope of authorization. This includes attempting to circumvent DGSI computer resource system protection facilities by hacking, cracking or similar activities, accessing or using another person's computer account, and allowing another person to access or use the User's account.

b. Notwithstanding subsection 1.a. above, a user may authorize a colleague or clerical assistant to access information under the user's account on the user's behalf while away from a DGSI or when the user is unable to efficiently access the information on the user's own behalf (including as a result of a disability), but delegated access will be subject to the rules of Section 10 – Security, below.

c. DGSI computer resources may not be used to gain unauthorized access to another computer system within or outside of DGSI. users are responsible for all actions performed from their computer account that they permitted or failed to prevent by following ordinary security precautions. DGSI security advisories and resources are available at http://security.dgsi.ca/securityadvisories

2. Purpose.

a. Use of DGSI computer resources is generally limited to activities relating to the performance by DGSI employees of their duties and responsibilities. For example, use of DGSI computer resources for private commercial or not-for-profit business purposes, for private advertising of products or services, or for any activity meant solely to foster personal gain, is prohibited. Similarly, use of DGSI computer resources for partisan political activity is also prohibited.

b. Except with respect to DGSI employees, where a supervisor has prohibited it in writing, incidental personal use of DGSI computer resources is permitted so long as such use does not interfere with DGSI operations, does not compromise the functioning of DGSI computer resources, does not interfere with the User's employment or other obligations to DGSI, and is otherwise in compliance with this policy, including subsection 2.a. above. Users should be aware that personal messages, data and other information sent or received through a user's DGSI account or otherwise residing in a DGSI computer resource are the property of DGSI and are subject to DGSI review pursuant to Section 13 of this policy and may also be subject to public disclosure in accordance with Canadian PIPEDA law and provincial PIPA law.

3. Compliance with Law.

a. DGSI computer resources may not be used for any purpose or in any manner that violates DGSI rules, regulations or policies, or federal, provincial or local law. Users who engage in electronic communications with persons in other provinces, states or countries or on other systems or networks may also be subject to the laws of those other states and countries, and the rules and policies of those other systems and networks. users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular use.

b. Examples of applicable federal and provincial laws include those addressing defamation, invasion of privacy, obscenity and child pornography, and online gambling, as well as the following can be found using the following online links:

Criminal Code (R.S.C., 1985, c. C-46) Unauthorized use of a computer
Canadian Personal Information Protection and Electronic Documents Act
Canadian Privacy Act
Alberta Personal Information Protection Act
Pornography and Obscenity

4. Licenses and Intellectual Property.

a. Users may use only legally obtained, licensed data or software and must comply with applicable licenses or other contracts, as well as copyright, trademark and other intellectual property laws.

b. Much of what appears on the internet and/or is distributed via electronic communication is protected by copyright law, regardless of whether the copyright is expressly noted. Users should generally assume that material is copyrighted unless they know otherwise, and not copy, download or distribute copyrighted material without permission unless the use does not exceed fair use as defined by the Canadian Federal Copyright Act of 1985 (C-42). Protected material may include, among other things, text, photographs, audio, video, graphic illustrations, and computer software.

5. False Identity and Harassment. Users may not employ a false identity, mask the identity of an account or computer, or use DGSI computer resources to engage in abuse of others, such as sending harassing, obscene, threatening, abusive, deceptive, or anonymous messages within or outside DGSI.

6. Confidentiality.

a. Users may not invade the privacy of others by, among other things, viewing, copying, redistributing, posting such data to the internet, modifying or destroying data or programs belonging to or containing personal or confidential information about others, without explicit permission to do so.

b. DGSI employees must take precautions by following all IT Security Policies and Procedures to protect the confidentiality of Non-Public DGSI Information encountered in the performance of their duties or otherwise. For a description of non-public information, please refer to section III.(4).

7. Integrity of computer resources. Users may not install, use or develop programs intended to infiltrate or damage a DGSI computer resource, or which could reasonably be expected to cause, directly or indirectly, excessive strain or theft of confidential data on any computing facility. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms. users should consult with the IT department before installing any programs on DGSI computer resources that they are not sure are safe or may cause excess strain.

8. Disruptive Activities.

a. DGSI computer resources must not be used in a manner that could reasonably be expected to cause or does cause, directly or indirectly, unwarranted or unsolicited interference with the activity of other users, including:

i. chain letters, virus hoaxes or other e-mail transmissions that potentially disrupt normal e-mail service;

ii. spamming, junk mail or other unsolicited mail that is not related to DGSI business and is sent without a reasonable expectation that the recipient would welcome receiving it;

iii. the inclusion on e-mail lists of individuals who have not requested membership on the lists, other than the inclusion of members of the DGSI community on lists related to DGSI business; and

iv. downloading of large videos, films or similar media files for personal use.

b. DGSI has the right to require users to limit or refrain from other specific uses if, in the opinion of the IT Director, such use interferes with efficient operations of the system, subject to appeal to a CEO or the CFO

9. DGSI Names and Trademarks.

a. DGSI names, trademarks and logos belong to the company and are protected by law. Users of DGSI computer resources may not state or imply that they speak on behalf of DGSI or use a DGSI name, trademark or logo without authorization to do so. Affiliation with DGSI does not, by itself, imply authorization to speak on behalf of DGSI.

b. Notwithstanding subsection 9.a. above, DGSI employees may indicate their DGSI affiliation on e-mail, LinkedIn, other correspondence, publications or professional appearances, so long as they do not state or imply that they are speaking on behalf of DGSI.

10. Security.

a. DGSI employs various measures to protect the security of its computer resources and of users' accounts. However, DGSI cannot guarantee such security. Users are responsible for engaging in safe computing practices such as guarding and not sharing their passwords, changing passwords regularly, logging out of systems at the end of use, and protecting non-public information, as well as for following DGSI's IT Security Policies and Procedures.

b. Users must report incidents or suspected incidents of non-compliance with DGSI IT Security Policies and Procedures or other security incidents to the Director of IT immediately after discovery.

11. Filtering. DGSI reserves the right to install spam, anti-malware, and spyware filters and similar devices if necessary in the judgment of DGSI's Director of IT to protect the security and integrity of DGSI computer resources. DGSI will not install filters that restrict access to e-mail, instant messaging, chat rooms or websites based solely on content, unless such content is illegal or not approved by the IT department.

12. Confidential Information. Employees who use DGSI computer resources to collect, examine, analyze, transmit or store information that is required by law or regulation to be held confidential or for which a promise of confidentiality has been given are responsible for taking steps to protect such confidential research information from unauthorized access or modification. In general, this means storing the information on a computer or auxiliary hard drive that provides strong access controls (passwords) and encrypting files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks. Robust encryption and passwords must be used to protect non-public information, and is strongly recommended for information stored electronically on all computers, especially portable devices such as notebook computers, Personal Digital Assistants (PDAs), and portable data storage (e.g., auxiliary hard drives, memory sticks) that are vulnerable to theft or loss, as well as for information transmitted over public networks. Software and protocols used should be reviewed and approved by DGSI's Information Technology Department.

13. DGSI Access to computer resources.

a. Copying. DGSI may copy a User's account and/or hard drive on a DGSI computer resource, without monitoring or inspecting the contents of such account and/or hard drive, at any time for preservation of data or evidence, without notice to the user.

b. General Monitoring Practices. DGSI does not routinely monitor, inspect, or disclose individual usage of DGSI computer resources without the user's consent. In most instances, if the company needs information located in a DGSI computer resource, it will simply request it from the author or custodian. However, DGSI IT professionals and staff do regularly monitor general usage patterns as part of normal system operations and maintenance and might, in connection with these duties, observe the contents of web sites, e-mail or other electronic communications. Except as provided in this policy or by law, these individuals are not permitted to seek out contents or transactional information, or disclose or otherwise use what they have observed. Nevertheless, because of the inherent vulnerability of computer technology to unauthorized intrusions, users have no guarantee of privacy during any use of DGSI computer resources or in any data in them, whether or not a password or other entry identification or encryption is used. users may expect that the privacy of their electronic communications and of any materials stored in any DGSI computer resource dedicated to their use will not be intruded upon by DGSI except as outlined in this policy.

c. Monitoring without Notice.

i. Categories. DGSI may specifically monitor or inspect the activity and accounts of individual users of DGSI computer resources, including individual login sessions, e-mail and other communications, without notice, in the following circumstances:

A. when the user has voluntarily made them accessible to the public, as by posting to social media or a web page;

B. when it is reasonably necessary to do so to protect the integrity, security, or functionality of DGSI or other computer resources, as determined by the Director of IT, after consultation with DGSI's CEO's or CFO.

C. when it is reasonably necessary to diagnose and resolve technical problems involving system hardware, software, or communications, as determined by the Director of IT after consultation with DGSI's CEO's or CFO.

D. when it is reasonably necessary to determine whether DGSI may be vulnerable to liability, or when failure to act might result in significant bodily harm, significant property loss or damage, or loss of evidence, as determined by the Director of IT after consultation with DGSI's CEO's or CFO.

E. when there is a reasonable basis to believe that DGSI policy or federal, provincial or local law has been or is being violated, as determined by the Director of IT after consultation with DGSI's CEO's or CFO.

F. when an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns, as determined by the Director of IT after consultation with DGSI's CEO's or CFO.

G. as otherwise required by law.

ii. Other Disclosure.

A. DGSI, in its discretion, may disclose the results of any general or individual monitoring or inspection to appropriate DGSI personnel or agents, or law enforcement or other agencies. The results may be used in disciplinary proceedings, discovery proceedings in legal actions, or otherwise as is necessary to protect the interests of the company.

B. Any disclosures of activity of accounts of individual users to persons or entities outside of DGSI, whether discretionary or required by law, shall be approved by the General Counsel and shall be conducted in accordance with any applicable law. Except where specifically forbidden by law, DGSI employees subject to such disclosures shall be informed promptly after the disclosure of the actions taken and the reasons for them.

14. Waiver of Policy

a. A DGSI employee may apply to the Director of IT, a CEO for the CFO for an exception or waiver from one or more of the provisions of this policy. Such application may be for a single use or for periodic or continuous uses, such as in connection with regular business use and requirements. Any application for a waiver should be made prior to using the DGSI computer resource for the purposes described in the application.

b. The written waiver application must state:

i. the policy provision or provisions for which the user is seeking a waiver;

ii. how the user plans to use DGSI computer resource to be covered by the waiver and the reasons why the user believes a waiver should be approved;

iii. if the waiver involves confidential research information, what steps will be taken to protect such information;

iv. the length of time for which the waiver is being requested.

c. Users should be aware that DGSI cannot waive federal, provincial or local law; for example, the contents of DGSI computer resources (including confidential information) may be subject to a valid subpoena regardless of the terms of any waiver.

15. Enforcement.

a. Violation of this policy may result in suspension or termination of an individual's right of access to DGSI computer resources, disciplinary action by appropriate DGSI management, referral to law enforcement authorities for criminal prosecution, or other legal action, including action to recover civil damages and penalties.

b. Violations will normally be handled through company disciplinary procedures applicable to the relevant user. For example, alleged violations by employees will normally be investigated, and any penalties or other discipline will normally be imposed, by management

c. DGSI has the right to temporarily suspend computer use privileges and to remove from DGSI computer resources material it believes violates this policy, pending the outcome of an investigation of misuse or finding of violation.

16. Additional Rules. Additional rules, policies, guidelines and/or restrictions may be in effect for specific computers, systems, or networks. Any such rules which potentially limit the privacy or confidentiality of electronic communications or information contained in or delivered by or over DGSI computer resources will be subject to the substantive and procedural safeguards provided by this policy.

17. Disclaimer.

a. DGSI shall not be responsible for any damages, costs or other liabilities of any nature whatsoever with regard to the use of DGSI computer resources. This includes, but is not limited to, damages caused by unauthorized access to DGSI computer resources, data loss, or other damages resulting from delays, non-

deliveries, or service interruptions, whether or not resulting from circumstances under the DGSI's control.

b. Users receive and use information obtained through DGSI computer resources at their own risk. DGSI makes no warranties (expressed or implied) with respect to the use of DGSI computer resources. DGSI accepts no responsibility for the content of web pages or graphics that are linked from DGSI web pages, for any advice or information received by a user through use of DGSI computer resources, or for any costs or charges incurred by a user as a result of seeking or accepting such advice or information.

c. DGSI reserves the right to change this policy and other related policies at any time. DGSI reserves any rights and remedies that it may have under any applicable law, rule or regulation. Nothing contained in this policy will in any way act as a waiver of such rights and remedies.

I have read, understand, and agree to abide by the terms of the above described **DGSI Acceptable Use of Computer Resources Policy** regarding access to electronic information, services, and networks. Should I commit any violation or in any way misuse my access to the DGSI computer network and/or the Internet, I understand and agree that my access privilege may result in suspension or termination of my right of access to DGSI computer resources and not limited to further disciplinary action as deemed appropriate by DGSI management.

User's Name (Print): _____

User's Signature: _____ Date: _____