DGSI INFORMATION TECHNOLOGY

Security & Privacy Policy and Procedures

I. General

1. Introduction – Each DGSI Branch and all users with access to DGSI information available in electronic files and systems, whether in computerized or printed form, are continually responsible for maintaining the integrity, accuracy, and privacy of this information. Loss of data integrity, theft of data, and unauthorized or inadvertent disclosure could lead to a significant exposure of the company and its constituents as well as those directly responsible for the loss, theft, or disclosure. Non-compliance with provincial or federal laws could lead to direct financial loss to DGSI. Users are directed by these Information Technology Security Procedures ("IT Security Procedures"), which cover all DGSI networks and systems.

Any proposed exception to these IT Security Procedures must be communicated in writing and approved by the Director of IT prior to any action introducing a non-compliance situation.

2. Non-Public DGSI Information – For the purpose of these IT Security Procedures, the term "Non-Public DGSI Information" means personally identifiable information (such as an individual's Social Insurance Number; driver's license number or non-driver identification card number; bank 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; and parent's surname prior to marriage); other information relating to the administrative and business activities and operations of DGSI (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.

II. Access

1. Access to DGSI Information

(a) General. Access to DGSI information available in electronic files and systems, whether in electronic or hard copy form, must be limited to individuals with a strict need to know, consistent with the individual's job responsibilities.

(b) Employees Permitted Access to Non-Public DGSI Information. Except as provided elsewhere in this section 3, access to Non-Public DGSI Information must be restricted to full-time and regular part-time employees of the DGSI and its related entities, and employees of DGSI's contractors who have been permitted such access under a written agreement with company.

(c) Employees Requiring Waiver. Employees of DGSI or its related entities who are not full-time and regular part-time employees (e.g., individuals hired as part of a temporary staff augmentation or in connection with an individual project), or employees of DGSI's contractors who have been permitted access to Non-Public DGSI Information under a written agreement with DGSI may not be permitted any such access, except pursuant to the waiver procedure set forth in section 3(d) below.

(d) Waiver Procedure. An individual who is not permitted access to Non- Public DGSI Information under sections 3(c) and (d) above may be permitted such access on a strict need to know basis, consistent with the individual's job responsibilities, but only if a waiver is granted by 2 or more of the following: the CEO's, CFO or Director of IT. Any waiver granted will be limited to a specific period of time, which may not exceed one year. In order to extend the waiver after expiration, this waiver procedure must be repeated. The written waiver request must state:

- the specific status of the individual as an employee of DGSI or one of its related entities or contractors
- the type and form of access that is being requested,
- the length of time for which access is being requested,
- the reasons for permitting such access, and
- how and by whom the individual will be supervised.

The Director of IT will be responsible for maintaining all documentation of any waiver request and disposition.

(e) Acknowledgment of DGSI Policy. All employees described in section 3(b) above and all employees granted a waiver under section 3(d) above must acknowledge, by signature, receiving a copy of DGSI's Policy on Acceptable Use of Computer Resources (available at http://security.dgsi.ca) and these IT Security Procedures.

2. Review of Access to DGSI Files and Systems – At least twice during each calendar year, and no less than 5 months apart, the Director of IT must review individuals having any type of access to DGSI files and systems and direct the removal of IDs and access capabilities that are no longer current. This review includes, but is not limited to, access to DGSI networks, applications, sensitive transactions, databases, and specialized data access utilities.

An attestation letter of such review must be completed by the Director of IT and submitted to the CFO no later than the date specified in the instructions for completing the attestation letter. Documentation showing the review steps taken in arriving at the attestation must be retained in IT Departmental files and be made available for further by DGSI Executive and internal/external audit entities as appropriate.

3. Severance of Access upon Termination or Transfer of Employment – Access to DGSI files and systems must be removed no later than an individual's last date of employment. User IDs must not be re-used or re-assigned to another individual at any time in the future.

For job transfers, access to DGSI files and systems access must be removed no later than the individual's last date in the old position and established no sooner than his or her first date in the new position.

In special circumstances where underlying information attributed to a user ID must be retained and made accessible from duplicate systems or business units, approval must be obtained from both management leaders of the business units. Such arrangements, if approved, will be for a fixed duration of time, determined on a case-by-case basis.

4. Authentication – Users of DGSI files and systems must use an individually assigned user ID to gain access to any DGSI network or application.

5. User IDs – Users of DGSI files and systems other than technical employees within Information Technology departments must have no more than one individually assigned user ID per system. The user ID must be in a format consistent with DGSI naming standards, clearly identifiable to a user, and not shared.

Generic-named user IDs used in background/batch processes or multiple user IDs required to maintain, support, and operate systems by technical employees within Information Technology departments will be allowed under limited circumstances, provided that use of such identities is auditable, and individual user accountability is assigned to each of these identities, oversight is administered by management or supervisor of the user assigned to the account, and use of these accounts is specifically approved by the Director of IT.

The DGSI Information Technology department must maintain an accurate record of the person to whom each user ID has been assigned, including name, title, level of access, office, department, and phone number.

6. Passwords – Passwords and private encryption keys must be treated as Non-Public DGSI Information and, as such, are not to be shared with anyone. A password must be entered by the user each time he or she authenticates to a DGSI system. Use of auto-complete features to expedite or script user logins (e.g., "Windows Remember My Passwords?") is prohibited.

All passwords must be changed at least every 90 days. Accounts which have privileged access must be changed at least every 30 days. Privileged access accounts are identities with elevated authority across multiple user accounts and/or system-wide permission rights, typically named *root*, *administrator*, *admin* or *supervisor*. This also includes any accounts with domain admin or administrator group access. Passwords should not be based on personal information (e.g., family names, pets, hobbies, and friends) and should be difficult to guess. Passwords should be at least eight characters in length, Have 1 uppercase. Privileged accounts must additionally have 1 special character.

7. Remote Access – Access to administrative and IT support systems from non-DGSI locations is allowed only through secure remote connections (e.g., VPN) that provide for unique user authentication and encrypted communications. The Director of IT must approve in writing all requests for remote access capability. Requests for remote access can be found at http://security.dgsi.ca/DGSI_VPN_Request_Form.pdf

III. Disclosure Issues

8. Disclosure of Non-Public DGSI Information

(a) General Rule. Unless otherwise required by law, users of DGSI files and systems must not disclose any Non-Public DGSI Information (as defined in section 2 above) to the general public or any unauthorized users.

(b) Definition of Social Insurance Numbers. For the purpose of these IT Security Procedures, the term "Social Insurance Number" means the nine-digit account number issued by the Canadian Government and any number derived therefrom. It does not include any number that has been encrypted.

(c) Special Rules for Social Insurance Numbers. Unless required by law, users of DGSI files and systems must not:

(i) Intentionally communicate to the general public or otherwise make available to the general public in any manner an individual's Social Insurance Number.

(ii) Publicly post or display an individual's Social Insurance Number or place a Social Insurance Number in files with unrestricted access.

(iii) Print an individual's Social Insurance Number on any card or tag required

for the individual to access products, services, or benefits provided by the DGSI.

(iv) Print an individual's Social Insurance Number on any identification badge or card, including any time card.

(v) Require an individual to transmit his or her Social Insurance Number over the Internet, unless the connection is secure or the Social Insurance Number is encrypted.

(vi) Require an individual to use his or her Social Insurance Number to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the Internet website.

(vii) Include an individual's Social Insurance Number, except the last four digits thereof, on any materials that are mailed to the individual, or in any electronic mail that is copied to third parties, unless state or federal law requires the Social Insurance Number to be on the document to be mailed. Notwithstanding this paragraph (vii), Social Insurance Numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend, or terminate an account, contract, or policy, or to confirm the accuracy of the Social Insurance Number. A Social Insurance Number that is permitted to be mailed under this paragraph (vii) may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.

(viii) Encode or embed a Social Insurance Number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the Social Insurance Number as required by this section 12.

(ix) Transmit an individual's Social Insurance Number onto portable devices without encryption as specified in section 11 below.

These special rules do not prevent the collection, use, or release of a Social Insurance Number as required by provincial or federal law, or the use of a Social Insurance Number for internal verification, fraud investigation, or administrative purposes.

9. Web Accessible Data – Because Non-Public DGSI Information must not be made accessible to the general public, all DGSI web pages must be programmed with a parameter to prevent the caching of Non-Public DGSI Information by Internet search engines. Directory/folder listings of files through a web page must be disabled. Secure and encrypted data transfer protocols must be used when uploading data to a web site.

10. Security Incident Response and Reporting

(a) Acknowledgment and Reporting of Security Related Incidents. The Director of IT within 24 hours of receipt acknowledge or respond in writing to any initial security incident report issued by the DGSI Executive or any other management member. The Director of IT must make a full written report of such incident to the DGSI Executive, including root cause identification, explanation of the remediation plan, and extent of data loss, within 72 hours of the DGSI's receipt of the initial Security incident report.

(b) DGSI Breach Reporting Procedure. The DGSI Breach Reporting Procedure (available at http://security.dgsi.ca) must be followed whenever a security breach or reportable incident occurs involving the unauthorized disclosure of any of the following Non-Public DGSI Information without encryption:

(i) Social Insurance Number;

(ii) driver's license number or non-driver identification card number; or

(iii) 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.

(c) Limiting Disclosure. When any Non-Public DGSI Information has been disclosed without valid authorization and encryption, all reasonable efforts must be taken to eliminate further disclosure, including immediate disconnection of any computer device involved from the DGSI network.

11. Portable Devices/Encryption – The Non-Public DGSI Information listed in section I (2) above must not be stored, transported, or taken home on portable devices (e.g., laptops, flash drives) of any type without specific approval of both the Director of IT and the business unit leader. Where approval is granted, additional password protection and encryption of data are required, and will be treated as a privileged network account. In addition, the Non-Public DGSI Information listed in section I (2) above stored on non-portable devices or transmitted between devices (e.g., servers, workstations) must be encrypted. DGSI has made encryption tools available to staff to comply with the requirements of this procedure.

12. Safeguarding and Disposal of Devices and Records Containing Non-Public DGSI Information – Whenever records containing Non-Public DGSI Information are subject to destruction through customer or client agreements, the storage devices such as hard disk drives and other media (e.g. tape, diskette, CDs, DVDs, cell phones, digital copiers, or other devices) and hard copy documents that contain such information must be securely overwritten or physically destroyed in a manner that prevents unauthorized disclosure. While in use, such devices and documents must not be left open or unattended on desks or elsewhere for extended periods of time.

IV. Maintenance of Data and Systems

13. Change of Data in Records

(a) Authorization of Changes. When updates are not part of normal business processing, individuals within Information Technology departments who have access to DGSI information to support ongoing operations of administrative files and systems must not alter any such information unless given specific approval by the CFO, Director of Accounting or relevant business unit leader. A record of any data change, including evidence of approval, must be retained in DGSI Information Technology records.

(b) No Changes from Non-Compliant Endpoints. Change to official DGSI data of record by DGSI employees (i.e., faculty and staff) must only be performed from endpoints that are in compliance with section 15, "Device Management." Due to the increased risk of the presence of insidious malware that captures and/or interferes with the integrity of entered data, such changes may not be made from publicly accessible computers, Internet "cafés" and similar uncontrolled environments.

14. Vulnerability Assessments – DGSI must establish a routine program to test, monitor, and remediate technical and data vulnerabilities on its network. The program should include a combination of continuous monitoring and on-demand testing tools. Monitoring and testing should report on operating system configuration, software patch level vulnerabilities, and unprotected data. The DGSI Information Technology Department may initiate vulnerability testing at its discretion. Regular reporting of test results must be made available to the DGSI Executive.

15. Device Management – All devices that are allowed to connect to DGSI networks and systems that support administrative, business activities and operations must be maintained at current anti-virus/malicious code protection at all times. In addition, updates to operating systems must be applied on a timely basis after appropriate testing. Although DGSI does not support employee home systems, procedures should be implemented to minimize the risk to DGSI files and systems.

16. Management Responsibility –The Information Technology Group is responsible for maintaining compliance with these IT Security Procedures within their line responsibilities. Oversight and administration of the IT Security Policy shall be the responsibility of the Director of IT.

17. Information Technology Security Procedure Governance – The information Technology department will proactively and continually identify and establish procedures and other areas of change that may be instituted to further protect the integrity of DGSI files and systems. Total governance over these policies will be provided by the DGSI IT Steering Committee.

Additional and/or revised procedural statements may be adopted from time to time and introduced for DGSI compliance. Further procedural documents may be developed to elaborate detail on these IT Security Procedures, but they will in no way detract or suggest a different level of compliance that is expected or required.

Non-compliance with these IT Security Procedures may result in termination of access to DGSI network and applications until such time that compliance is re-established. Non-compliance may also result in disciplinary action.