DGSI INFORMATION TECHNOLOGY

DGSI NON-PUBLIC INFORMATION BREACH REPORTING PROCEDURES

PURPOSE

The purpose of this protocol is to outline the steps that must be followed once a possible breach of Non-Public DGSI Information (personal privacy) is identified.

Non-Public DGSI Information – For the purpose of this Breach of Private Information Procedure, 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.

PROCEDURE

When a possible privacy breach has occurred, immediate action should be taken. The following procedure will assist in controlling the situation and ensuring that, if a breach of privacy occurs, steps will be taken to minimize the risks of a similar breach from happening again.

Step 1) Confirm and Contain. Confirm the validity of the suspected information breach. If the breach can be reasonably ascertained, containment should occur immediately. Containment includes, but is not limited to, disconnection of the host (e.g., server or other device) from the network or shutting down an application. Care should be taken not to destroy data, but to preserve it without any form of network connection. Re- connection of the device to the network is not allowed until such time as remedial steps have been completed and re-connection is specifically approved by the Director of IT.

Step 2) Report. The following individuals are required to be informed as soon as possible:

a) The Director of IT
b) All members of the DGSI Executive

The report should indicate whose personal information was disclosed, to whom it was disclosed, when it was disclosed, how it was disclosed/accessed, and what steps have been taken in response to the disclosure.

Step 3(a) Retrieve. Any documents or contents of electronic documents that have been disclosed to, or taken by, an unauthorized recipient should immediately be retrieved and/or secured (electronic documents or paper documents in facsimile form or printed e- mail messages) or taken offline. Documents, in any form, should not be destroyed until specific instruction is received. This may require personal attention to secure the documents and return them to their original location, remove them permanently from electronic storage, or send them to the intended authorized recipient.

Step 3b) Remove. Private information taken offline (Step 1 and Step 3a) may still be accessible and discoverable on the Internet via Internet Search engines (e.g., Google). The usual time periods for information to be removed by the search engines through routine web crawling techniques is too elongated (e.g., weeks) and requests must be made to remove the information from search engine indexes and cache directly to the Internet Search engines companies. These requests must be made as quickly as possible.

Step 4) Notify. In cases where the breach results in the disclosure of personal information, provincial law may require that DGSI notify the individuals affected.

Determination of the reporting requirements will be made by DGSI General Counsel and with the DGSI Legal Affairs Designee on a case-by-case basis. All notification letters must be reviewed by General Counsel prior to being sent.

Step 5) Investigate. DGSI's General Council, CEO's, CFO, Vice-President Human Resources, and the Director of IT will investigate the details of any breach, for the purpose of determining and recording all the relevant facts concerning the breach and making recommendations. The objectives of this investigation should include: a review of the circumstances surrounding the event as well as the adequacy of existing policies and procedures in protecting personal private information.

Step 6) Management Review. The Director of IT, CFO, Vice-President Human Resources, and the CEO of the affected area will document and report the detail of the breach of privacy and remedial steps. DGSI Council in collaboration with the Director of IT will report on recommendations and actions to the appropriate parties within the executive group. Additional incident reporting will occur by the Director of IT to comply with internal incident reporting policies.

CONCLUSION

In June, 2015, the Digital Privacy Act amended Canada's foundational Personal Information Protection and Electronic Documents Act (PIPEDA) to state that organizations will be required to notify the Privacy Commissioner and affected individuals of "any breach of security safeguards involving personal information under the organization's control, if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual." The Digital Privacy Act provides for fines up to $100,000 for knowing violations of the breach notification requirements, and the requirement that organizations keep and maintain a record of every breach of security safeguards involving personal information under the organization's control.

A breach of private information is a serious matter. DGSI Executive and all staff must make every reasonable effort to prevent breaches from occurring. If one does occur, staff MUST ensure that compliance with this procedure is followed.