Office of the Chief Information Officer Directive: IT 5.07	Published: 02/2020
Chapter: Data Management	Last Review: 02/2024
Subject: **Anti-Spam Requirements**	

1 DIRECTIVE

1.01 GNB Information Security Policy will comply with Canada's anti-spam legislation (commonly known as "CASL").

1.02 The Senior Leaders shall ensure that the organization's policies, procedures, practices, and databases are established and compliant with CASL.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that GNB Information Security Policy complies with CASL, to avoid regulatory sanctions and lawsuits, and to protect GNB's brand and image, regarding the following activities:

1. Sending Commercial Electronic Messages (CEMs).
2. **Altering transmission** data so that it is delivered to a different destination than the one intended by the sender.
3. **Installing computer programs (i.e.**, **software)** on others' computer systems.
4. **Address harvesting** (i.e. collecting electronic addresses using specifically designed software, or using electronic addresses collected in this manner).

3 SCOPE

3.01 This directive applies to all employees, independent contractors, external service providers and business affiliates (i.e., personnel) who carry out any of the four activities above, for or on behalf of the organization.

3.02 This directive applies to activities with a Canadian nexus, which means that a computer system located in Canada is used to send or access the CEM; or send, route or access the electronically transmitted data that has been altered. For software installations, at the time of contravention, the computer system must be in Canada, or, the installers or the persons directing the installation must be in Canada when they give the directions. This means that CASL applies to international business affiliates acting on the organization's behalf in Canada or interacting with the organization's Canadian customers.

3.03 This directive also applies to persons indirectly responsible for violations of CASL. Thus, words like "send," "install," "alter" or similar words used in this directive may apply to those who "cause" the relevant activity to occur.

4 RESPONSIBILITY

4.01 The senior leaders are responsible for monitoring changes in the law and best practices, and periodically updating this directive.

4.02 The senior leaders are responsible for leading or coordinating CASL audits, and investigations regarding violations of, or complaints about, compliance with CASL or this directive.

4.03 The senior leaders and all other department heads are responsible for supervising direct reports and department functions to ensure compliance with CASL and this directive, and for advising the Chief Information Security Officer of violations, complaints or concerns relating to CASL or this directive.

4.04 All personnel are responsible for complying with CASL and this directive. Violations may result in disciplinary action up to and including dismissal.

5 DEFINITIONS

5.01 "**CASL**" (See section 6 below).

5.02 "**CEM**" (**Commercial electronic message**) is an electronic message that encourages participation in a commercial activity.

Electronic messages containing requests for consent to send CEMs are themselves CEMs.

Phone conversations and fax and phone messages are not CEMs, but they may be regulated through the "Do Not Call Registry." Electronic messages for law enforcement, public safety and national or international security purposes are also not CEMs.

5.03 "**Commercial activity**" is any activity of a commercial nature, including activities done without expectation of profit. Examples of commercial activities include offering goods or services for sale, lease or barter, and the promotion of business, gaming or investment opportunities. Law enforcement or public safety-type activities are not commercial activities.

5.04 "**Computer systems**" include computers, laptops, tablets, gaming consoles, smartphones, or other connected devices.

5.05 "**Electronic message**" is any message sent by telecommunications, including: texts or Short Message Service (SMS), emails, instant messages (i.e., IMs, like BlackBerry Messenger [BBM] or WhatsApp) and social media messages.

5.06 "**Transmission data**" is commonly referred to as metadata. Metadata is underlying data that provides information about other data. Metadata is included in electronic messages to facilitate telecommunication functions like signalling, connecting, dialling, routing and addressing, or is generated during telecommunications.

"Phishing" and "Pharming" scams are examples of the unauthorized **alteration of transmission data**. "Phishers" send purportedly legitimate emails, directing recipients to login using a link provided and to complete banking transactions, for example. The link is really to a fraudulent website, where individuals' login and personal information are stolen and used to defraud them. "Pharming" uses technical means to reroute individuals to fraudulent websites, with similar outcomes.

5.07 "**User**" refers to the owner or an authorized user of a computer system. An authorized user is anyone with permission to use the computer system. For example: (i) a corporate employer owns its computer system; its employees, directors or officers are authorized users; and (ii) parents own computer systems; their children are authorized users.

6 RELATED DIRECTIVE(S)

6.01 An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23, and related regulations (i.e., CASL)

OCIO IT 5.02 – Data Backup and Storage
OCIO IT 5.04 – Database Management
OCIO IT 8.04 – Confidentiality and Privacy