1 DIRECTIVE

1.01 **GNB Information Security Policy** will take all reasonable steps to maintain confidentiality of personal information under its control, by developing and implementing policies and procedures to address any **breach of security safeguards (i.e., security breach)**.

2 PURPOSE

2.01 The purpose of this Directive is to outline how GNB will respond in the event of a security breach.

3 SCOPE

3.01 This directive applies to the Board of Directors, all employees, as well as to suppliers and consultants providing goods and services to GNB (i.e., GNB personnel), and it applies whenever there is a proven or suspected security breach.

4 RESPONSIBILITY

4.01 The **Deputy Minister of Treasury Board** and the **Chief Information Officer, along with other Senior Management** shall ensure that management develops, maintains and tests appropriate policies, directives, and procedures to manage security breaches, to ensure compliance with applicable laws and best practices.

4.02 All GNB employees are responsible for complying with established security safeguards. If a necessary security safeguard has not yet been implemented, GNB personnel must choose courses of action that will minimize the likelihood and likely impact of any potential security breach.

4.03 The **Deputy Minister of Treasury Board** shall establish a **Security Breach Response Team (SRT)**, which should be headed by the **Chief Information Security Officer (CISO)** and the **Chief Privacy Officer (CPO)**. The **SRT** must also include appropriate representation from various business units including: Information Technology (IT), Human Resources, Finance, Public Relations and Communications, Risk Management and Legal. External participants may include: external counsel, IT experts, insurance GNB representatives and public relations firms.

4.04 The **Chief Information Security Officer (CISO)** and the **Chief Privacy Officer (CPO)** are responsible for mobilizing and leading security breach protocols, upon learning of an actual or suspected security breach.

4.05 The **SRT** will assist the CISO and CPO in mobilizing the security breach protocols. Where this directive assigns responsibilities to the CISO and CPO, the CISO and CPO may delegate performance to other members of the **SRT**, but will retain accountability for the delegated activities.

5 DEFINITIONS

5.01 "**Breach of security safeguards**" (**i.e., security breach**) is the loss of, unauthorized access to or disclosure of personal information arising from a breach of GNB's security safeguards or from GNB's failure to establish security safeguards.

5.02 "**Personal information**" means information that may be attributable to a specific individual, either directly or indirectly, by reference to an identification number or by one or more factors specific to his or her physical, psychological, economic, cultural or social identity. Personal information includes:

- Name, identification numbers
- Employee files, evaluations, comments, disciplinary actions, income, salary history
- Credit records, loan records, existence of a dispute between a consumer and a merchant
- Medical or health information, blood type
- Ethnic origin, religious or philosophical beliefs, political opinions

Personal information can also include business contact information like work email addresses and work telephone numbers, if used for purposes other than communicating or facilitating communication with individuals in relation to their employment, business or profession.

5.03 "**Real risk of significant harm**" occurs when there is a real risk, or likelihood that significant harm could occur, given the sensitivity, probability of misuse or other prescribed factors associated with the compromised information. The harm to consider includes: bodily harm; humiliation; damage to reputation or relationships; loss of employment, business or professional opportunities; financial loss; identity theft; negative effects on credit records; and damage to or loss of property.

6 RELATED DIRECTIVES

Personal Information Protection and Electronic Documents Act (PIPEDA)
Provincial privacy statutes, where applicable

Digital Privacy Act

OCIO IT 4.02 – Role-based User Management CSD IT 4.03 – Internet Access
OCIO IT 6.02 – Access Administration
OCIO IT 9.03 – Data Access Controls
OCIO IT 8.04 – Confidentiality and Privacy