Office of the Chief Information Officer Directive: IT 9.02	Issued: 02/2020
Chapter: Data Security	Last Review: 01/2022
Subject: **Data Classification**	

1 DIRECTIVE

1.01 Business Owners must classify all their data and document the classification.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that:

(a) All data in the enterprise is reviewed regarding its potential for loss to the enterprise in the event of accidental or intentional disclosure.

(b) No data may be publicly disclosed unless a business owner has explicitly labelled it **Public**.

(c) The enterprise will have legal recourse against any entity having unauthorized possession of any data classified **"Confidential"** or higher.

3 SCOPE

3.01 This policy applies to all employees.

4 RESPONSIBILITY

4.01 Business Owners are responsible to classify their data and to use appropriate GNB standards for handling and best practice decisions associated with the classification.

5 DEFINITIONS

5.01 "**Business owner**" is a senior member within the organization who is accountable for overall management of defined data set for a line of business. The business owner has decision-making authority for who accesses and uses the data and is usually supported by data stewards. They approve processes and policies to uphold data quality and standardize data management processes.

5.02 **Reliability Status (RS)** may be required by an employee working on sensitive government contracts/documents to access confidential information and assets.

5.03 **Personal Security Clearance (PSC)**

Required by an employee working on a sensitive government contract to access information Classified higher than GNB Highly Confidential or Canadian Federal Protected C (this includes federal standards Confidential, Secret, Top Secret). Used to transfer to the Canadian federal government.

5.04 **Cyber Security Classification Levels**

Data classification levels are defined by the level of disclosure control that needs to be applied to data within the enterprise based on the potential for loss or damage to the enterprise in the event of inadvertent or malicious disclosure to the public or to the competition. Different types of classification include:

"**Public**" means the data may be disclosed outside the enterprise. This data may be pre-approved for public disclosure because it is desirable or required to be in the public domain. Examples are annual reports, earning disclosures, news and announcements.

"Internal" data is GNB business related but not Public. Applies to information assets that, if compromised, could cause injury to an individual, organization or government.

Examples: draft reports before publication, draft analysis and statistics, and other GNB documents

"Confidential" data is that must be protected according to legislation, acts, regulation or law. Applies to information assets that, if compromised, could cause serious injury to an individual, organization or government.

Examples are Personal Health information, personnel evaluations and investigations, provincial grade 12 exams, industrial trade secrets, financial records, solicitor-client confidence, 3rd party business information submitted in confidence. Executive Privilege or Advice to Minister may also fall under this classification.

"Highly Confidential ", data is information that, if disclosed outside GNB, could seriously damage the organization, even to the point of failure. If compromised, these information assets could cause extremely grave injury to an individual, organization or government. "Highly Confidential" information may require a security clearance to view.

Examples are critical infrastructure vulnerabilities, criminal records,

police informant documents, criminal investigations "Protected C" information may require a reliability status, or a security clearance, to view.

Cyber Security Classification Table

GNB Classification	Comments	Canadian Federal Standard
Public	Available on GNB websites / open data	Unclassified
Internal	GNB business related but not public	Protected A
Confidential (Legislation, acts, regulation or law)	Personal Health Information, Mental Health information, Advice to Minister, Executive Privilege	Protected B
Highly Confidential (may need security clearance)	Critical infrastructure vulnerabilities, criminal records, witness protection	Protected C

6 RELATED DIRECTIVES

CSD IT 9.01