Office of the Chief Information Officer Directive: IT 9.03	Issued: 02/2020
Chapter: Data Security	Last Review: 01/2022
Subject: **Data Access Controls**	

1 DIRECTIVE

1.01 Access controls must be established for all data classified as **"Confidential"** or higher.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that there are adequate controls over access to data based on the data's classification.

3 SCOPE

3.01 This directive applies to all employees.

4 RESPONSIBILITY

4.01 Business owners are responsible to:

(a) Restrict access to their data classified as **"Confidential"** or higher. If data access is delegated to an operations group, owners must communicate the data classification controls required to the operations group

(b) Maintain, update and review access approval lists for their data classified **"Confidential"** or higher

(c) Review access logs for data classified as "Highly Confidential"

(d) Ensure that sufficient controls are available on all systems that provide read access for their data that is classified **"Confidential"** or higher

(e) Update access lists when they are notified regarding an employee's departure from the enterprise

4.02 IT System administrators are responsible to:

(a) Manage data access controls as directed by business owners

(b) Identify the highest level of data classification that their system may support

4.03 Users who have access to data classified higher than "Public" are responsible to respect the controls required for data access corresponding to the data's classification. If a user copies data classified higher than "Public", the user must control access to the copy corresponding to its classification.

Under no circumstances may a user copy data classified as "Highly Confidential"

5 DEFINITIONS

5.01 **Business owner** is a senior member within the organization who is accountable for overall management of an application or 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

OCIO IT 9.01 – Data Business Ownership
OCIO IT 9.02 – Data Classification
OCIO IT 9.06 – Data Encryption