Office of the Chief Information Officer Directive: IT 11.03	Published: 10/2020
Chapter: Backup and Disaster Planning	Last Review: 01/2022
Subject: **Identification of Critical Processes**	

1 DIRECTIVE

1.01 All GNB departments must identify and prioritize critical IT processes and associated data, required hardware, and required software and report this information to the disaster planning team.

1.02 All GNB departments and IT service providers must assign members to the department's disaster planning team.

1.03 The Disaster Planning Team meets annually to review and update the disaster recovery plan.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that, in the event of a disaster at a GNB IT infrastructure site:

(a) All critical IT processes for the site may be re-established in a prioritized order within a documented timeframe.

(b) GNB will have the capability to start up and continue executing that site's critical IT processes to maintain business continuity.

(c) GNB can re-establish the site's critical IT processes in a timely manner following the occurrence of any disasters whether these stem from natural, accidental or intentional causes.

3 SCOPE

3.01 This directive applies to all departments in GNB which have any dependencies on IT processes.

4 RESPONSIBILITY

4.01 Business owners in GNB are responsible to identify their critical IT based business processes, data, hardware and software to their GNB IT infrastructure site liaison for the disaster planning team.

4.02 Each department is required to assign a GNB IT infrastructure site liaison

4.03 Each GNB IT infrastructure site liaison, communicates with the IT Service Provider (often SNB) and the departmental business owners.

4.04 The disaster planning team is responsible:

(a) To document all identified critical IT processes, data, hardware and software in the disaster recovery plan.

(b) To develop backup plans to enable the continued execution of all critical IT processes within a stated and agreed-upon period after a disaster has been declared.

5 DEFINITIONS

5.01 "**Critical IT process**" is a computer-assisted process which is vital to the operation of a business or organization.

5.02 "**Critical data, hardware and software**" is that data, hardware and software that is needed for continued execution of one or more critical IT processes.

5.03 **GNB IT infrastructure site liaison** – each department assigns an individual to communicate between business owners and IT

5.04 **Disaster Planning Team** – a team composed of Departmental Business IT Process owners, GNB IT infrastructure site liaisons and Information Technology Service Delivery Organization experts, that meets annually to review, test, and update the disaster recovery plan.

6 RELATED DIRECTIVES

OCIO IT 11.01 – Disaster Planning Team