Office of the Chief Information Officer Directive: IT 11.09	Issued: 06/2020
Chapter: Backup and Disaster Planning	Last Review: 01/2022
Subject: **Disaster Recovery Plan Review**	

1 DIRECTIVE

1.01 The disaster recovery plan (DRP) must be reviewed any time there is a change and/or on an agreed upon lifecycle to incorporate changes regarding GNB's critical processes.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that all critical IT processes currently in production are addressed in the DRP.

3 SCOPE

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

4 RESPONSIBILITY

4.01 All departments/functions in GNB are responsible to identify the following to their site liaison for the disaster planning team:

(a) Changes to existing critical processes, data, hardware and software currently identified in the DRP. This should include any discontinuations of obsolete elements.

(b) Critical IT processes, data, hardware and software which have been implemented since the last DRP review.

(c) Key business unit resources and contact information.

4.02 Each GNB IT Infrastructure site liaison is responsible to report the site's critical IT processes, data, hardware and software to the disaster planning team identifying all changes to the existing DRP.

4.03 The disaster planning team (DPT) is responsible:

(a) To change the DRP documenting all current critical IT processes, data, hardware and software.

(b) To change the backup plans incorporating all identified changes to critical processes, data, hardware and software.

(c) To establish, renew or discontinue offsite processing agreements as determined in the DRP.

4.04 GNB IT infrastructure site management is responsible to approve:

(a) All changes to the DRP.

(b) All renewals and changes to offsite processing agreements as

determined in the DRP.

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.

6 RELATED DIRECTIVES

OCIO IT 11.01 – Disaster Planning Team
OCIO IT 11.03 – Identification of Critical Processes
OCIO IT 11.04 – Backup Schedule
OCIO IT 11.05 – Backup Data Stored Onsite
OCIO IT 11.06 – Backup Data Stored Offsite
OCIO IT 11.07 – Offsite Processing Agreements