Office of the Chief Information Officer Directive: IT 11.10	Issued: 06/2020
Chapter: Backup and Disaster Planning	Last Review: 01/2022
Subject: **DISASTER RECOVERY TEAM**	

1 DIRECTIVE

1.01 IT site management will establish the members of the disaster recovery team (DRT).

1.02 The DRT will prepare the detailed recovery and business continuity plans for the disaster.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that:

(a) Recovery processes and activities following a disaster are planned and handled by the most qualified personnel.

(b) Recovery plans and budgetary restrictions are overseen by the appropriate business owner.

3 SCOPE

3.01 This directive applies to all GNB IT sites.

4 RESPONSIBILITY

4.01 IT site management is responsible:

(a) To determine the makeup of the Disaster Recovery Team (DRT)

(b) To monitor and budget the costs of recovery

(c) To notify all affected parties as documented in the DRP and any new affected parties involved since the last DRP review

(d) To approve the recovery and IT processing continuity plans

4.02 The DRT is responsible to:

(a) Assess the extent of the damages resulting from the disaster

(b) Assess the recovery requirements for critical processes corresponding to the DRP

(c) Identify requirements for the IT site location, equipment affected, infrastructure, services, data restore and supplies

(d) Recommend restore, repair and replace decisions regarding the IT processing site, infrastructure, services and hardware

(e) Identify IT site relocation requirements for IT processing continuity and eventual recovery

(f) Identify personnel requirements and personnel needs such as transportation, meals and housing for processing continuity considerations and eventual recovery

(g) Offsite processing required for critical IT processing continuity, including personnel required for offsite processing.

(h) Prepare a disaster recovery time-line that includes:
(i) IT processing continuity relocation (if required)
(ii) Site preparation
(iii) Recovery effort required
(iv) Hardware repair and replace lead times
(v) System, application and data restore
(vi) IT and office infrastructure repair and/or replacement
(vii) Services reinstated onsite or transferred to an alternate site
(viii) Supplies replacement
(ix) Offsite processing brought back in-house
(i) Implement the critical processing continuity plan.
(j) Initiate the approved disaster recovery process.
(k) Declare when the disaster recovery is complete.
(l) Initiate the return in-house for offsite critical processes.

5 DEFINITIONS

None

6 RELATED DIRECTIVES

OCIO IT 11.02 – Disaster Notification

OCIO IT 11.03 – Identification of Critical Processes

OCIO IT 11.05 – Backup Data Stored Onsite

OCIO IT 11.06 – Backup Data Stored Offsite

OCIO IT 11.07 – Offsite Processing Agreement

OCIO IT 11.08 – Disaster Recovery Plan Testing

OCIO IT 11.09 – Disaster Plan Review