

1 DIRECTIVE

1.01 A backup schedule must be established for restoring critical data in the event of a disaster up to a specified recovery point objective for each critical process to achieve the documented business continuity targets.

1.02 Data archive, data retention and source document retention policies must conform to all business and legal requirements governing data retention.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that disaster recovery processes requiring restoration of critical data are clear, concise, and easy to understand so that they may be executed without undue delay to critical business processes.

3 SCOPE

3.01 This directive applies to all backup schedules for data identified as critical in the GNB's IT disaster recovery plan.

4 RESPONSIBILITY

4.01 Each owner of a critical business process is responsible to specify the data restore timing requirements for their processes and retention time for backups.

4.02 The IT disaster recovery planning team is responsible to document data restore timing objectives for critical applications.

4.03 IT Operations is responsible:

- (a) To establish a data backup schedule for each critical application to ensure that recovery of the data is possible within the documented timing objectives.
- (b) To exercise/test data recovery processes to ensure that they can, in fact, meet the time objectives.
- (c) To report on data recovery test results.

5 DEFINITIONS

5.01 "**Data backup**" is the process of making one or more copies of data so that the data may be restored in the event of damage to or loss of the data.

5.02 "**Data archive**" is the process of moving data from online disk to offline storage

(tape, CD/DVD, disk cartridge, other) because it is no longer needed and takes up valuable disk space.

- 5.03 “**Data retention**” is a requirement to keep data safe from destruction for a specified period of time.
- 5.04 “**Recovery point**” is a state for the data when it was copied to a backup medium. All changes applied to the data following the recovery point need to be reapplied following a data restore to bring the data up to date.
- 5.05 “**Source document**” is an original document from which data is entered into an IT application, file or database. It may be necessary to re-enter data from retained source documents after a data restore to reflect changes to the data made after the recovery point.

6 RELATED DIRECTIVES

OCIO IT 5.02 – Data Backup and Storage

OCIO IT 11.05 – Backup Files Stored Onsite

OCIO IT 11.06 – Backup Files Stored Offsite