DEVELOPMENT AUTHORITY OF THE NORTH COUNTRY

AUTHORITATIVE POLICY: Information Technology and Security

Board Resolution No.: 2013-10-01

PROCEDURE: 2.14 – Disaster Recovery Procedure

1.0 Introduction

Policy:
A disaster recovery plan, protecting all key applications, will be implemented and included in the Business Continuity Plan.

Purpose:
To define system recovery procedures for the restoration of systems and data in the event of a disaster.

Scope:
This policy applies to all Authority personnel and IT systems, networks, and assets.

Responsibilities:
The IT Director is responsible for developing and reviewing the IT Disaster Recovery Plan.

The IT Director is responsible for testing of the IT Disaster Recovery Plan.

The IT Director is responsible for various recovery tasks, such as installation and testing of replacement equipment, operations systems, applications software, communications, etc.

All Authority employees are responsible for notifying the IT Director in the event of an actual or suspected disaster that may affect any part of the Authority's IT systems, infrastructure, or assets.

Definitions:
Business continuity – The degree to which an organization may achieve uninterrupted stability of systems and operational procedures.

IT disaster – A sudden, significant event that may result in the loss or destruction of Authority information and/or loss of service on the Authority's IT network.

2.0 Procedure - IT Disaster Recovery Planning

The Authority shall develop an IT Disaster Recovery Plan. The IT Disaster Recovery Plan (DRP) shall be an integral part of the Authority's overall DRP, just as information technology is an integral part of the Authority.

Authority shall implement the Plan, educating employees in their roles and responsibilities; test the Plan, to see if it will ensure rapid and full recovery; and fix flaws identified in testing, to better ensure the Plan will work when it is most needed.

3.0 IT Disaster Recovery Plan

3.1 The IT Director shall ensure daily backups of Authority information stores (databases, etc.)

3.2 The IT Director shall periodically conduct a test of all backed-up data for integrity and recovery speed; frequency and extent of such testing shall be determined by mission criticality of the information.

3.3 In the event any employee knows of or suspects an IT disaster, the employee shall contact the IT Director and he or she shall begin the response and recovery process in accordance with the Plan.

4.0 IT Disaster Recovery Plan Review

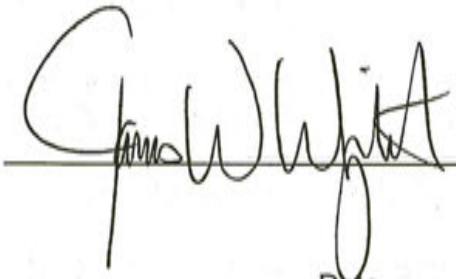
4.1 The IT Department shall test IT disaster response and recovery at least once every 12 months. The IT Department should also test response and recovery upon any changes to the Plan.

4.2 The IT Department shall review the IT Disaster Recovery Plan on a regular basis (annually, at a minimum) to determine if it continues to meet company, customer, and legal/regulatory requirements.

5.0 IT Disaster Recovery Plan Revision

5.1 After any review of the IT Disaster Recovery Plan, the IT Director shall be responsible for updating the Plan.

5.2 Within three months of any such update, the IT Director shall verify that the update is capable of providing the desired results by conducting a response and recovery test.

Date Adopted: April 1, 2014 Authorized: 

User Signature _____ Date _____