DEVELOPMENT AUTHORITY OF THE NORTH COUNTRY

AUTHORITATIVE POLICY: Information Technology and Security

Board Resolution No.: 2013-10-01

PROCEDURE: 2.6 - Wireless Network Management

1.0 Introduction

Policy:
The Authority's wireless network will be operated in a manner compliant with Federal Information Process Standards 140-2 and will use an AES encryption algorithm.

Purpose:
To delineate procedures for accessing the Authority IT wireless network.

Scope:
This applies to all personnel with access to the Authority IT wireless network.

Responsibilities:
All Authority personnel are responsible for knowing and adhering to this usage policy and procedure.

The IT Director is responsible for enforcing this procedure.

Definitions:
User – Anyone with authorized access to the Authority technology resources including permanent and temporary employees or third party personnel such as temporaries, contractors, consultants, and other parties with valid Authority access accounts.

2.0 Procedure:

2.1 Wireless Network Access

Wireless access to the Authority network is provided using WPA2 Enterprise security, which is Federal Information Process Standards (FIPS) 140-2 compliant and uses an AES encryption algorithm and 802.1 x-based authentications. WPA2 provides government grade security.

Wireless access for Smart Phones and tablets is not guaranteed due to limitations of some devices to process the authentication protocols.

Wireless use should be limited to work environments that have limited "wired" access. Using wireless and wired simultaneously is not recommended.

2.2 Inappropriate Use – Rogue Access Points

Inappropriate wireless network use is strictly prohibited. This includes installing any wireless access points not approved by the IT Director. Rogue, or unauthorized access points, pose a great security risk to the entire IT network.

2.3 Guest Wireless Access

Internet access may be provided to Authority guests through the use of the wireless network; however, the access shall be segmented with the use of a separate VLAN that does not have access to the Authority resources. The GUEST wireless connection will be secured with WPA2 encryption. Authority programs and files will not be accessible while connected to the GUEST network.

Date Adopted: April 1, 2014 Authorized: _____

User Signature _____ Date _____