DEVELOPMENT AUTHORITY OF THE NORTH COUNTRY

AUTHORITATIVE POLICY: Information Technology and Security

Resolution No. 2013-10-01

PROCEDURE: 2.5- Firewall Intrusion Protection

1.0 Introduction

Policy:
The Authority will employ state of the art firewall technology to protect the network from external threats.

Purpose:
The Authority operates a perimeter firewall between the Internet and its internal network in order to create a secure operating environment for Authority's computer and network resources. A firewall is just one element of a layered approach to network security.

Scope:
This applies to all IT systems and assets.

Responsibilities:
The IT Director is responsible for the management of the perimeter firewall.

Definitions:
Firewall Audit – An examination of a firewall system for security problems and vulnerabilities.

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 Processes

All services will be denied by the firewall unless expressly permitted in this procedure, or by management. The "allowed services" list can be found at the end of this document.

Outbound – All Internet traffic to hosts and services outside of the Authority. All traffic is subject to firewall and content filtering. All user Internet access is controlled and filtered by a Barracuda Web Filter.

Inbound – Only Internet traffic from outside the Authority that supports the business requirements of Authority will be permitted.

VPN (Virtual Private Network) access to the Authority network is provided using Cisco VPN client software. The software forwards a connection request to the firewall. Remote Authentication Dial-In User Service (RADIUS) and Network Policy Server (NPS) are then used to authenticate the user's request to connect to network and are either granted or denied access. (See 2.7-Remote Access Procedure). Users must have Management approval to be granted VPN access.

3.0 Operational Procedures

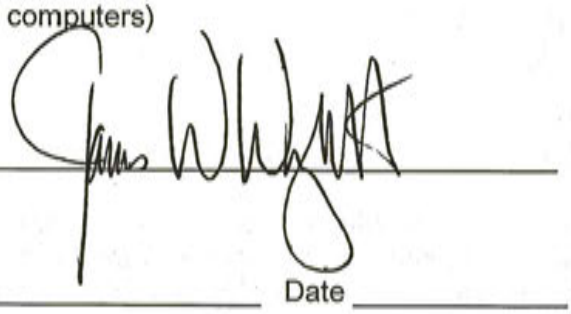
Requests for changes to the firewall's configuration must be submitted to the IT Director for review and must require justification as to what business need is being met. All requests will be assessed to determine if they fall within the parameters of acceptable risk. Approval is not guaranteed as associated risks may be deemed too high. If this is the case, an explanation will be provided to the original requestor and alternative solutions will be explored.

Firmware updates will be checked for monthly and applied to the firewall as needed.

The firewall configuration will be backed up before and after any configuration or firmware updates are applied; these will be stored on the network in a secure directory.

Current Allowed Services

1. HTTP (web browsing)
2. HTTPS (web browsing with authentication)
3. FTP (used for file transfers)
4. ICMP (used for network diagnostics/ping)
5. Pop3 (used by email systems)
6. SIP (used by our Voice over IP phone system)
7. RDP (used for remote connections to computers)
8. VNC (used for remote connections to computers)

Date Adopted: April 1, 2014 Authorized: 

User Signature _____ Date _____