Development Authority of the North Country
Governance Policies

Subject: Information Technology and Security Policy
Adopted: September 19, 2019
Resolution: 2019-09-85

Information Technology and Security Policy

1.0 Introduction

The Authority operates complex systems across northern New York, and utilizes its IT network to manage those operations. The use of modern information technology entails both benefit and risk. This policy is designed to reduce risks to an acceptable level, providing reasonable protection in a prudent manner, so that information can be shared appropriately and employed effectively in pursuit of Authority goals.

This policy document is intended to include policy statements broadly written. The name of the document is not intended to limit its scope or fully characterize the content.

The policy is issued by the Board of Directors. Development of procedures and implementation of the policy is the responsibility of the Executive Director and the Director of Information Systems.

2.0 Policy Statements

2.1 Acceptable Use The Authority's computing and communications resources shall be used securely, respectfully, and cooperatively in support of the Authority's mission.

2.2 Assignment of User Rights The Authority will assign access rights to network users based on the user's job responsibilities and the needs of the Authority.

2.3 Password Management The Authority will require users of its network to create strong passwords in order to help protect the network from unauthorized use.

2.4 Virus/Malware Protection The Authority shall protects its IT assets from infection by malicious software, viruses or malware.

2.5 Firewall/Intrusion Protection The Authority will employ state of the art firewall technology to protect the network from external threats.

2.6 Wireless Network 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.

2.7 Remote Access Remote access to the Authority IT network will be appropriately controlled and provisioned to ensure required security.

2.8 Cell Phone and Electronic Devices Cell phones and other electronic devices shall be used in compliance with NYS laws and other appropriate regulations, and authorized mobile devices will be connected to the Authority IT network.

2.9 **IT Device Inventory** IT assets will be acquired and managed in a manner consistent with the Authority's procurement policies and technology requirements.

2.10 **Electronic Mail** The use of electronic mail (email) shall be to support the Authority's business needs.

2.11 **Patch Management** The Authority will deploy a Patch Management platform that will provide software updates to all Authority computers.

2.12 **Data Back-up** The Authority will perform a backup procedure to ensure the integrity and availability of mission critical data.

2.13 **Disaster Recovery** An IT Emergency Response Plan (ERP) will outline a recovery strategy in the event of a disaster that effects the Authority IT network.

2.14 **IT Security Training and Awareness** The Authority will train and test employees on cybersecurity detection in order to reduce the risk of a cyberattack.

2.15 **Physical Controls** The Authority will restrict physical access to server rooms and protect these resources from intentional or unintentional harm or loss.

2.16 **Private Information Breach Notification** The Authority will follow New York State Technology Law with regard to breach of security of a system(s) as it relates to private information.

3.0 Procedures

3.1 The Director of Information Systems shall be authorized to develop and implement the necessary procedures, to achieve policy compliance subject to the Authorization of the Executive Director.