Office of the Chief Information Officer Directive: IT 10.02	Published: 04/2019
Chapter: Network Security	Last Review: 01/2024
Subject: **Firewall Protection**	

1 DIRECTIVE

1.01 All GNB networks must be designed, configured, tested, and implemented with appropriate and current firewall protection systems.

1.02 Servers and GNB provided computing devices must have firewall protection installed and configured to limit network traffic to only those protocols required for business processes.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that GNB systems and networks are protected against network threats.

3 SCOPE

3.01 This directive applies to all GNB networks and network-connected appliances, servers, and computer devices.

4 RESPONSIBILITY

4.01 The Network Architect is responsible to ensure that the network design incorporates industry-best firewall protection at each network access point, system server, and personal computer system.

4.02 IT Support is responsible:

(a) To ensure that all network appliances, servers, and GNB provided computing devices have their firewall applications configured appropriately.

(b) To review firewall logs for recognized and suspected intrusion attempts.

5 DEFINITIONS

5.01 **"Firewall"** refers to hardware or software, or a combination of both, that protects networked computers against hostile intrusion attempts from a connected public network like the Internet. Successful intrusion could compromise data confidentiality or integrity, or result in data corruption or denial of service.

6 RELATED DIRECTIVES

OCIO IT 6.01 – Configuration and Systems Management
OCIO IT 8.02 – Systems Security
OCIO IT 10.03 – Remote Access
OCIO IT 10.06 – File Transfer Protocol (FTP)
OCIO IT 10.07 – Email Security
OCIO IT 10.08 – Instant Messaging