Office of the Chief Information Officer Directive: IT 10.07	Issued: 11/2019 Last
Chapter: Network Security	Review: 01/2024
Subject: **Email Security**	

1 DIRECTIVE

1.01 The GNB's email service must provide for outgoing email encryption and incoming email decryption. The encryption technique must be the strongest available in the public domain.

1.02 For all email attachments, employees must follow the directives identified for downloaded files before opening the attachments. See **CSD IT 3.06 – Software Downloading** and **CSD IT 4.04 – Downloading**.

1.03 Users may not open an email message received from an unfamiliar source. Messages from unfamiliar sources must be summarily deleted and purged unless there is evidence that the message may be legitimate. In this case, each such message must be reported to the IT Service Desk where it will be thoroughly investigated before it is opened to determine the source and objective of the email.

2 PURPOSE

2.01 The purpose of this Directive is to ensure that security exposures associated with email are minimized.

3 SCOPE

3.01 This directive applies to IT Support and all users who send or receive email.

4 RESPONSIBILITY

4.01 IT Support is responsible to ensure that:

Email encryption technology is available for both outgoing and incoming email

4.02 All employees with email capability are responsible to take appropriate documented precautions regarding email and email attachments.

5 DEFINITIONS

6 RELATED DIRECTIVES

OCIO IT 3.06 – Software Downloading

OCIO IT 4.04 – Downloading

OCIO IT 8.05 – Controls for Viruses, Worms, and Malware

OCIO IT 9.06 – Data Encryption