Office of the Chief Information Officer Directive: IT 8.05	Published: 04/2019
Chapter: Physical and Systems Security	Last Review: 01/2022
Subject: **Controls for Viruses, Worms and Malware**	

1 DIRECTIVE

1.01 The GNB network will be defended by a firewall against unwanted intrusion from the public Internet and against unauthorized communications from inside the firewall to the public Internet.

1.02 All computer systems will be protected against malware infections with GNB-selected anti-virus software (AVS).

1.03 All systems must be updated with the latest AVS protection on a periodic basis coinciding with the AVS-vendor update schedule.

1.04 All programs, files, and documents introduced to a computer system from an external source must be scanned for malware infection by the AVS before use.

1.05 GNB network users must delete immediately any email received from an unrecognized sender.

1.06 All email attachments must be scanned for malware infection before being viewed or executed by the AVS.

2 PURPOSE

2.01 The purpose of this Directive is to minimize the risks to GNB computer systems attributable to infestation by malware.

3 SCOPE

3.01 This directive applies to all employees.

4 RESPONSIBILITY

4.01 All employees are responsible to watch for symptoms of any malware infestation on computer systems which they use.

5 DEFINITIONS

5.01 The following terms describe various types of malware:

5.02 **“Adware”** is software that specifically monitors a person's Web surfing and disrupts it by displaying contextual pop-up advertising.

5.03 A **"backdoor"** is software installed surreptitiously on a computer system that gives a malicious user unauthorized access to the system for any nefarious purpose.

5.04 A **"dialer"** is a program that exploits a computer's dialing capability through an attached modem and telephone line. It may replace a telephone number stored in the modem's dial-up connection with either a long-distance telephone number or a pay-per-dial number in order to run up phone charges. An alternate function may be to dial out at night to send "key logger" or other information to a hacker.

5.05 A **"key logger"** is software that copies a computer user's keystrokes to a file. Often, this software is programmed to be enabled only when the user is connected to a particular type of website such as a financial institution for capture of account numbers and access codes before they are encrypted and transmitted to the financial institution. The file may be transmitted at a later time to the hacker who created the key logger software.

5.06 **"Malware"** (derived from "malicious software") is a software program designed to fulfill any purpose contrary to the interests of the person running it.

5.07 **"Spam"** is unwanted email which is sent out in a large volume. It typically places an unwarranted and undesirable load on email systems, often contains other types of malware, and includes is fraudulent information.

5.08 **"Spyware"** is software that surreptitiously captures personally identifiable information about a person or organization, such as names, log-on identifiers, credit card numbers, passwords, email addresses, contact lists, and telephone numbers. It will either save such information or send it to third parties when the person is connected to the Internet. Another example of spyware is a program that peruses a person's modem to change dial-up numbers.

5.09 A **"Trojan horse"** is software that appears to be useful but will intentionally do damage after it is installed or run on a computer. Some Trojan horses are designed not to do damage directly but install a backdoor on the computer.

5.10 A **"virus"** is a self-replicating malicious program that spreads by attaching copies of itself, possibly modified, into other executable code or documents thus infecting the code or documents. The virus spreads when the infected files are copied to uninfected systems by removable media or as an email attachment and executed or opened there.

5.11 A **"wabbit"** is a type of malware that does damage to a computer system by quickly replicating itself with possibly malicious side-effects designed specifically for a denial-of-service attack.

5.12 A **"worm"** is a malicious program that spreads by taking advantage of file or network transport features on a computer system that allows it to spread unassisted.

6 RELATED DIRECTIVES

OCIO IT 10.02 – Firewall Protection

OCIO IT 10.03 – Remote Access