ANTI-VIRUS & MALWARE POLICY

NextGen CGI, LLC

Document Owner: NextGen CGI, LLC
Effective Date: January 1, 2021
Updated:

NextGen CGI, LLC Anti-Virus & Malware Policy							
Effective Date:				**Document Owner:**			
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0	01/01/2021	Policy	S. Hall	S. Hall	01/01/2021	S. Hall	01/01/2021

1. Overview

The number of computer security incidents related to malware and viruses and the resulting cost of business disruption and service restoration continue to escalate. Implementing anti-malware and anti-virus systems, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are best practice actions that must be taken to reduce risk and manage the organization's environment.

The word 'malware' is used collectively to denote many types of malicious software, including viruses, ransomware, worms, trojans, macros, mail bombs, and rootkits. A virus is a piece of self-replicating computer program code that is designed to destroy or damage digital information, or to steal user or business data.

There are many potential sources of malicious software, including websites, social media, USB memory sticks, unsolicited CDs, electronic mail, and software or documents copied over networks such as the corporate intranet or the public internet.

2. Purpose

The purpose of this policy is to describe requirements for preventing and addressing computer virus, worm, spyware, malware, and other types of malicious software.

3. Scope

This policy applies to all company officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that possess or manage assets owned by the organization. It is the responsibility of all the above to familiarize themselves with this policy and ensure adequate compliance with it.

4. Policy

The CESO or designee shall ensure:

- Procedures and tools exist to guard against, detect, and report malicious software
- IT personnel are trained and proficient in the use of the security solutions used to protect against malicious software
- End users are aware of the security policies enforced on their workstations

Below is a table that summarizes the current, approved anti-virus/anti-malware software solutions that all assets connected to the network should have installed and properly configured:

Asset Type	Operating System	Anti-Virus Solution
CONFIDENTIAL	CONFIDENTIAL	CONFIDENTIAL

4.1 Computing Assets

4.1.1 All workstations and server-based assets used for business, whether connected to the network or stand-alone units, must use organizationally-approved anti-virus/anti-malware protection software and configurations. The following procedures shall be followed by all personnel:

- Virus protection software must not be disabled or bypassed
- Settings for the virus protection software must not be altered in a manner that will reduce the software effectiveness
- Automatic update frequency cannot be altered to reduce the frequency of updates
- All servers attached to the network must utilize approved/standard virus protection software and setup to detect and address identified viruses
- All electronic mail gateways, devices, and servers must use organizationally-approved email virus/malware/spam protection software and must adhere to rules for the setup and use of this software
- Any threat that is not automatically cleaned, quarantined, and subsequently deleted by malware protection software constitutes a security incident and must be reported to IT and the Chief Executive Security Officer (CESO)).
- Anti-virus/anti-malware signature updates shall occur on a frequency defined by the organization but shall occur minimally once each calendar day
- All personal computers, devices, and servers connected to the organization's network must run a supported version of the Operating System (OS) and installed applications with the latest available patches applied.

4.2 Application Installation and Management

4.2.1 All authorized applications and software shall be installed by assigned resources within the organization. Managed anti-virus/anti-malware software shall ensure:

- Authorized applications and software operate according to a clearly defined security policy
- All unauthorized applications and software are prevented from being executed
- Email attachments must be scanned by an anti-virus product before delivery.

4.3 Licensing, Maintenance, and Support

4.3.1 Maintenance actions (software updates, definition updates, infections, etc.) shall be logged and retained for a period aligned with the Data Retention Policy to allow proper investigations into malware-related incidents.

4.3.2 Management shall ensure proper licensing, tracking, and related documentation. This shall include processes and procedures supporting:

- Anti-virus software installation on all systems

- Regular threat-scanning capable of detecting, removing, and protecting against known types of malicious software
- Annual review and re-evaluation of low-risk systems and appliances not considered affected by malicious software based on current best practice
- Proactive monitoring and update mechanisms supporting this policy
- Verification that mechanisms are in place for preventing users from disabling or modifying antivirus detection tools
- Processes and procedures for exceptions to the policy exist and are followed based on a case-by-case evaluation
- If anti-virus mechanisms are disabled, additional security measures may need to be implemented for the period of time during which anti-virus protection is not active.

4.3.3 The organization reserves the right to disconnect any device from the network if an infection is found or suspected. The device will be disconnected until the infection is removed and suitable preventative tools have been installed on the device.

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this policy. Appropriate controls include:

- Virus and malware installation settings and update logs
- Associated virus scan and history logs
- Procedures for quarantine and removal of threats
- Documented remediation and communication procedures for large scale incidents

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Related Standards, Policies, and Processes

- Data Retention Policy
- Configuration Management Policy
- Asset Management Policy

8. Definitions and Terms

The following definition are not all-inclusive and should be updated as new information is made available:

Term	Definition