[Insert Company Name and Logo]	
Title: Protection from Malicious Software	**P&P #:**
Approval Date:	**Review:**
Effective Date:	**Security Team**

Purpose: This policy communicates security processes used to protect the confidentiality, availability and integrity of sensitive and/or regulated data by each employee and/or department from malicious software.

Scope: This policy applies to all employees and other members of the workforce (whether paid, volunteer or contractor) given access to electronic information systems under the organization's ownership.

Definitions:

1. Sensitive and Regulated Data: any information that should only be accessed by authorized personnel. It includes Protected Health Information, financial information, personnel data, trade secrets, and any information that is deemed sensitive, regulated, or confidential, or that would negatively affect [Insert Company name] if inappropriately handled.
2. Security Officer: the individual appointed by [Insert Company name] to be the point person in charge of data security under applicable including, but not limited to: HIPAA Security Officer under §164.306(2) of the HIPAA Security Rule.
3. Malicious software (malware): Any software that gives partial to full control of your computer to do whatever the malware creator wants. Examples include virus, worm, trojan, adware, spyware, root kit, etc.

Procedure:

1. [Insert Company name] has developed, implemented, and periodically reviews a documented process for guarding against, detecting, and reporting malicious software posing a risk to sensitive and/or regulated data. Malicious software prevention, detection, and reporting procedures will include, but are not limited to:
    a. Anti-malicious software installed and updated on ePHI Systems.
    b. Procedures for workforce members to report suspected or confirmed malicious software.
    c. Plan for recovering from malicious software attacks in accordance with the Disaster Recovery Plan.
    d. Process to examine electronic mail attachments and downloads before they can be used on systems.
2. Workforce members must not bypass or disable anti-malicious software installed on any Systems without direct authorization by the Security Officer.

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.

3. [Insert Company name] provides periodic training and awareness to its workforce members about guarding against, detecting, and reporting malicious software. Training and awareness for workforce members on protection from malicious software will include, for example, the following topics:
    a. How to discover malicious software
    b. How to report malicious software
    c. How to discover malicious software fraud
    d. How to keep from downloading or receiving malicious software including not opening or launching email attachments that may contain malicious software
    e. How to use anti-malicious software appropriately.

VIOLATIONS:
Any known violations of this policy should be reported to the Security Officer. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with documented procedures, up to and including termination.

[Insert Company name] may advise law enforcement agencies when a criminal offense may have been committed.

Attachments: None

Related Policies: None

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.