Antivirus Policy

Document Number: ITS-0027

Date Published(sys): 6/16/2022

General Description

Policy Summary:

Ensuring anti-virus and anti-malware initiatives are implemented on all applicable system components.

Purpose:

This policy and applicable supporting procedures are designed to provide Trinity University with a documented and formalized process for ensuring antivirus and anti-malware technical controls are implemented on all applicable system components. Additionally, compliance with the stated policy and supporting procedures helps ensure the confidentiality, integrity, and availability (CIA) of Trinity University's system components.

Scope:

This policy and supporting procedures encompass all system components that are owned, operated, maintained, and controlled by Trinity University and all other system components, both internally and externally, that interact with these systems.

- Internal system components are those owned, operated, maintained, and controlled by Trinity University and include all servers, laptops, desktops, mobile devices, internet and email gateways, etc.
- External system components are those owned, operated, maintained, and controlled by any entity other than Trinity University, but for which such external resources may impact the confidentiality, integrity, and availability (CIA) and overall security of "Internal system components".
- While Trinity University does not have the ability to provision, harden, secure, and deploy another organization's system components, Trinity University will follow best practices in obtaining all relevant information ensuring that such systems are safe and secure.

Exceptions:

In a few instances, Trinity systems may require to be exempted from the Antivirus Policy due to possible technical difficulties or third-party contractual obligations. Any such exceptions to the current policy must be documented and approved via the Trinity's Exceptions Management Process.

Policy Content

① Roles & Responsibilities

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees, and users of system components, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to Trinity University information systems, all relevant parties are helping promote the Confidentiality, Integrity, and Availability (CIA) principles for information security in today's world of growing cybersecurity challenges.

Role	Responsibilities
Management Commitment	Responsibilities include providing overall direction, guidance, leadership, and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The CIO is to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture.
Trinity Employees	Responsibilities include adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any Trinity University internal system components. Additionally, Trinity University employees are to report instances of non-compliance to ITS.
Vendors & Contractors	Responsibilities for such individuals and organizations are much like those stated for Trinity University Employees: adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any such system components
ITS CORE Infrastructure Administrators	Responsible for the oversight of all anti-malware initiatives. Configure the antivirus settings to ensure

	security. They also perform comprehensive analysis of all security tools before any of those are placed into any of the University environments. These administrators will also be responsible for anti-malware software installation, configuration, maintenance, operation, and will modify the software as needed. The ITS Core Infrastructure team will take appropriate actions to contain virus infections and other malwares, and assist in their removal as needed.
ITS CORE Infrastructure Manager	In the event of a relevant security incident where the regular tools are not capable to contain and remediate it, the Core Infrastructure Manager will coordinate the incident handling and communication plan described in the TU's Incident Response Plan
ITS Technical Support Services team	Responsible for addressing or supporting employees with infected devices.

② Policy

Trinity is to ensure that all applicable users adhere to the following policies for purposes of complying with the mandated organizational security requirements set forth and approved by management:

- All computing systems and devices connected to the TU's network or data systems must have anti-malware software installed, including laptops, desktops, servers, internet gateways, etc.
- Authorized ITS personnel are to undertake a comprehensive analysis for ensuring that University has acquired the best possible anti-malware software solutions, which include antivirus, anti-spyware, and other necessary utilities.
- The applicable solutions are to be evaluated on an annual basis for ensuring their adequacy and sufficiency.
- All University system resources that require antivirus must be regularly updated.
- The applicable antivirus programs are to be capable of detecting, removing, and protecting against known types of malicious software.
- Antivirus should be executed on every boot or at least every 24 hours. Also, anti-malware tools must scan every email, file download, media introduced, email attachment, and web traffic.
- Settings for the virus protection software must not be altered in a manner that will reduce the software effectiveness.
- If feasible, an infected computer device may be disconnected from the network until the infection has been removed.
- Pro-active monitoring and alerting mechanisms supporting this policy must be implemented.

- Exceptions to this policy may be allowed if the computer device cannot have antivirus software installed.
- If malware is identified or there is suspicion of infection, the user must notify the ITS Technical Support Services at ITSupport@trinity.edu or extension x7409.
- Antivirus logs must be centrally monitored and regularly maintained.
- Antivirus software should not be disabled or altered by users, unless specifically authorized by ITS on a case-by-case basis for a limited time period.
- Any antivirus solutions utilized by Trinity must be from an approved vendor and offer ongoing customer support pertaining to the installation and maintenance of the applicable antivirus software.
- Trinity ITS Employees who distribute computers to Trinity faculty, students and staff are responsible for ensuring that those computers have current antivirus software installed with a current antivirus signature.
- Trinity University mail servers are to be configured with anti malware solutions, such as antivirus and anti-spam, along with other essential utilities for blocking and containing email viruses and other malware threats. Specifically, all email communications and web browsing for webmail must be sent through the applicable email filtering systems.

③ Incident Response Measures

Should a user suspect a malware threat, the following steps must be taken immediately:

- Immediately notify ITS Technical Support Services (TSS) via ITSupport@trinity.edu, and inform them of the situation.
- Follow the instructions and guidance given by the ITS TSS support personnel.
- If no immediate ITS TSS personnel are available – because of outside of normal business hours or communication constraints, discontinue the use of the system resource in question.
- Undertake measures on the affected system resource for removing all viruses, which may include reformatting procedures, along with possible physical destruction of critical devices (i.e., hard drive, etc.), or the entire system altogether.

Note: Common examples of malware threats include the following: error messages, continuous pop-up advertisements, system performance issues, actual antivirus warnings, alerts, and other suspicious activities.

Performance Evaluation

Consequences of Policy Violation:

1. Any behavior in violation of this policy is cause for disciplinary action and violations of this policy may result in, but are not limited to, any or all the following:
    1. Loss of university computing, email and/or voice mail privileges.

2. Disconnection from all Trinity University networks and systems.
3. University judicial sanctions as prescribed by the student code of conduct.
4. Reassignment or removal from university housing and/or suspension or expulsion from the university.
5. Prosecution under applicable civil or criminal laws.

2. Violations will be adjudicated, as appropriate, by the CIO, the Office of the Dean of Students, the Office of Housing and Residential Life, and/or the Office of Human Resources.
3. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Terms & Definitions

Terms and Definitions:

Term:	Definition:
Anti-Malware solutions	Antivirus is without question the foundation for any anti-malware platform, but there are additional software solutions that can greatly assist in such endeavors, such as anti-spyware, and others, thus Trinity is to utilize such tools as necessary for ensuring the safety and security of system resources. These tools are to go through a comprehensive analysis by authorized ITS personnel before being placed into any such environments.
Anti-Spyware	Software designed to detect and remove spyware.
Antivirus Software Signature	A virus signature (also known as a virus definition) is a file or multiple files that are downloaded by a security program to identify a computer virus. The files enable detection of malware by the antivirus (and other anti-malware) software in conventional file scanning and breach detection systems.
Behavior-based Heuristics Tools	In a method called behavioral analysis, antivirus technologies crack down on viruses that aim to circumvent previous methods used for antivirus processes. The move of companies towards a behavioral analysis pattern for their antivirus indicates the rise of a proactive antivirus strategy, as opposed to a reactive one.
File Integrity Monitoring (FIM) Tools	IT security process and technology that tests and checks operating system (OS), database, and application software files to determine whether they have been tampered with or corrupted. FIM, which is a type of change auditing, verifies and validates these files by comparing the latest versions of them to a known, trusted “baseline.” If FIM detects that files have been altered, updated, or compromised, FIM can generate alerts to ensure further investigation, and if necessary, remediation takes place. File integrity monitoring encompasses both reactive (forensic) auditing as well as proactive, rules-based active monitoring.

Term:	Definition:
Malware	Malicious software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, keyloggers, spywares, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code (malware).
Virus	A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

Revision Management

Revision History Log:

Revision #:	Date:	Recorded By:
v2.0	6/16/2022 8:51 AM	Ben Lim
v1.0	5/12/2022 9:47 AM	Dan Carson

Vice President Approval:

Name:	Title:
Ben Lim	Chief Information Officer