Standard: Malware Protection

Effective Date:	2019.05.26
Revision Date:	2020.02.06
Review Date:	2021.02.06
Approving Body:	Director, Information Security and Compliance
Authority:	Information Security Policy
Responsible Owner:	Director, Information Security and Compliance
Classification:	Public

Purpose

The Malware Protection Standard describes the acceptable standards to ensure the security and integrity of university information and information technology resources. Malicious software such as viruses, worms, trojans, etc. ("MALWARE") must be actively guarded against, eradicated, or quarantined. Anti-virus/malware software works to detect, block, and remove computer viruses and other malicious software.

Who/what does the standard apply?

The requirements in this standard apply to all university owned servers, desktops, tablets, that are capable of supporting an anti-malware solution.

Definitions

- **Malware:** is the general term covering all the different types of threats to end point safety such as viruses, spyware, worms, trojans, rootkits and other related terms.
- **Anti-Virus software:** computer software used to prevent, detect and remove malicious software.

Compliance

Systems must align to the requirements and specifications outlined within this standard. Where systems and applications are unable to comply, please submit an Information Security Decision Request to the Director of Information Security and Compliance for review.

Specifications

Requirement	Specifications
Installation of Anti-Virus software.	All devices which are used for collecting, creating, storing, processing, or distributing university information must have the most recent version of IST approved anti-virus/malware software installed.
Update of Anti-Virus software.	The anti-virus software must be active, be scheduled to perform virus checks on all files at regular intervals, and have its virus definition files kept up to date.
Reporting Incidents.	If a user suspects that a computer is infected with virus/malware, it must be reported to the Service Desk.
Exceptions	Exceptions to this standard may be approved if a device cannot have anti-virus software installed or an alternate solution is desired. Possible examples of this would be vendor-controlled systems, or devices where anti-virus software has not yet been developed. Please submit a Decision Request Form.

References

Policy, Procedure or Standard	
Information Security Policy and Procedure	
Use of Computer Facilities Policy and Procedure	