Malware Protection and Management

I. INTRODUCTION

This policy establishes a proactive malware management program, as the Information Security policy requires.

II. POLICY OVERVIEW

Operating system and software program vendors periodically release security-related patches that must be applied to maintain a secure environment. The objectives of this policy are to:

- Safeguard the University's information from security threats that could harm its operations or reputation
- Fulfil the University's duty of care toward the information with which it is entrusted
- Protect the confidentiality, integrity, availability, and value of information through the optimal use of security controls

III. POLICY PROCESS

A. Requirements

1. All University-own systems, where technically feasible, must run anti-malware software supplied and managed by the University.
2. All personal computers, devices, and servers connected to the University network must run a supported version of the Operating System and installed applications with the latest available patches applied.
3. Any non-University-owned devices must run an appropriate anti-malware product. Details of suitable products can be found at [Link].
4. The University 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. The University may restrict or deny network access to any systems without up-to-date anti-malware software.
6. The University will use an enterprise-wide malware management tool to perform continuous and real-time malware detection, eradication, and monitoring. Systems that cannot use the standard malware management tools for detection and protection shall identify an alternate malware protection process where technically feasible and prudent.
7. Configuration of the malware protection system shall follow vendor recommendations and best practices. The system shall hinder end-users from uninstalling or disabling the malware protection services.
8. Email attachments must be scanned by the anti-malware system before delivery.

9. The malware protection system must be configured to block malicious URLs and email attachments, including but not limited to the types listed in Appendix A.
10. Systems connected to the University's network must regularly be scanned for malware. Full scans must be performed weekly or when significant changes occur to the system.
11. The malware protection system must be monitored continuously to detect and address potential malware threats.
12. The malware protection system must be updated with new detection logic continuously. The University will actively monitor online threat detection services to proactively tune and train the malware protection system for new threats.
13. Malware detections shall be tracked and logged.

B. Roles and Responsibilities

1. The Information Security Office (InfoSec) is responsible for developing, implementing, and running the malware protection and management program.

IV. DEFINITIONS

- **Malware** - Malware describes malicious applications or code that damages or disrupts the normal use of endpoint devices. When a device becomes infected with malware, you may experience unauthorized access, compromised data, or being locked out of the device unless you pay a ransom.
- **Operating System** – An Operating System (OS) is system software that manages computer hardware and software resources and provides common services for computer programs. Microsoft Windows, Windows Server, Linux, macOS, iOS, etc. are common OS's DU uses.
- **URL** - A Uniform Resource Locator, colloquially termed as a web address, is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A URL is a specific type of Uniform Resource Identifier, although many people use the two terms interchangeably.