IT: MALWARE PROCEDURE

Procedure Type:	Institution	**Initially Approved:**	April 01, 2011
Procedure Sponsor:	VP Administration	**Last Revised:**	August 11, 2020
Administrative Responsibility:	Computing & Technical Services (CTS)	**Review Scheduled:**	August 2025
Approver:	President and CEO		

A. INTENT

Computing and Technical Services (C+TS) shall manage a program to detect and prevent the installation or activation of malware on devices connected to the AUArts wired and wireless networks.

B. SCOPE

This procedure authorizes the deployment of processes and programs to monitor systems on the AUArts network in order to detect and remove malware, as well as provide education and awareness to all users accessing AUArts Information Assets.

C. PROCEDURES

1. AUArts-owned devices shall be configured appropriately to ensure real time malware protection.

2. C+TS shall configure the malware protection software on AUArts devices to retrieve virus signature and other updates in a timely manner.

3. Implementation of security patches and software upgrades for operating system software and the malware protection software shall follow the Change Management Procedure.

4. Access to the configuration of the malware protection software shall be managed and controlled by C+TS.

5. All AUArts devices shall have a malware scan scheduled regularly but no less than every week.

6. Devices detected with malware that are not managed by AUArts (i.e. User Device) will be removed from the network.

Roles and Responsibilities

7. C+TS shall:
   - 7.1 Ensure appropriate and effective malware protection software is installed and configured on all AUArts devices, updates are enabled, and tampering is prevented.
   - 7.2 Review malware protection software reports to assess effectiveness.
   - 7.3 Monitor malware protection software performance.
   - 7.4 Monitor the evolving malware landscape to remain current on potential threats to the AUArts computing environment.
   - 7.5 Work collaboratively with industry, PSI peers and Advanced Education to implement cybersecurity best practices.
   - 7.6 Restrict or deny access for User Devices without appropriate malware protection.
   - 7.7 Provide education and awareness for end users on safe technology practices that aid in the detection, prevention and spread of malware.

D. DEFINITIONS

Authorized Users	Students, staff, faculty, employees and third-party users such as contractors, consultants, temporary users, suppliers and service providers.
AUArts Devices:	All AUArts-owned desktops, laptops, servers, or other programmable devices connecting to the AUArts network or Information Assets.
User Devices:	All user-owned programmable devices connected to the AUArts network or Information Assets.
Information:	AUArts data in any form or media, including databases and computer files, which is collected, transmitted, stored or maintained on AUArts' information systems or elsewhere.
Information Systems:	AUArts' Information Technology (IT) networks, systems and applications.
Information Assets:	Information and Information Systems.
Malware:	An umbrella term used to describe hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.
Malware Protection Software:	A generic term used to describe all programs that detect and prevent the introduction and operation of malicious software.

E. RELATED POLICIES

- Information Security Policy
- Acceptable Use Policy

F. RELATED LEGISLATION

G. REVISION HISTORY

Date (mm/dd/yyyy)	Description of Change	Sections	Person who Entered Revision (Position Title)	Person who Authorized Revision (Position Title)
07/31/2020	Template Change and Content Revisions		Director, CTS	