Administrative Policy

Policy Title:	Malware Removal Policy
Policy Number:	LC-1619
Date Adopted:	4/10/2013
Version:	2.0
Review Cycle:	Biannual
Date Last Reviewed:	7/13/2016
Office Responsible:	Information Technology
Reviewing Committee:	Measurement and Knowledge Management
Related Policies:	N/A
Related Laws:	N/A

Policy Summary: The purpose of this policy is to provide preventative measures that shall be taken by Jackson Community College employees to help achieve effective virus detection and prevention.

Scope: This policy applies to all Jackson College Employees.

Definitions:

Computer Virus: a piece of potentially malicious programming code that will cause some unexpected or undesirable event.

Malware: malicious software or code that typically damages or disables, takes control of, or steals information from a computer system.

Administrative Rights: allows the user to install software, and change configuration settings on their computer.

Policy Statement:

Viruses and Malware can be transmitted via e-mail, instant messaging, attachments, downloadable Internet files, diskettes, memory sticks, external hard drives, CD's and DVD's. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to JC, in terms of lost data, lost staff productivity, violations of sensitive customer information, and/or loss of reputation. As a result, one of the goals of JCC is to provide a computing network that is secured and virus-free.

Jackson College installs licensed copies of Antivirus software on its network. All computers attached to the Jackson College network must have the standard college supported anti-virus software installed. This software is installed on college owned computers and automatically performs virus checks at regular intervals, and keeps virus definition files up to date. The computer will update virus software automatically once logged into the JC network.

If an employee receives what he/she believes to be a virus or malware or suspects that a computer is infected with a virus they must report to the IT department immediately via the Solution Center. Any virus-infected computer will be removed from the network until it is verified as virus-free. If a malicious program is found on the employee's computer IT will perform a reload on the computer, in order to ensure all parts of the program are removed. Any data that is saved to the Desktop or the C: Drive cannot be recovered after a reload.

If it is found that a specific user is having reoccurring malware problems on their computer Information Technology will remove the users' administrative rights to the computer to prevent further installation of malicious programs at the discretion of the IT Director.

Any activities with the intention to create and/or distribute malicious programs onto the Jackson College network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

Rules for Virus and Malware Prevention:

1. Users must always run the standard anti-virus software provided by JC.
2. Users must never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
3. Users must be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link.
4. Users must not copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
5. Users must not click on unexpected website pop-ups asking users to perform a function (install, download, open etc.). Clicking on the close button will likely download malware. Right-click the pop-up ad in the taskbar and select "Close" from the menu.
6. Users must not install toolbars or software that are not necessary to their job function. Websites that ask you to install additional toolbars often also contain malware.

Change Log:

Date Of Change	Version	Description of Change	Responsible Party
4/10/2013	1.0	Initial Release	J. Dobbs
07/13/2016	2.0	Review	J. Dobbs