REFERENCE ID NUMBER: 009	POLICY TYPE: IT INFORMATION SECURITY MANAGEMENT
OWNER: CHAD PETERSON	
EFFECTIVE DATE: 2/26/16	DOCUMENT NAME:
REVISION DATE: 7/26/16	**MALICIOUS SOFTWARE AND VIRUS PROTECTION**

MALICIOUS SOFTWARE & VIRUS PROTECTION

PURPOSE

To detect, guard against and have formal procedures in place for the reporting of malicious software and virus protection.

SCOPE

This policy applies to all Koble-MN HIO participants and workforce; participants, employees / authorized users, temporary staff, contracted staff, and credentialed provider staff.

SECURITY CONTROLS TO MITIGATE RISK OF MALWARE AND VIRUS DISRUPTION

Koble-MN HIO, their Vendor, and each Koble-MN HIO Participant shall ensure that it employs security controls that meet applicable industry or Federal standards.

The intent of security controls is so that information being transmitted and any method of transmitting such information will not introduce any malware or other program designed to disrupt the proper operation of a system, the network or any part thereof, or any hardware or software used by the Koble-MN HIO, Vendor, and each Participant in connection therewith.

In the absence of applicable industry standards, Koble-MN HIO, Vendor, and each Participant shall use all commercially reasonable efforts to comply with the requirements of this policy.

In addition, Malware (Virus) protection shall be installed and activated on all applicable Koble-MN HIO resources. This includes all computer equipment kept up to date with operating systems security software patches and fixes.

The Koble-MN HIO IT Department will regularly check that software is in place and up-to-date for all Koble-MN HIO systems to identify spyware, viruses, worms, Trojans and other forms of various malicious software.

REVISION HISTORY

DATE	DESCRIPTION OF REVISION	AUTHOR	APPROVAL DATE	APPROVED BY NAME & TITLE
7/26/16	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	7/28/16	Koble-MN Advisory Committee