Policy Name: Virus Protection Policy

Responsible Department: Information Technology

Approving Body: Policy Committee

Approved Date: Tuesday, December 15, 2014

Purpose:
N/A

Policy:
All computers directly attached to the WNMU network shall have current virus protection. Only computers meeting the current WNMU minimum requirements (WNMU police # XXX – Minimum Computer Requirements) will be allowed to attach to the network. WNMU-IT will make a licensed virus protection application available for installation on each computer directly attached to the network. WNMU-IT will also make up-to-date virus definition files available for maintaining the virus protection application.

All operating systems on computers directly attached to the WNMU network shall have the most recent security upgrades installed. The most recent security upgrade and installation instructions will be available from the WNMU IT file server.

Note that while IT will make the necessary data and software easily available, YOU are responsible for keeping your computer’s virus protection up to date.

Any computer that is acting as a source for destructive software will be disconnected from the WNMU network. Such computers will remain disconnected until it is demonstrated that the computer is free of destructive software and has all required security software installed. All computers attached to the WNMU network will be periodically scanned for the presence of current virus protection software and virus description data. Any computer that does not have current virus protection installed will be notified. If within a reasonable time, current virus protection software and current virus description data are not installed, the computer will be removed from the network.

All computers attached to the WNMU network will be periodically scanned for the presence of
the most recent service level upgrade. Any computer that does not have the most recent service level upgrade installed will be notified. If the required service level upgrade is not installed within a reasonable time, the computer will be removed from the network.

Specific "conditions of use" for information resources within other jurisdictions such as labs, libraries and dorms may be defined and enforced. These statements must be consistent with this overall policy but may provide additional detail, guidelines and/or restrictions. Where such "conditions of use" exist, enforcement mechanisms defined therein shall apply. These regulations and policies must be published and easily available to users of the equipment for which they are established.

**Procedures:**

None