MVNU PROTECTION OF ELECTRONIC DATA POLICY

Purpose of the Policy: This policy is designed to protect key electronic data of MVNU in the event of a major natural or man made catastrophe or act of terrorism at MVNU.

Definitions:

Key electronic data: Is any data that is kept in an electronic formation, the loss of which would cause considerable economic damage to MVNU or the use of substantial personnel resources to recover.

Secured off site location: Is a location, not owned or operated by MVNU which is located greater than one-half mile from the MVNU campus at 800 Martinsburg Road, Mount Vernon, Ohio. The site shall not be a personal residence. The site shall contain a locked vault structure which provides protection from natural and man made disasters. Authorized MVNU personnel shall provide proof of authorization to obtain admission to the site.

Storage device: Is a device sufficient to safely contain the key electronic data. The device shall be locked and accessible only by authorized personnel via key or code. It shall be placed in the secured off site location.

Authorized personnel: Shall include those authorized in writing by the President, Vice President of Academic Affairs and Vice President for Business and Management.

Statement of Policy:

The Vice President for Academic Affairs and Vice President for Business and Management acting with their appropriate advisors shall identify no less than annually all key electronic data for MVNU.

Key electronic data shall be updated and stored in duplicate form at the designated secured off site location no less than every seven (7) days. When necessary or advisable, the key electronic data may be duplicated in shorter intervals. The duplicate key electronic data shall be placed in the designated secured off site location by authorized personnel. At no time shall non-authorized personnel be allowed access to key electronic data that is not properly secured.

At no time shall duplicate key electronic data be in a location other than a secured location on campus or the secured off site location.

Transportation of key electronic data shall be made in a locked device accessible only by authorized personnel.

Approved by Compliance Advisory Council on April 6, 2006
Adopted by Cabinet on April 17, 2006

Prior to being designated an authorized personnel, the individual shall receive training on campus security regulations, this policy, Family Educational Rights and Privacy Act (FERPA), Health Information Portability and Accountability Act of 1996 (HIPAA), Graham Leach Bilely Act (GLB) and other applicable federal and state laws especially those that concern privacy.

Approved by Compliance Advisory Council on April 6, 2006
Adopted by Cabinet on April 17, 2006