MOUNT HOLYOKE

Electronic Data Storage and Retrieval Policy Statement

This policy addresses the College's approach to the storage, retrieval and disposal of electronic data in order to assure that privacy and security concerns are appropriately addressed. It does not address the archiving of historically important information.

Backup Procedures

Email inboxes are backed up to disk on a daily basis. After two days these files are written over. Central application systems such as Student, Human Resources, Financial, Financial Aid, Learning Management, Content Management, eThesis, and various other systems supporting the College are backed up on a daily basis.

Saved message folders in individual home directories (including email folders other than the inbox and departmental network folders), as well as central application systems, are backed up both to disk and to tape. Tape backups are also stored in off-campus locations.

Daily and weekly email and network backups are incremental backups and are done between full system backups. Full System backups occur about quarterly. Incremental backups are generally retained for 2 months. The full system backups are retained for at least a semester and normally for a year. Central application systems undergo full system backups on a daily basis.

Backups are made for purposes of restoration in the event of a system failure (to the individual desktop server or to a larger departmental or institutional server). They are not intended to provide ready access to or recovery of individual files or records.

Backup disks and tapes that have reached the end of the retention cycle are overwritten with more recent backup information or destroyed.

In the Event of Notice of Possible Litigation

If a written claim or complaint, subpoena, or other formal demand is made against the College for which documentation that could support or refute such a claim exists in the College's computer system (e.g., e-mails, written records or financial records), the manager receiving the claim shall notify the Director of Networking as to the particulars of the claim immediately. The Director of Networking will work with appropriate campus officials (e.g., the Director of Human Resources, the Dean of Faculty, the Dean of the College, the Director of Risk Management) to notify those involved that any files associated with the

event cannot be destroyed and perform targeted backups of the files of involved parties to assure that they are preserved.

Information that employees or students store on a local computer (e.g., C: drive) or other local media (e.g., CD's or flash drives) should also be retained and backed up to a secure location on a College server. All paper records are also required to be kept and produced if required by legal action or demand. Employees are prohibited from destroying any data upon notice of a potential claim. Deliberate destruction of identified data is a serious offense, and any person who deliberately destroys identified data will be subject to disciplinary action including termination of employment.

THE Campus Privacy and Security Committee
Revised 6/3/05