Backup Policy Statement

- Backups of all records and software must be retained such that computer operating systems and applications are fully recoverable. This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs, or other techniques.
- The frequency of backups is determined by the volatility of data; the retention period for backup copies is determined by the criticality of the data. At a minimum, backup copies must be retained for 30 days.
- At least three versions must be maintained.
- At a minimum, one fully recoverable version must be stored in a secure, off-site location. An off-site location may be in a secure space in a separate University building, or with an off-site storage vendor approved by Computer Services.
- Derived data should be backed up only if restoration is more efficient than creation in the event of failure.
- All information accessed from workstations, laptops, or other portable devices should be stored on networked file server drives to allow for backup. Information located directly on workstations, laptops, or other portable devices should be backed up to networked file server drives.
- Required backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period. Documentation of the restoration process must include procedures for the recovery from single-system or application failures, as well as for a total data center disaster scenario, if applicable.
- Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.
- Recovery procedures must be tested on an annual basis.