OFFICE OF INFORMATION TECHNOLOGY
Policies and Procedures Manual

1.7. Electronically Stored Information Retention Policy

1.7.1. Approval and adoption

1.7.1.1. Approved by the Chief Information Officer and Executive Vice President and adopted effective 2/14/2017.

1.7.1.2. Updated to replace “tapes” with “disk drives” as tapes are no longer used to backup data, also updated references to cloud services. Reviewed and approved by the Chief Information Officer and Vice President for Facilities & Technology Services and adopted effective 11/1/2017.

Signature/Title/Date:

1.7.2. Purpose

1.7.2.1. To document the University of La Verne retention periods for its electronically stored information.

1.7.3. Policy

1.7.3.1. All electronically stored information on University of La Verne technologies including, but not limited to servers, desktop and laptop computers, PDA’s, cell phones, and any other devices capable of storing information electronically is the property of the University and the University retains the right to access or copy the information as deemed necessary for University purposes.

1.7.3.2. All electronically stored information pertaining to University matters on personal technologies including, but not limited to home computers and laptops, personal cell phones, PDA’s and any other devices capable of storing information electronically may be discoverable and the employee is responsible for its retention and backup.

1.7.3.3. The University of La Verne has three types of centralized retention for electronically stored information: retention for Disaster Recovery purposes, retention for Litigation purposes, and retention for Compliance purposes.

1.7.3.3.1. **Disaster Recovery retention** of electronically stored information is

conducted by backing up the electronically stored information onto media such as disk drive backups, which are then stored for a defined period of time on a rotating schedule with disk drives being overwritten after they reach the end of the retention period. As such, they are point-in-time copies of the data that can be used to restore information needed in the case of a disaster or data loss. These backup disk drives are for disaster recovery purposes only. *Disaster Recovery retention of centrally-maintained servers is the responsibility of the Office of Information Technology*.

Disaster recovery retention of desktop or personal technologies is the responsibility of the individual assigned the equipment. The disk drive backups are also replicated to a remote site for Disaster Recovery on a daily basis to an East Coast facility (Iron Mountain).

1.7.3.3.1.1. Disk drives used for Disaster Recovery retention purposes are maintained offsite by synchronization with Iron Mountain. The disk drives are numbered and electronically cleared of data after the 30-day expiration before being re-issued into the backup inventory. Obsolete or damaged disk drives no longer part of the disaster recovery rotation are wiped clean and physically destroyed.

1.7.3.3.1.2. Office of Information Technology Disaster Recovery retention periods are:

1.7.3.3.1.2.1. **Voicemail**. Main campus voicemail backed up by OIT on a nightly basis and retained for 30 days. Remote site voicemails are not backed up by OIT.

1.7.3.3.1.2.2. **File and Print Servers**. Backed up by OIT on a nightly basis and retained for 30 days.

1.7.3.3.1.2.3. **Enterprise Application Servers**. Main campus backed up by OIT on a nightly basis and retained for 30 days. Ontario Law School and RCA sites not backed up by OIT.

1.7.3.3.1.2.4. **Departmental Servers**. The Office of Information Technology does not back up servers maintained by individual departments outside the purview of OIT Data Centers.

1.7.3.3.1.2.5. **PDAs.** The Office of Information Technology does not

back up individuals' PDAs. Individual users are responsible for maintaining backups of their PDA information for disaster recovery or compliance purposes.

1.7.3.3.1.2.6. **Desktop and Laptops**. The Office of Information Technology does not perform centralized backups of desktop or laptop computers with the exception of those specifically listed below. Backups of data stored on individual desktop and laptop computers rather than on University servers is the responsibility of the individual user. Backups can be done onto servers or onto external media such as CDs. DVDs, thumb drives, etc.

1.7.3.3.1.2.6.1. **Natural Science Division desktop computers**. Faculty desktops in the Natural Sciences Division are backed up onto the Natural Sciences Server on a nightly basis, with file overwrite. The server is backed up by OIT for Disaster Recovery retention purposes on a nightly basis and the backup retained for 30 days.

1.7.3.3.2. **Litigation retention** of electronic information is initiated in response to an obligation to preserve records relevant to anticipated litigation. *Litigation retention is the responsibility of the Office of Risk Management*. No special back-up disk drives may be created outside the standard Disaster Recovery retention process without written authorization from the Office of Risk Management. The Office of Risk Management must inform University Legal Counsel of any such action in writing (paper or email). Special back-up disk drives created for litigation preservation purposes override standard Disaster Recovery retention practices regarding back-up tape disposal and will be retained until ordered destroyed by the Office of Risk Management.

1.7.3.3.3. **Compliance retention** of electronically stored information is conducted by creating electronic archival copies of certain data files or databases, such as year-end financials, that must be kept for a prescribed period of time. These files are stored electronically until such time as they are deleted by the data owner (once past the required compliance retention period). As such, electronically stored information retained for compliance purposes is also retained on the Disaster Recovery backups and would therefore be available for the length of the Disaster Recovery retention period even after deleted

from the computer at the end of the Compliance Retention period. *Compliance retention is the responsibility of the individual functional departments responsible for the data in question and as such the retention period is determined and documented by the respective departments in their individual departmental documentation*.

1.7.4. Procedure

1.7.4.1. Backup disk drives maintained offsite in the Iron Mountain database via data synchronization.

1.7.4.2. Special disk drives created for litigation preservation purposes will be stored in offsite in the Iron Mountain database via data synchronization.