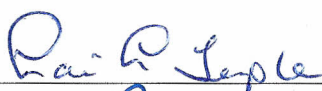




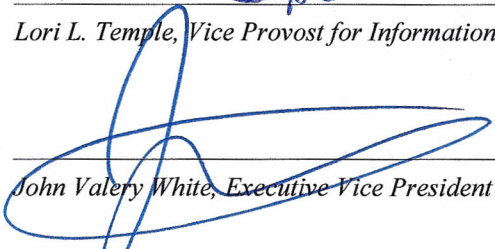
OFFICE OF INFORMATION TECHNOLOGY

COMPUTER MANAGEMENT POLICY

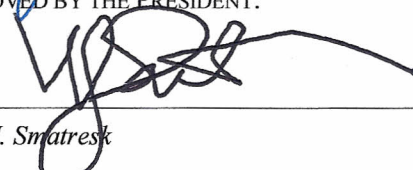
RESPONSIBLE ADMINISTRATOR: VICE PROVOST FOR INFORMATION TECHNOLOGY
RESPONSIBLE OFFICE(S): OFFICE OF THE VICE PROVOST FOR INFORMATION TECHNOLOGY
ORIGINALLY ISSUED:
APPROVALS:

APPROVED BY:


Lori L. Temple, Vice Provost for Information Technology 11/13/12
Date



John Valery White, Executive Vice President & Provost 11/14/12
Date

APPROVED BY THE PRESIDENT:


Neal J. Smatresk 11/19/12
Date

REVISION DATE: NA

STATEMENT OF PURPOSE

The purpose of this policy is to:

- Facilitate centralized desktop administration.
- Assist with maintaining desktop software licensing compliance.
- Ensure all computers meet minimum security requirements.

ENTITIES AFFECTED BY THIS POLICY

Entities affected by this policy include UNLV employees.

WHO SHOULD READ THIS POLICY

UNLV employees who use a university-issued computer should read this policy.

POLICY

All university-issued computers will be connected to a centralized computer management system.

Refer to the Office of Information Technology's Policies and Procedures web page at <https://www.it.unlv.edu/policies> for additional information, including how to request an exception to this policy.

RELATED DOCUMENTS

Not applicable.

CONTACTS

Refer to the Office of Information Technology's Policies and Procedures web page at <https://www.it.unlv.edu/policies> for a list of individuals who can answer questions about the policy.

DEFINITIONS

Centralized computer management - The management of university-owned computers remotely. Automates regular computer support activities such as deploying critical security updates for operating systems and applications; installing software; and tracking inventory for each connected computer.

Computer – Any university-issued desktop or laptop listed as property of UNLV/NSHE on the university inventory list, regardless of whether the desktop or laptop is properly labeled or tagged as such.

Minimum security requirements – Computer system is kept updated to current OIT-approved levels and anti-virus software is installed, active, and using the most current virus definitions.