UNLV

OFFICE OF INFORMATION TECHNOLOGY

NETWORK ACCESS COMPLIANCE POLICY

RESPONSIBLE ADMINISTRATOR:	VICE PROVOST FOR INFORMATION TECHNOLOGY
RESPONSIBLE OFFICE(S):	OFFICE OF THE VICE PROVOST FOR INFORMATION TECHNOLOGY
ORIGINALLY ISSUED:	JULY 2012
APPROVALS:	APPROVED BY:

7/31/12

Lori L. Temple, Vice Provost for Information Technology *Date*

APPROVED BY:

7/31/12

John Valery White, Executive Vice President & Provost *Date*

APPROVED BY THE PRESIDENT:

8/1/12

Neal J. Smatresk *Date*

REVISION DATE: NA

STATEMENT OF PURPOSE

The purpose of this policy is to:

- Create a secure network environment for UNLV's computer and network resources by establishing different levels of network access to meet the needs of UNLV staff and students as well as the general public.

- Ensure UNLV is in compliance with the Nevada System of Higher Education (NSHE) guidelines and network security best practices.

ENTITIES AFFECTED BY THIS POLICY

Entities affected by this policy include UNLV students and employees and anyone who accesses the UNLV network.

WHO SHOULD READ THIS POLICY

UNLV students and employees and anyone who accesses the UNLV network should read this policy.

POLICY

The UNLV network is divided into publicly accessible and non-publicly accessible areas. Systems may be placed on the UNLV network only in consultation with and with the approval of the Office of Information Technology (OIT). Systems in the non-publicly accessible areas of the network can be accessed only through methods approved by OIT.

Refer to the Office of Information Technology's Policies and Procedures web page at http://oit.unlv.edu/about-oit/policies for additional information and contact information for questions about the policy.

RELATED DOCUMENTS

Nevada System of Higher Education Procedures and Guidelines Manual, Chapter 14: Data and Information Security, Sections 2.1 and 3.3
http://system.nevada.edu/tasks/sites/Nshe/assets/File/BoardOfRegents/Procedures/P&GM%20CH14%20-%20DATA%20AND%20INFORMATION%20SECURITY.pdf

Guidelines on Firewalls and Firewall Policy
http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

Guides to Enterprise Telework and Remote Access Security
http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf

CONTACTS

Refer to the Office of Information Technology's Policies and Procedures web page at http://oit.unlv.edu/about-oit/policies for a list of individuals who can answer questions about the policy.

DEFINITIONS

These definitions apply to these terms as they are used in this policy.

Network – An underlying infrastructure of cabling, equipment, and management software that electronically transmits and directs the flow of information among devices.

Non-publicly accessible - Campus network resources available to only those who have been authorized to have access.

Publicly accessible - Campus network resources available to the general public.

Systems - Devices and applications accessed via the network.