University of New Mexico ± Gallup

Information Technology Services

Security Practices

20 August 2010

This document is required by University Business Practices UBP 2520 ªComputer Security Controls and Guidelinesº Sec 1 ªGeneralº which states:

> "Therefore, all departments operating University owned computers, including those operated by faculty, staff, and students, must develop departmental security practices which comply with the security practices listed below." See UBP 2520 "Computer Security Controls and Guidelines" Sec 2 "Security Practices".

The intent of this document is to supplement and expand on UBP policy. If anything in this document conflicts with UBP, UBP shall take precedence.

1. General

Department heads are responsible for computer security awareness and for ensuring reasonable protection of departmental computing systems against breaches of security, through methods such as virus protection and password usage. Department heads should ensure users of their system users have the necessary training for appropriate use of the system. A portion of available resources is listed at http://its.unm.edu/training/ and http://www.gallup.unm.edu/HOWTO/. Prior to gaining access to UNM - Gallup computing resources, all users must sign a Computer Use Agreement (Exhibit A.), which the Human Resources (HR) department and Information

2.2. Administrative Account Passwords

Due the the special nature of administrative computer accounts; ITS will ensure that all administrative

UNM Policy 2030, ªSocial Security Numbersº,
UNM Policy 7215, ªCredit Card Processingº,
UNM Policy 4610, ªAcquisition and Disposition of UNM Surplus Equipmentº,
New Mexico Inspection of Public Records Act, and
University policies found in the Regents Policy Manual, in the Faculty Handbook, Student Pathfinder, the University Business Policies and Procedures Manual, and all UNM - Gallup data handling policies and standards and procedures.

It is the responsibility of each user of UNM data to ensure that data in their position is properly handled when stored or in transit by the use of appropriate security measures for example password protection, encrypted or both. See the UNM Data Classification Standard
http://cio.unm.edu/standards/DataClassificationStandard041608.pdf

2.7. Virus Protection

Virus detection and elimination software is essential to protect University data and systems. All UNM owned computers shall have approved virus protection software installed and working at all times. It is the responsibility of all users to inform IT Services if they have reason to believe that the system they are using does not have approved anti-virus software installed or that they believe the software is not functioning properly or has not been recently updated.

It is the responsibility of UNM - Gallup IT Services to provide and install working anti-virus software on any UNM - Gallup computer they are aware of that does not satisfy the above anti-virus software requirement.

2.8. System Backups

Data backup is one of the primary methods ensuring that UNM - Gallup operational data is preserved in the event of a disaster, equipment failure of human error. It is the responsibility of each individual computer user to ensure that their electronic operational data is preserved by copying that data to the networked storage server provided by ITS. This data must be copied frequently enough to ensure minimal data loss in the event of a problem on their system.

It is the responsibility of ITS to ensure that all servers including storage servers are backed up on a regular basis and to ensure minimal data loss in the event of a problem with the server.

It is the responsibility of ITS to implement and maintain the systems and communications paths necessary to execute UNM - Gallup procedures for off-site storage of electronic operational data and for Disaster recovery.

2.9. Security Violations

Users shall not:

attempt to defeat or circumvent any security measures, controls, accounts, or record-keeping systems;

use computing services to gain unauthorized access to UNM©s or anyone else's computing services;

intentionally alter, misappropriate, dismantle, disfiguring, disable or destroy any computing information and/or services;

knowingly distribute or launch computer viruses, worms, Trojans, or other rogue programs, or

physically or electrically attach any additional device (such as a printer, modem, wireless access point, or video system) to a University communications device, or network connection without specific pre-authorization.

2.10. Security Violation Handling

Department heads should detect and correct any non-compliance with this and other University, including UNM - Gallup, computer policies or practices. If they detect serious security violations they should report their findings to UNM - Gallup Police. All investigations should follow proper investigative procedures to ensure confidentiality and due process. Any employee who detects or suspects non-compliance should report such conduct to the department head. Misconduct should be reported in accordance with "Reporting

Misconduct and Retaliation" Policy 2200, UBP.

3.0 Sanctions

Use of University, including UNM - Gallup, computing services in violation of applicable laws or University policy or practices may result in sanctions, including withdrawal of use privilege such as detaching from the network; disciplinary action, up to and including, expulsion from the University or discharge from a position; and legal prosecution under applicable federal and/or state law.

4. Attachments

Exhibit A. - UNM - Gallup Computer Use Access Agreement

University of New Mexico - Gallup
Computer Use Agreement

20 August 2010

I am requesting an active directory account on a computer system operated by Information Technology Services (ITS), a department of the University of New Mexico - Gallup (UNM-G). By accepting this account, I affirm that I have read and will abide by UNM-G's Acceptable Computer Use Policy, in particular:

1. I will be responsible for all use of this computer account.
2. I will not use the computer account for commercial purposes.
3. I will not use the computer account to engage in any form of illegal software copying or other copyright infringement.
4. I will not attempt to access accounts, files or information belonging to other users without their knowledge and consent.
5. I will not willfully use my computer account to harass other computer users.
6. I will not use the computer account in such a way as to violate state or federal law or UNM or UNM-G policy.

FAILURE TO COMPLY WITH THESE RULES WILL RESULT IN SANCTIONS, INCLUDING REMOVAL OF ACCOUNT AND DISCIPLINARY ACTION, AND MAY SUBJECT YOU TO CRIMINAL PENALTIES.

Return to: Human Resources, University of New Mexico - Gallup 200 College Rd, Gallup NM 87301. Phone: (505) 863-7538

Employee

Signature: ____________________________________ Date: __________________________

Print Name: ___________________________________

Department: ___________________________ Phone: ________________________________

I am (check one): __ Faculty __ Staff __ Adjunct __ Visiting Faculty

__ Other. Specify: ____

OFFICE USE ONLY

Employment __ Verification Signature (HR)