University of New Mexico – Gallup
Information Technology Services
Security Practices
20 August 2010

This document is required by University Business Practices UBP 2520 “Computer Security Controls and Guidelines” Sec 1 “General” 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 Technology Services (ITS) department keep on file. Department heads are responsible for ensuring that all users with current access to UNM - Gallup computing resources have a signed Computer Use Agreement on file with HR and ITS.

2.0. Access Control

2.1. User Account Passwords

Passwords authenticate the user's identity and match the user to the privileges granted on UNM - Gallup computer networks and systems. A password is a security measure designed to prevent unauthorized persons from logging on with another person's computer account and reading or changing data accessible to that user. Users should create passwords carefully and handle them with care and attention. For this security feature to be effective the user must protect the secrecy of his/her password. Each user should:

- change their password regularly and at any time the user feels the password may have been compromised;
- avoid writing the password down;
- not disclose or share the password with anyone including ITS personnel;
- not ask anyone for their password;
- choose a password that is easy to remember but hard to guess, and
- do not allow another person to use your account.

ITS requires users to change their user account passwords at least once every 180 days. Users can not repeat passwords and all passwords are required to satisfy the following requirements:

- passwords must contain a minimum of 8 characters, and
- must contain characters from at least three (3) of the following four (4) character sets:
  - Numbers: 0, 1, 2, ...
  - Uppercase letters: A, B, C, ...
  - Lowercase letters: a, b, c, ...
  - Special characters: ~ ! @ # $ % ^ & * ( ) _ + ` - = { } | [ ] : ; < > ? , .

2.2. Administrative Account Passwords

Due the the special nature of administrative computer accounts; ITS will ensure that all administrative account passwords are changed at lease every 90 days. See section 2.1 "User Account Passwords" for additional information about individual user responsibilities and password requirements.

2.3. User Account Access

User accounts shall grant access to computers, systems, networks, and data based on the role of the user. ITS personnel shall modify user access accordingly within 48 hours of being notified of a users change in role. In the event of separation from UNM employment or affiliation, the user account will be deleted within 48 hours of notification by HR. In the event of account deletion, all user data stored on UNM - Gallup storage and email servers will be archived for a period of 6 months unless otherwise notified by UNM - Gallup or UNM administration.

2.4. User Account Locking

As the first level of intervention, and to protect the UNM's computer systems and resources, as well as personal and administrative data, ITS will lock UNM - Gallup user accounts for the following reasons:

compromised or stolen account
compromised password
misuse/abuse of system or network resources (third event)
harassment
violations of UNM - Gallup's Acceptable Computer Use policy
BSA or manager/supervisor request
department/organization account violations
attempts to defeat IT security
multiple or varied off-site logins
delinquent pay-for-use accounts
post-reinstatement violations

ITS reserves the right to lock UNM - Gallup computer accounts, and to require violators undergo education and training on the proper use of their accounts. In addition, ITS will provide violators with a copy of UNM - Gallup's Acceptable Computer Use policy in either electronic or hard copy form. Certain locking violations could also result in disciplinary action by the University or in criminal prosecution.

2.5. Password Protection For Unattended Computers

It is the responsibility of each computer user to ensure that they do not leave a computer accessible to others while unattended. If the user is through using the computers they should log off. If they are not through, they should "lock the computer" to prevent unauthorized access in their absence. The locking process should require the use of their user account password to gain access.

ITS will force all non-shared computers to lock after 1 hour of inactivity and will force a log off for all shared computers after 10 minutes of inactivity.

2.6. Access to and Protection of Information

Each user of UNM data must take appropriate measures to ensure privacy and confidentiality of data in accordance with applicable laws and policies such as but, not limited to:

UNM Student Records Policy
Family Educational Rights and Privacy Act of 1974
Department of Health and Human Services, Health Information Privacy,
UNM Policy 7200, "Cash Management",
UNM Policy 2040, "Identity Theft Prevention Program",

UNM Policy 2030, “Social Security Numbers”,
UNM Policy 7215, “Credit Card Processing”,
UNM Policy 4610, “Acquisition and Disposition of UNM Surplus Equipment”,
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): _____ Date:_____

Account Name Assigned (ITS): _____ Date:_____

Employment Termination Signature (HR): _____ Date:_____

Account Removal Signature (ITS): _____ Date:_____