Approval Signatures:

Authorizing Agent and Sponsor

Norma Grijalva
(Signature)

6/19/2018
(Date)

Name: Norma Grijalva

Position: CIO/AVP Information Technology

Organization: New Mexico State University in a role as CIO

Oversight and Enforcement Responsibility

(Signature)

6-19-2018
(Date)

Name: Carlos S. Lobato

Position: IT Compliance Officer

Organization: New Mexico State University in a role as Chief Privacy Officer

System-wide Governing Review and Approval

(Daniel Howard)

(Signature)

06/21/18
(Date)

Name: Daniel Howard

Position: Executive Vice President and Provost

Organization: New Mexico State University in a role as NMSU’s IT Governance Council Chair

Endorsed by: ICT Leadership Team

Endorsed by: IT Governance Council
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged Account Management Standards</td>
<td>4</td>
</tr>
<tr>
<td><strong>Overview</strong></td>
<td></td>
</tr>
<tr>
<td>Administrative Standards</td>
<td>4</td>
</tr>
<tr>
<td><em>Background checks for IT Administrators</em></td>
<td></td>
</tr>
<tr>
<td><em>Non-Disclosure Agreement</em></td>
<td></td>
</tr>
<tr>
<td><em>On/Off Boarding for IT Administrators</em></td>
<td>5</td>
</tr>
<tr>
<td><em>On/Off Boarding for ICT Administrators</em></td>
<td>5</td>
</tr>
<tr>
<td><em>Training</em></td>
<td></td>
</tr>
<tr>
<td>Technical Standards</td>
<td>6</td>
</tr>
<tr>
<td><em>Account Inventory for IT Administrators</em></td>
<td></td>
</tr>
<tr>
<td><em>Account Inventory for ICT Administrators</em></td>
<td></td>
</tr>
<tr>
<td><em>Accounts</em></td>
<td></td>
</tr>
<tr>
<td><em>Logs to Track Account Usage</em></td>
<td>8</td>
</tr>
<tr>
<td><em>Password Management for IT Administrator Accounts</em></td>
<td></td>
</tr>
<tr>
<td>Oversight Responsibility and Maintenance</td>
<td>9</td>
</tr>
<tr>
<td>Definitions</td>
<td>9</td>
</tr>
<tr>
<td>References</td>
<td>10</td>
</tr>
</tbody>
</table>
Privileged Account Management Standards

Overview

New Mexico State University's (NMSU's) Office of the Chief Information Officer (CIO) and managers of the Information & Communication Technologies (ICT) department have developed these standards intended to establish consistent and effective privileged account management procedures for the institution that promote the security, integrity, availability, and the confidentiality of university information systems that contain, process, or transmit data. This manual was reviewed by the IT Governance Committee to ensure that the NMSU standards for access through ICT resources comply with university policies.

Access to NMSU’s information systems and protected information may be provided only to those needing specific access to accomplish an authorized task and must be based on the principles of need-to-know, least-privilege best practices, and best information security application development standards. Authorization and authentication controls must be implemented for access to university information systems and protected data.

System owners must have documented processes for provisioning approved additions, changes, and terminations of access rights and reviewing access of existing account holders that complies with these standards. Access to campus information systems and protected information must be denied until specifically authorized by proper authorities.

NMSU takes safeguarding of its information systems and regulated entrusted information seriously. IT directors and managers directly responsible for administering information technology infrastructure at NMSU must operate according to the required standards outlined below.

Administrative Standards

Background checks for IT Administrators

Appropriate background checks by Human Resources (HR) are required for all IT employees. Background checks are required for student employees who need access to PSL, NMSU Police department or at the discretion of the hiring manager.

Non-Disclosure Agreement

All IT employees including student employees are required to fill out the NMSU Non-Disclosure Agreement (https://www.nmsu.edu/legal/nondisc.html) with annual renewals. The completed annual form will be filed in the employee’s personnel file.

This Non-Disclosure Agreement defines the responsibilities of those employees who have access to NMSU records containing sensitive or confidential data about NMSU students, employees, donors, or other affiliates. By signing this agreement, the employee acknowledges and accepts responsibility.

As part of performing IT duties, IT employees have access to technical sensitive information, and therefore are required to complete a Non-Disclosure Agreement as part of the on-boarding and off-boarding process. Departments may also have additional non-disclosure forms for other types of sensitive data.
On/Off Boarding for IT Administrators

An on/off boarding template must be completed by a supervisor for each new IT employee. Each department will work with their HR liaison to complete their template. Additional on/off boarding tasks not included in the template will be determined by each department. A blank template along with instructions can be found under ICT's website labeled “Standards and Guidelines” - (https://ict.nmsu.edu/standards-and-guidelines/).

On/Off Boarding for ICT Administrators

An on/off boarding template established by both the HR liaison in the CIO office and the ICT managers will be followed. The template will be completed by the HR liaison and kept in the employee’s personnel file. Additional on/off boarding tasks not included in the template will be completed by each ICT unit. The manager of each unit will keep a list of any items they need completed as part of their on/off boarding procedures. These templates will be used as a guide to provide directors/managers and the CIO HR liaison the information needed to add or remove account privileges from the employee. The account credentials are either removed or changed following an employee’s employment status.

Frequency of review:
The completed on/off boarding template will be kept in a secure location by the CIO HR liaison’s office. Any additional lists of items will be kept by the manager/director of the ICT sub-unit. All lists will be reviewed on an annual basis by the IT Compliance Officer or as part of an audit by the Office of Audit Service or by the IT independent auditor.

Training

Before a new employee is granted access to administer an NMSU IT infrastructure service, they must complete the required compliance training as part of their new employee orientation. It will be the supervisor’s (i.e., manager/director) responsibility to assure the employee’s compliance training has been completed before providing an IT administrator account.

It is the responsibility of the employee’s supervisor to record and describe the reason of the employee’s need for access to an administrator account. This must be recorded on the employee’s on/off boarding form.

All IT Administrators are required as part of the onboarding process to complete the IT Administrators training relating to effective management of Privileged Accounts for System, Application, Database, and Network Administration. It will be the supervisor’s responsibility to ensure the employees under their direct supervision complete this training with annual refreshers. This training module is available at the Center for Learning & Professional Development training central website as part of the computing & web training (https://training.nmsu.edu/).
Technical Standards

Account Inventory for IT Administrators
IT units at NMSU shall use a standard Excel password encrypted template or other equivalent password acceptable product to log all account inventory to include a set of standard attributes as defined by the ICT IT managers in collaboration with the IT Compliance Officer. The template will be reviewed annually.

Account Inventory for ICT Administrators
ICT keeps a file known as “Account Inventory.” The ICT director/manager may add additional attributes as appropriate to the unit, but must complete the attributes required by the template for each account. The IT director/manager is responsible for ensuring proper account inventory. A blank template along with instructions can be found under ICT’s website labeled “Standards and Guidelines” - (https://ict.nmsu.edu/standards-and-guidelines/).

Process:
For IT business continuity, each IT unit will keep the account inventory file, with all account attributes and passwords, in a secure restricted folder location on the NMSU’s network. Both the inventory file and password file will be stored in the same location with a different password encryption for each. The account credentials are either removed or changed following an employee’s employment status.

Frequency of review:
Each quarter a meeting is called by the IT Compliance Officer to include all ICT managers to review the “IT Privileged Access Management Manual”, account review process and discuss any account structure that may need updates.

Team Members:
ICT directors/managers, Project Manager, and IT Compliance Officer.

Accounts
IT departments may have a variation of accounts they track using the account inventory template, and to ensure IT business continuity, each account must have an alternate/secondary designated account administrator. Account credentials should not contain the administrator’s NMSU username and password. The exception to using the user’s NMSU username exists when there are valid technical limitations within the system in which case a Risk Acceptance Form (RAF - https://ict.nmsu.edu/files/2016/05/Risk-Acceptance-Form-RAF-05232016.pdf) must be completed. Anytime this occurs, it should be noted in the account inventory file. The standard account details include the following:

- account name
- account types
- service account or administrator account
- product name
- environment (DEV, TEST, PROD, OTHER)
- who creates the account
- account administrator
- alternate designated account holder
• who is notified on account changes
• expiration (automated or manual)
  o Any accounts that do not have an automated notification of password expiration must be monitored by the IT administrator of the account. It will be the responsibility of the IT administrator to let the alternate know the password needs to be changed or has been changed.
• complexity meets NMSU Password Standard for Privileged Accounts (automated or manual)
• date of last password change
• location noted for the instructions on how to change the password and account access

A blank account inventory template along with instructions can be found under ICT's website labeled “Standards and Guidelines” - (https://ict.nmsu.edu/standards-and-guidelines/).

Service accounts:
All service accounts should be administered according to NMSU Privileged User Account Password Standard (https://ict.nmsu.edu/files/2018/06/NMSU-Privileged-User-Account-Password-Standard-06192018.pdf).

Administrator accounts:
Administrator (admin) accounts are authorized to have the minimum privileges necessary to control, monitor, or administer the system, including security functions that ordinary users are not authorized to perform. Each admin account is created using a set of credentials established by the administrator. The password is stored in the password inventory template (see Password Management for IT Administrator Accounts section).

An administrator account may use their NMSU username as an exception when they need to elevate their temporary privileges via SUDO “super userdo” - a Linux command that allows programs and commands to be executed as a super user. The credentials for SUDO must meet or exceed the standards for privileged accounts. Anytime this occurs, it is noted in the account inventory file. All passwords for admin accounts follow the standards outlined in the NMSU Privileged User Account Password Standard (https://ict.nmsu.edu/files/2018/06/NMSU-Privileged-User-Account-Password-Standard-06192018.pdf).

Shared accounts:
There are systems that only allow for the creation of one main administrator account to administer the system, service or application. These accounts must be shared with more than one IT Administrator in order to ensure NMSU’s IT Business Continuity. These privileged accounts are commonly known as “shared accounts” and must clearly identify a primary and an alternate designated account administrator. All account information is kept in the account inventory file with clearly identifying the administrator and alternate. All passwords for shared accounts follow the standards outlined in the NMSU Password Standard for Privileged Accounts System.

Vendor accounts:
These accounts are created for vendors who need to log into a system to help install, troubleshoot or perform health checks. The users of these accounts are asked to fill out the Vendor Account Request Form and VPN Firewall Bypass Access Form. The user of the vendor account is required to follow the NMSU Password Standard for Privileged Accounts by acknowledging it on the Vendor Account request form. All accounts are reviewed twice yearly to extend or remove privileges.
Student accounts:
Accounts are created based on the job responsibilities for each ICT sub-unit. A non-disclosure form is signed when each student is hired for ICT and kept in their personnel file. The student is required to comply with the NMSU Password Standard for Privileged Accounts System by acknowledging it on their onboarding form.

Logs to Track Account Usage
The use of all accounts is logged based on the system they are tied to. They keep track of what the account is doing and in some cases have details as to what the account accessed and what modifications it made. Record at least the following audit trail entries for all system components for each event unless technical limitations exist, which must be documented via the completion of a RAF:

Log file must include at minimum in the log entries:
- user identification
- type of events
- date and time stamp
- login success or failure indication
- origination of event such as source IP or MAC address
- identity or name of affected data, system component, or other resources

The recording of these audit details will help to validate or negate a potential compromise and will provide detail to know who, what, where, when, and how of an event.

It is the responsibility of each IT administrator/manager to ensure logs of their accounts is occurring and being reviewed on a quarterly basis. All non-IT administrator accounts need to be monitored and reviewed by the IT administrator of that account. All IT administrator accounts activity should be sent to the Information Security team and kept in NMSU’s security information event management system (SIEM), monitored and reviewed by an Information Security Administrator regularly but at minimum on a quarterly basis. Logs should be regularly sent (continuous, daily, weekly, months, etc.) as a file tape, or other method as agreed by the IT administrator and Information Security team.

Each IT unit should review their logs to identify anomalies or suspicious activity and ensure that:

- Audit trails are viewed only by positions with job-related need
- Audit trail files are protected from unauthorized modifications
- Audit trail files are promptly backed up to media that is difficult to alter
- File-integrity monitoring software exist to monitor logs to ensure that existing log data cannot be changed without generating alerts

Regular reviews but at minimum quarterly reviews will need to be performed by the IT administrator. All reviews must be documented by email or kept on a spreadsheet that documents when the review took place. The IT Auditor may ask for the documented reviews on an ad-hoc basis.

Password Management for IT Administrator Accounts
All IT units must keep a master list of all passwords for their account inventory. The file must be encrypted and follow NMSU’s Password Standard for Privileged Accounts. All files must be kept on a NMSU local shared drive that is regularly backed-up and access restricted.
Each manager within each IT unit will complete the password inventory template and turn it in to the CIO office in a sealed envelope to include their signature and department on the outside of the envelope. The CIO office will log when the envelope was turned in to include who turned it in, department, date, and time. The person also receiving the sealed envelope will sign and date the envelope. The CIO office will then inform the IT Compliance Officer and Manager of Enterprise Computer Operations of the received envelope(s) and these individuals will take the envelope(s) to an off-site vault.

**Frequency of review:**
Each quarter the IT Compliance Officer will perform an ad-hoc audit to verify the information on the password inventory template. ICT unit managers will update their password to the password inventory file each time a manager leaves their position within ICT.

A password inventory blank template along with instructions can be found under ICT’s website labeled “Standards and Guidelines” - (https://ict.nmsu.edu/standards-and-guidelines/).

**Oversight Responsibility and Maintenance**
The Office of the CIO has the ultimate responsibility to enforce these standards via NMSU's IT Compliance Officer. NMSU's IT Project Manager will work collaboratively with the IT Compliance Officer and IT managers to maintain and update the manual as needed. This manual will be considered a living document to ensure it properly portrays the actual management practices of IT departments at NMSU. Employees and the department are required to comply with the policies set forth by the Administrative Rules and Procedures (ARP) section located at https://arp.nmsu.edu/10-10/.

**Definitions**

**Account Credentials** - the authorization, authentication, and account used to access NMSU data.

**Account Privileges** – the right to perform a particular type of work, usually on system data. Typically the work is usually on critical information systems involving the control, monitoring, or administration of the system, including security functions.

**Application Development Standards** – provides a methodical approach to solving business and information technology problems and a means of managing, accessing, directing, monitoring and controlling the process of application/software.

**Data** – factual information that is collected, stored, processed, and can be used to make business or system decisions.

**IT Administrators** - is a person who supports a multi-user computing environment and ensures continuous optimal performance of IT services, security parameters, and supports and maintains IT infrastructure on behalf of NMSU.

**IT Infrastructure** - refers to NMSU’s technological components related to but not limited to, Systems, Network, Databases, Applications, Device Management or other services.
**IT Unit** - refers to an IT area (centralized or decentralized) within NMSU that is responsible for administering information technology, which is part of NMSU’s IT infrastructures such as Systems, Network, Databases, Applications, Device Management or other required services.

**Least Privilege** – the principle of least privilege (POLP) is the practice of limiting access rights for users and/or accounts with the bare minimum permissions they need to perform their work.

**Non-IT administrator** – is someone who is considered a normal end user of a system or application. This end user is granted access via the completion of an access request form with supervisor's approval.

**Privileged Account Management** - managing and auditing account and data access by privileged users.

**Privileged user** - someone who has administrative access to critical systems or to a vast amount of confidential data with edit privileges. For instance, anyone who can set up and delete user accounts and roles on your Oracle database is a privileged user.

**SUDO "super userdo"** - a Linux command that allows programs and commands to be executed as a super user (aka root user) or another user.

---

**References**


Administrative Rules and Procedures (ARP) - [https://arp.nmsu.edu/chapter-15/](https://arp.nmsu.edu/chapter-15/)

Non-Disclosure Agreement - [https://www.nmsu.edu/legal/nondisc.html](https://www.nmsu.edu/legal/nondisc.html)