Policy Statement

The University shall develop, implement, and regularly review a formal, documented process for appropriately creating, modifying and safeguarding passwords used to validate a user’s identity and establish access to the University’s information systems and data.

Purpose of Policy

The purpose of this policy is to establish guidance regarding the creation and management of OU accounts, including but not limited to the OUNetID in order to protect the security of the network, protect data integrity, and protect information systems.

Web Address for this Policy

http://www.ou.edu/content/ouit/security/compliance.html

Scope

This policy establishes the account requirements for any person using an OU account at any time or location to access OU systems. This includes all students, faculty, staff, alumni, retirees, continuing and distance education students, and other University affiliates. These accounts should not be used for system administration or having access to administrative tools, management interfaces, and systems that access regulated or restricted data or affect their security.

The OUNetID account is a User ID and password combination that serves as the primary digital identity at the University of Oklahoma. The OUNetID account provides access to a wide range of OU Internet services such as the Web, e-mail, library resources, employee records, student records, research services, and student computing labs. Individuals may need additional University accounts for specialized services and these accounts must comply with the policy.

Policy
PASSWORD GUIDELINES

- Passwords will expire 365 days from the date of the last change.
- Passwords must be at least 8 characters
- Passwords between 8-15 characters must contain a combination of upper and lowercase letters and at least one number or symbol.
- Passwords or passphrases 16 characters or more do not have a complexity requirement.
- Passwords must not be the same as the user ID
- Passwords must be different than the last 5 passwords used.

INDIVIDUAL RESPONSIBILITY

- Users must have their own unique individual account. To ensure proof of authorship, an account cannot have more than one human user.
- Users must create and change their own passwords. However, password resets and account initializations are an exception discussed below in OU IT responsibility.
- Create a strong password.
- Change the password if the account is known to be compromised.
- Reserve any OU Account User ID and password for OU systems and services only. Individuals should create a different username and password for external services such as stores, banks, music services, Web sites, personally owned computers, or other systems.
- Users must never share their password or answers to their security questions with anyone else, even with IT.
- OU IT Staff should never have a valid reason to ask a user for their password.
- A human should not send passwords in clear text such as email, social media, instant messaging, etc. except as outlined in the password initialization and reset process below.

IT RESPONSIBILITY

- The password initialization and reset process must be a one-time use, auto-generated random password (sent separately from the username if sent in plain text) that may only be used for systems that require an immediate first login password change by the user.
- Systems must detect and limit repeated failed access attempts by locking out the account after 50 attempts (the maximum number of failed login attempts).
- Systems must enforce a minimum lockout duration of 30 minutes or until an administrator unlocks the account.
- Systems must detect and disable or remove end user accounts left inactive for 365 days.
- Systems must never display passwords in their entirety in clear text except from a password reset message or from within a password vault.
• Password storage mechanisms must be encrypted or hashed (a process of mapping data of an arbitrary size to data of a fixed size, thus providing a layer of security) and have strict access permission.
• Systems must log all successful and unsuccessful login attempts.
• Authentication logs must be sent to a central log repository that can be monitored by staff.
• System log monitoring must send alerts to system administrators if the maximum number of login attempts is reached.
• Passwords must be changed when there is indication of possible system or account compromise. If an account owner is unresponsive the account may be disabled.
• Directory Services must detect and disable or remove any non-local accounts left inactive for a period of time determined.

**ENFORCEMENT**

This policy is authorized and approved by the Security Governance Executive Council. The University’s Internal Auditing department is responsible for monitoring and enforcement of this policy. This policy will be reviewed every 3 years or as needed.

**REVIZIONS AND APPROVALS**

**REVIZIONS**

<table>
<thead>
<tr>
<th>Revision Date</th>
<th>Version</th>
<th>Revised By</th>
<th>Changes made</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/5/2016</td>
<td>1.0</td>
<td>Anna Biggers</td>
<td>Creation</td>
</tr>
<tr>
<td>8/31/2016</td>
<td>1.0</td>
<td>Anna Biggers/Caleb Muckala</td>
<td>SGAC and SGEC feedback and formatting</td>
</tr>
</tbody>
</table>

**APPROVALS**

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Approved By</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>8/31/2016</td>
<td>SGEC</td>
<td>CIO, OLC, AF, Provost</td>
</tr>
</tbody>
</table>

**REVIEW HISTORY**
<table>
<thead>
<tr>
<th>Version</th>
<th>Review Date</th>
<th>Reviewed By</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>