OU IT Password Policy

Policy ID:	400	Version:	2.0
Effective Date:	07/31/2020	Compliance Date:	07/31/2021

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.

The purpose of this policy is to establish guidance regarding the creation and management of OU accounts in order to protect the security of the network, protect data integrity, and protect information systems.

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.

The OU account is a User ID and password combination that serves as the primary digital identity at the University of Oklahoma. The OU 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.

This Policy applies to all Information System operators responsible for access management of Information Systems. This Policy focuses on requirements for systems and applications.

POLICY STATEMENTS

PR.AC-1-1 USER IDENTITY MANAGEMENT

The Office of Information Technology's (OU IT) Account Management processes address the creation and maintenance of the University accounts that distinguish one individual from another. University accounts will be created, and labeled accordingly, for individuals within the following categories:

A. **Student Accounts**
   (1) Student accounts will be created and maintained for prospective, admitted, or enrolled students, or those with an ongoing relationship with the University.
   (2) Student accounts will be uniquely associated with a specific individual.
   (3) 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.
   (4) Student accounts must be disabled in accordance with the *OU IT Access Control Standard.*

B. **Staff or Faculty Accounts**

(1) Staff or Faculty accounts may be created and maintained for staff, faculty, or residents with a full- or part-time appointment and individuals with Emeritus status.
(2) Staff or Faculty accounts will be uniquely associated with a specific individual.
(3) 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.
(4) Staff or Faculty accounts must be disabled in accordance with *OU IT Access Control Standard.*

C. Sponsored Accounts

(1) Sponsored accounts will be created and maintained for other individuals (e.g., vendors, visiting faculty, collaborative research partners, contractors) who are authorized to be onsite, and to use University Services and Facilities.
(2) Sponsored accounts will be uniquely associated with a specific individual.
(3) These accounts must not be permitted system administration permissions granting access to administrative tools, management interfaces, and systems that access regulated or restricted data or affect their security, without authorization from the Office of Information Technology.
(4) Sponsored accounts must be disabled in accordance with *OU IT Access Control Standard.*

D. Admin (Privileged) Accounts

(1) Admin accounts will be created and maintained for staff with an Information Technology job description, including staff out of OU IT and University Department Information Technology staff, that require extra privileges related to the management of a device or application.
(2) Admin accounts will be uniquely associated with a specific individual.
(3) These accounts must 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.
(4) Admin accounts must be disabled in accordance with the *OU IT Access Control Standard.*

E. Shared Accounts

(1) Shared accounts will be created and maintained only to support multiple users sharing the same identity. For example, these may be created when there is a need to share a set of resources or because a product implementation requires it.
(2) The use of Shared accounts is discouraged as it lacks accountability and the use of Shared accounts is prohibited for users accessing Category A, Category B, Category C, and Category D1 information.
(3) Shared accounts must be disabled in accordance with the *OU IT Access Control Standard.*

F. Service Accounts

(1) Service accounts will be created and maintained for Information Systems to authenticate to other systems or applications without any association to an individual.
(2) Service accounts should be created sparingly and the purpose for each must be documented.
(3) The use of Service accounts must be periodically reviewed.
(4) Service accounts must not be used by people to authenticate aside from initial testing.
(5) Service accounts with elevated privileges must be closely monitored for abuse.
(6) Service accounts must be disabled in accordance with the *OU IT Access Control Standard.*

G. Alumni Accounts

(1) Alumni accounts will be created for former students that have graduated or retired faculty or staff.
(2) Alumni accounts must be disabled in accordance with the *OU IT Access Control Standard.*

PR.AC-1-2 USER PASSWORD GUIDELINES

OU IT's Account Management processes address the enforcement of the University password guidelines that protect user accounts.

A. **Staff, Faculty, Sponsored,** and **Student** account types must inherit the OU Default Domain Password Policy that includes:
   - Passwords will expire three hundred and sixty-five (365) days from the date of the last change.
   - Passwords must be at least twelve (12) characters
   - Passwords must not contain commonly used dictionary words.
     Examples: Sooner, Boomer, Password, Qwerty.
   - Passwords must contain a combination of upper and lowercase letters and at least one number or symbol.
   - Passwords must not be the same as the user ID
   - Passwords must be different than the previous six (6) passwords used.

B. **Staff, Faculty, Sponsored,** and **Student** account types may submit an Exception Request to the OU IT at the numbers listed below, to opt-in to a shorter password length.

OUHSC IT Service Desk
servicedesk@ouhsc.edu
(405) 271-2203 or
Toll Free (888) 435-7486

OU-Tulsa IT Service Desk
ou.edu/tulsa/it/help
(918) 660-3550

OU-Norman IT Service Desk
needhelp.ou.edu
(405) 325-HELP (4357)

To be approved for the shorter password length, the account type must meet the following requirements:

- Passwords must be at least eight (8) characters.
- Passwords will expire ninety (90) days from the date of the last change.
- Passwords must not contain commonly used dictionary words.
  Examples: Sooner, Boomer, Password, Qwerty.
- Passwords must not be the same as the User ID.
- Passwords must be different than the previous six (6) passwords used.

C. **OU Admin** account types must inherit the OU Admin Account Password Policy that includes:
   - Passwords will expire three hundred and sixty-five (365) days from the date of the last change.
   - Passwords must be at least sixteen (16) characters
   - Passwords must not contain commonly used dictionary words.
     Examples: Sooner, Boomer, Password, Qwerty.
   - Passwords must not be the same as the user ID
   - Passwords must be different than the previous six (6) passwords used.

D. **Shared** account types must inherit the OU Shared Account Password Policy that includes**:**
   - Passwords will expire thirty (30) days from the date of the last change.

- Passwords must be at least eight (8) characters
- Passwords must not contain commonly used dictionary words.
  Examples: Sooner, Boomer, Password, Qwerty.
- Passwords must contain a combination of upper and lowercase letters and at least one number or symbol.
- Passwords must not be the same as the user ID
- Passwords must be different than the previous six (6) passwords used.

E. Service account types must inherit the OU Default Domain Password Policy that includes:

- Passwords must be changed every 365 days.
    - Except for service accounts that can only be invoked by a built-in privileged account; or
    - Except for service accounts that are already in use as of the effective date of this policy and where changing the password will result in an extended disruption of service, in which case, these accounts must be reported to IT GRC by sending an email to grc@ou.edu to request an exception.
- Passwords must be at least twelve (12) characters
- Passwords must not contain commonly used dictionary words.
  Examples: Sooner, Boomer, Password, Qwerty.
- Passwords must contain a combination of upper and lowercase letters and at least one number or symbol.
- Passwords must not be the same as the user ID
- Passwords must be different than the previous six (6) passwords used.

F. Alumni account types must inherit the OU Default Domain Password Policy that includes:

- Passwords will expire three hundred and sixty-five (365) days from the date of the last change.
- Passwords must be at least eight (8) characters
- Passwords must not contain commonly used dictionary words.
  Examples: Sooner, Boomer, Password, Qwerty.
- Passwords must contain a combination of upper and lowercase letters and at least one number or symbol.
- Passwords must not be the same as the user ID
- Passwords must be different than the last six (6) passwords used.

PR.AC-1-3 USER RESPONSIBILITIES

All users, regardless of account type must be aware of the following responsibilities:

(1) To function as an auditable credential and ensure non-repudiation, each account must be associated to a single unique (human) user.

(2) Create and change their own passwords. However, password resets and account initializations are an exception discussed below in PR.AC-1-4 INFORMATION TECHNOLOGY RESPONSIBILITIES.

(3) Successfully complete required annual required security and awareness training.

(4) Create a strong password.

(5) Change password immediately and contact the service desks below when there is a reason to believe a password has been improperly disclosed, accessed, or used by an unauthorized person.

OUHSC IT Service Desk
servicedesk@ouhsc.edu
(405) 271-2203 or
Toll Free (888) 435-7486

OU-Tulsa IT Service Desk
ou.edu/tulsa/it/help

(918) 660-3550

OU-Norman IT Service Desk
needhelp.ou.edu
(405) 325-HELP (4357)

(6) 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.
(7) Never share their password or answers to their security questions with anyone else, even with IT.
(8) OU IT Staff should never have a valid reason to ask a user for their password.
(9) Hunan users should never send passwords in clear text such as email, social media, instant messaging, etc. except as outlined in the password initialization and reset process below.
(10) Never leave a password in a location that can be readily obtained by another individual (e.g., writing a password on a note affixed to a monitor or underneath a keyboard);
(11) Not leave a computer/workstation without securing it (e.g., locking it, logging out); and
(12) Not access information within an Information System that is not related to current job responsibilities.

PR.AC-1-4 INFORMATION TECHNOLOGY RESPONSIBILITIES

Information System or Data Administrators are individuals with principal responsibility for the installation, configuration, security, and ongoing maintenance of Information Technology. S/he is responsible for safeguarding Information Technology, which includes, but is not limited to:

(1) Critical Information Systems permitting user access across public and untrusted networks must require Multi-Factor authentication in accordance with the *OU IT Access Control Standard.* A Critical Information System may include, but are not limited to:
  - Information Systems greater than $75,000 in value;
  - Storing greater than 500 Category A, C, D1, or E records; or
  - Information Systems unable to sustain an outage for greater than 48 hours.

(2) 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.
(3) Systems must detect and limit repeated failed access attempts by locking out the account after ten (10) attempts (the maximum number of failed login attempts).
(4) Systems must enforce a minimum lockout duration of fifteen (15) minutes or until an administrator unlocks the account.
(5) Systems must detect and disable or remove end user accounts left inactive for three hundred and sixty-five (365) days.
(6) Systems must never display passwords in their entirety in clear text, except from a password reset message or from within a password vault.
(7) 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.
(8) Systems must log all successful and unsuccessful login attempts.
(9) Authentication logs must be sent to a central log repository that can be monitored by staff.
(10) System log monitoring must send alerts to system administrators if the maximum number of login attempts is reached.
(11) 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.
(12) Directory Services must detect and disable or remove any non-local accounts left inactive for a period of three hundred and sixty-five (365) days.

REFERENCES

- General Data Protection Regulation (GDPR)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Payment Card Industry (PCI) Data Security Standards
- National Institute of Standards and Technology Special Publication 800-17, Controlled Unclassified Information
- Gramm-Leach-Bliley Act (GLBA)
- Family Education Rights and Protection Act (FERPA)

ASSOCIATED POLICIES AND STANDARDS

- 000: Information Protection Policy
- 000-01: Information Classification Standard
- 400-01: Access Control Standard

ENFORCEMENT AND COMPLIANCE

Failure to comply with this policy or other applicable laws, policies, and regulations may result in the limitation, suspension, or revocation of user privileges and may further subject the user to disciplinary action including, but not limited to, those outlined in the Student Code, Staff Handbook, Faculty Handbook, and applicable laws. This policy is enforced by the OU Chief Information Officer. Internal Audit, or other departments, may periodically assess compliance with this policy and may report violations to the Board of Regents. This policy will be reviewed every 2 years or as needed.

IT EXCEPTIONS

The CIO acknowledges that under rare circumstances certain cases will need to employ systems that are not compliant with this policy. Such instances must be documented using the IT Policy and Standards Exception Process by a Business or Process Owner owning the risk and approved in advance by an authorized IT Executive (an owner of the IT Policy that governs the policy/standard).

Table 1 Revision History

Revision Date	Version	Revised By	Changes Made
01/5/2016	1.0	Anna Biggers	Creation
08/31/2016	1.0	Anna Biggers/Caleb Muckala	SGAC and SGEC feedback and formatting
03/18/2020	2.0	OU IT System Security Governance, Risk, and Compliance Director	Added OU Account Types Added Option 1 and Option 2 password schemes
05/13/2020	2.0	OU IT System Security Governance, Risk, and Compliance Director	Revised, page 2, line 86 Admin Account minimum password length to 16 characters. Removed Admin Account complexity requirements from page 2, line 87. Added Service Account forced password expiration exception criteria to lines 113-118.
05/29/2020	2.0	OU IT System Security Governance, Risk, and Compliance Director	Lines 128-130, Added "Service accounts will be created and maintained for Information Systems to authenticate to other systems or applications without any association to an individual." Lines 94-97, Added "Admin accounts will be created and maintained for staff with an Information Technology job description, including staff out of the Office of Information Technology and University Department Information Technology staff, that require extra privileges related to the management of a device or application." Revised line 35 to "Student accounts will be created and maintained for prospective students, admitted students, students enrolled and attending the University, or those with an ongoing relationship with University." Revised line 37 to "These accounts should not be used for system administration, access to administrative tools or management interfaces of University systems that access regulated or restricted data or affect their security." Added "residents" to line 42. Revised line 44 to "These accounts should not be used for system administration, access to administrative tools or management interfaces of University systems that access regulated or restricted data or affect their security." Revised line 66 to include the ServiceDesk number at each campus. Revised the default domain policy and revised the opt-in policy to swap the requirements. Revised line 94 to "Shared accounts will be created and maintained only to support use-cases that require a single pair of credentials to authenticate multiple users."
07/14/2020	2.0	OU IT System Security Governance, Risk, and Compliance Director	Received ISRB approval of Policy with the criteria added to PR.AC-1-4 : "Critical Information Systems permitting user access across public and untrusted networks must require Multi-Factor authentication in accordance with the *OU IT Access Control Standard.* A Critical Information System may include, but are not limited to: (1) Information Systems greater than $75,000 in value; (2) Storing greater than 500 Category A, C, D1, or E records; or (3) Information Systems unable to sustain an outage for greater than 48 hours."

Table 2 Approval History

Version	Approval Date	Approved by:
1.0	8/31/2016	SGEC
2.0	07/14/2020	ISRB and SGAC

Table 3 Review History

Version	Review Date	Reviewed by:
0.2	03/10/2020	Security Governance Advisory Council (SGAC)
2.0	05/12/2020	OU Medicine Cyber Security and Risk Advisory Council (CSRAC)
2.0	05/12/2020	Information Security Review Board
2.0	05/29/2020	OU IT Access Management Subject Matter Experts Chris Jones, Kelsie Curtis, Chris Kobza, Chad Miller, Shad Steward, Justin Davis
2.0	07/14/2020	ISRB and SGAC