UNIVERSITY OF OKLAHOMA
Health Sciences Center
Information Technology
Security Standard

Account and Password Management

1. Purpose

The purpose of this Standard is to establish requirements for safeguarding user accounts and passwords that are used to access OUHSC Information Systems (IS). These safeguards are designed to protect the security of IS, network, and data from unauthorized access, disclosure or modification. They are necessary to comply with various legal and regulatory requirements, including but not limited to the Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), and the Payment Card Industry Security Standard (PCI DSS).

2. Standard

All IS users including faculty, staff, students, volunteers, contractors, vendors and others who are granted access to OUHSC IS must follow the account and password requirements defined in 2.1 through 2.4 below.

IS administrators must follow the relevant requirements defined in 2.5 through 2.6 below.

2.1 Individual User Responsibilities

- Passwords must be kept private and may not be shared with others[1].
- Users must agree to and comply with the Information System Acceptable Use policy.
- Users should report any suspicious computer account activity to the IT Service Desk immediately.

Recommendations and Best Practices for Users

- Do not respond to email or web links within an email message that ask for your user-id or password. (Cyber criminals use email addresses and web pages that appear to be legitimate to trick users into providing login credentials so the hackers can perform malicious activity on the user's account.)
- Do not use the same password for University accounts as for non-University accounts.
- Do not store your password in a web browser or similar unsecured application.
- Do not write your password down and leave it in a location easily accessible or visible to others.

2.2 User Password Requirements

- **User account passwords** must meet the requirements below:
  - Be at least eight characters long and no more than 26.
  - Contain characters from three of the following four categories:
    a. Uppercase characters (A - Z)

[1] In IT support scenarios where an IT administrator account cannot be used to perform the support function, an individual may allow a technician to utilize his/her computer under the individual's account even if the individual is unable to be present during the entire support session. Some IT departments have established support agreements and the capability to remote into an individual's computer to provide support. The remote session should only be allowed when the end user responds to an on-screen prompt from a known IT support technician.

If a support function requires that a password be shared, IT Security should be contacted by the IS Owner or IS Administrator for authorization and appropriate instruction. The individual must change their password immediately after the support session is complete.

    b. Lowercase characters (a - z)
    c. At least one Number (0 - 9)
    d. At least one Special Character (For example: ! $, #, or %)
  - Not contain all or part of the user's account name (User-ID).
  - Not be one of the last six passwords used.
  - Be changed at least every 90 days.

- **Unique Passwords** – User account passwords, should be unique in nature and not used for other accounts or sites. User accounts passwords must never be shared with other individuals.

2.3 Changing Passwords and Unlocking Accounts

Users must follow one of the methods defined below to change (reset) their password or unlock their account:

- Self-Service web site: Type "ouhsc.edu/password" into a web browser address bar and follow the instructions on the web site.
- Use the built-in password change function of your University computer. For MS-Windows hold down the Ctrl-Alt-Del keys and choose "Change a password".
- Service Desk walk-in: Bring your OUHSC ID card to the IT Service Desk, David L. Boren Student Union, Room 105.
- Call the IT Service Desk at 405-271-2203 or toll free at 1-888-435-7486 and provide information to verify your identity.

2.4 Mobile Device Password Requirements

Mobile devices such as smartphones and tablets must meet the security requirements listed below. OUHSC IT has implemented an automated process for these security settings, which are automatically deployed to devices that are configured to synchronize email with the OUHSC Exchange server. These settings may not be changed by users.

- **Device Passcode** – A passcode setting of at least four (4) numbers or letters must be set. (Fingerprint readers on mobile devices may be used to unlock the device, but a compliant password must still be established.)
- **Password-Protected Screen Saver -** Password-protected screen saver must be configured to automatically lock the screen after a maximum of fifteen (15) minutes of inactivity and will require a passcode to unlock the device.
- **Local Data Wipe for Failed Login Attempts**– A setting that implements a local data wipe after 10 failed authentication attempts must be enabled.

2.5 Responsibilities of Information System Administrators Provisioning Accounts and Passwords

IS Administrators are responsible for configuring the systems they manage to meet the following requirements. This applies to all servers, applications, and websites on the OUHSC network[2].

- Users must be assigned their own unique individual user account (user-ID) and password. Unique user identification is necessary to provide accountability and non-repudiation for regulatory compliance.
- New account passwords must be one-time use and require the user to change their password at first log-on.

[2] If a system is technically unable to meet these account and password requirements, then the IS Administrator responsible for that system must file an Exception request with IT Security. If approved, the Exception Request must be submitted to IT Security annually. An Exception Request form is available from IT Security.

- Initial passwords must be securely transmitted to the individual. Acceptable procedures are to use encrypted (Secure) email sent to the individual's third-party email address or an internal email sent to the individual's payroll coordinator. Type [secure] in the subject line to encrypt the email.
- IS must require password changes in accordance with regulatory and/or University requirements. Password change frequency must be set to a maximum of 90 days.
- Accounts must be set to lock after 5 failed login attempts. This setting limits attempts to compromise accounts by brute force-attacks and guessing at passwords. Accounts will remain locked for fifteen (15) minutes unless the IT Service Desk is contacted and the user's identity is verified, in which case the Service Desk can unlock the account sooner.
  - If you need assistance unlocking your account, please contact the Service Desk:
    1. OUHSC OKC IT Service Desk
       a. Phone: 405-271-2203
       b. Email: Servicedesk@ouhsc.edu
    2. OUHSC Tulsa IT Service Desk
       a. Phone: 918-660-3550
       b. Email: tulsait-servicedesk@ouhsc.edu
  - Systems must **never** display passwords in their entirety in clear text.
  - Password storage mechanisms must be encrypted or hashed and have strict access permissions to prevent unauthorized access.
  - Default and vendor supplied passwords must be changed before production use or the default account must be disabled.
  - IT or the IS Administrator must reset a user's password immediately in the event a compromise is suspected or reported.

2.6 Service Account Password Requirements

Service accounts refer to accounts that are used to access IS and do not correspond to an actual person. These accounts are often built-in accounts that the systems and services use to access resources they need to perform their functions.

- **Unique Identifier** – All OUHSC service accounts that require system-level access to networks, IS, devices, programs, equipment, or applications must be assigned a unique identifier by Campus IT.
- **Service account passwords** must meet the requirements below as completely as possible:
  - Be at least eight characters long and no more than 26.
  - Contain characters from three of the following four categories:
    - Uppercase characters (A - Z)
    - Lowercase characters (a - z)
    - At least one Number (0 - 9)
    - At least one Special Character (For example: ! $, #, or %)
  - Not contain all or part of the user's account name (User-ID).
  - Not be one of the last six passwords used.
  - Must be changed at least annually.
- **Unique Passwords** – service account passwords, wherever possible, should be unique.
- **Service Account Password Vault** - service account passwords must be stored in the OUHSC password vault, restricting personnel access to those on a "need to know" basis.
- **Root Access –** privileged users must elevate user privileges through the use of 'sudo'.
- **Account Management Procedures –** Procedures must be documented by IS Administrators or IS Owners to reset passwords upon the termination or separation of employees from the department or University who have knowledge of service account passwords.

Registration of Service Accounts – IS administrators who create Service Accounts must follow the Service Account Registration process defined by IT Security.

Service accounts that are unable to meet the above requirements must be presented to OUHSC IT Leadership as a risk decision to be made. Service account risks and the associated risk decision must be documented in the OUHSC IT Security Risk Register.

2.7 Enterprise Directory Services

The Enterprise Directory Service for OUHSC computer accounts is MS Active Directory Domain Services (AD DS). AD DS must be used to manage accounts and provide user logon and authentication services to other systems. AD DS provides a single system for configuring and applying user account and password policies.

- All IS must use the OUHSC enterprise AD DS, AD LDAP or RADIUS for authentication services.
- If the IS is not technically capable of using OUHSC directory services then the IS administrator must manually configure the IS to meet all of the account and password requirements in this Standard.
- The IS Administrator must document the method of account authorization, creation, modification and termination. This document must be reviewed by the department annually, and is subject to review by IT Security, Internal Audit and University administration.

2.8 Reporting a Violation or Suspected Compromise

Use of OUHSC accounts and passwords that is not consistent with this Standard should be reported to campus IT Security or the IT Service desk.

If you believe your account or password has been compromised, immediately notify any of the following offices:

- OUHSC OKC IT Service Desk
  - Phone: 405-271-2203
  - Email: Servicedesk@ouhsc.edu
- OUHSC Tulsa IT Service Desk
  - Phone: 918-660-3550
  - Email: tulsait-servicedesk@ouhsc.edu
- IT Security
  - Phone: 405-271-2476
  - Email: IT-Security@ouhsc.edu

3. Related Documents

- Access to University Data Policy

4. Regulatory References

- HIPAA 45 CFR 164.308(a)(1)(ii)(B)
- 16 CFR Part 314 Standards for Safeguarding Customer Information [section 501(b) of the Gramm-Leach-Bliley Act (''GLB Act'')
- 16 CFR Part 314 Standards for Safeguarding Customer Information, GLB Act
- Payment Card Industry Data Security Standard (PCI DSS)

5. Scope

This Standard applies to all users of accounts created for use with OUHSC Information Systems.

6. Revision, Approval and Review

6.1 Revision History

Version	Date	Updates Made By	Updates Made
1.0	04/11/2007	OUHSC IT	Baseline Version

1.1	10/29/2015	OUHSC IT	Baseline Revision
2.0	11/05/2015	OUHSC IT	This document consolidates multiple documents into one Standard for password management. It will replace the Password Management Policy.
2.1	06/20/2016	OUHSC IT	Modified maximum password age to 90 days. Applied new IT Security Standard template.
2.2	06/20/2016	OUHSC IT	Corrected inconsistencies and added best practice section Fixed Footer for pages past page 1 to say Standards
2.3	08/10/2016	OUHSC IT	Added section on Service Accounts
2.3	10/12/2016	OUHSC IT	Added RADIUS as approved authentication method in section 2.7 Enterprise Directory Services
2.4	10/25/2016	OUHSC IT	Added section on registration of Service Accounts and reviewed changes requested by LC

6.2 Approval History

Version	Date	Approved By
1.0	04/11/2007	Dean's Council
2.4	11/08/2016	Information Security Review Board

6.3 Review History

Date	Reviewed By
11/18/2014	OUHSC IT
06/20/2016	OUHSC IT
06/20/2016	OUHSC IT
10/12/2016	OUHSC Legal Counsel