CEHD Information Security Procedure
IS-5 Account Management

Procedure Statement

From TAMU Security Catalog AC-2 Account Management[1]

Access to CEHD information resources is generally controlled by a logon ID associated with an authorized account. Proper administration of access controls (login IDs and passwords) is important to ensure the integrity of CEHD information and the normal business operation of CEHD managed and administered information resources.

Account Management Procedures

<u>New CEHD employees</u>

1. A notification is sent to the Technology Services ticket system (TeamDynamix) by the CEHD online payroll action request (PAR) system when a new hire or transfer in event is created. (See appendix for copy of notification)
2. Technology Services staff act upon these notifications within 5 business days.
    1. For students, no action is taken.
    2. For employees (faculty and staff), NetIDs are added to the appropriate groups and a home drive is created.
    3. Since the default account is the NetID, no account is created until special circumstances are identified.
    4. All new CEHD employees are required to sign an acknowledgement of TAMU Information Security rules as part of the new hire process. (See IS-4)

<u>Terminated CEHD employees</u>

1. A notification is sent to the Technology Services ticket system (TeamDynamix) by the CEHD online payroll action request (PAR) system when a termination or transfer our event is created. (See new hire notification for format.)
2. Technology Services act upon termination notifications within five business days. Actions will be immediate if Technology Services in notified of an urgent case.
    - If the employee had a CEHD managed account, the account is set to expire, disabled, or deleted.
    - The employee's accounts (NetID, CEHD) are removed from CEHD security groups.

Changes to Employee Status

1. Requests for changes to authorization to CEHD information resources are made through the Technology Services ticket system (TeamDynamix).
2. Changes are implemented by Technology Services staff and the results documented through the ticket system.

CEHD Account Types

Texas A&M NetIDs

- Whenever practical, CEHD will use NetIDs for authentication
- All aspects of these accounts are managed by TAMU IT (e.g., new, terminations, password policy, password changes).
- For systems using NetIDs, Technology Services grants access to resources to specified NetIDs.
- Systems that use NetIDs
    - CEHD Data Portal (all access to secured resources is done through NetIDs)
    - Windows logins. (NetIDs are used for almost all non-admin accounts.)
        - The exceptions are those users still using a CEHD account, scheduled to be eliminated by summer 2017.
        - Any other exeptions should be documented in the IS-5 Special Accounts document.
    - Linux servers (for non-administrative users)

ED Active Directory Accounts

Policy Type	CEHD Policy	Current Setting
Minimum password length	8 characters	8 characters
Password history retained	5	8
Maximum password age (days)	365	365
Password complexity	Enabled	Enabled
Account lockout threshold	5	7
Account lockout duration (min)	10	10
Reset account lockout counter (min)	10	10
Policy set in Group Policy		

- Administrative account of Technology Services employees
    - Technology Services employees (staff, students) who need an administrative account to manage computers and servers on CEHD computers are granted an ED account.
    - Accounts should be created when the employee is hired.

        - A NDA should be signed and given to the CEHD ISO before account information is given to the new employee.
    - Accounts should be disabled when terminated.
- Other ED accounts should be documented within the document “IS-5 Special Accounts”

CEHD Linux Server Accounts

Policy Type	CEHD Policy	Current Setting
Minimum password length	16 characters	16 characters
Password history retained	5	0
Maximum password age (days)	Unlimited	Unlimited
Password complexity	Enabled	Enabled
Account lockout threshold	5	5
Account lockout duration (min)	10	15
Reset account lockout counter (min)	10	15

- Administrative accounts for server administrators
    - Each server has 2-3 administrators who manage the server
    - Accounts will be created when the employee is hired
        - A NDA should be signed and given to the CEHD ISO before account information is given to the new employee.
    - Accounts should be disabled when terminated
- Non-administrators will be granted access via NetIDs.
    - These require a local account to be created. However, these accounts will be set with 16+ character random passwords that will be unknown to all.
- Other (non-NetID, non-Administrative) linux accounts should be documented within the document “IS-5 Special Accounts”

CEHD Active Directory Accounts

Policy Type	CEHD Policy	Current Setting
Minimum password length	8 characters	8 characters
Password history retained	5	8
Maximum password age (days)	365	365
Password complexity	Enabled	Enabled
Account lockout threshold	5	7
Account lockout duration (min)	10	10
Reset account lockout counter (min)	10	10
Policy set in Group Policy		

- CEHD employess were assigned a CEHD account when hired.

- Accounts should be disabled when terminated or migrated to TAMU Exchange and NetID.
- No new accounts have been created since 9/1/2016
- The CEHD domain is scheduled to be retired by Summer 2017. All remaining accounts will disabled and removed by that time.

Local Windows Accounts

Policy Type	CEHD Policy	Current Setting
Minimum password length	8 characters	8
Password history retained	5	8
Maximum password age (days)	365	365
Password complexity	Enabled	Enabled
Account lockout threshold	5	7
Account lockout duration (min)	10	10
Reset account lockout counter (min)	10	10

- The only local account on Windows workstations is the standard "Administrator" account.
    - This account is managed by a Windows server that resets this local account weekly and keeps the passwords within the server in case they needed.
- If other local accounts are needed for a specific function, they should be documented within the Special Accounts document.
- CEHD faculty or staff may request to be a local administrator for their computer. If this request is granted by the Dean of the CEHD, then a local account will be created for them to use to manage their computer.

Local Mac Accounts

Policy Type	CEHD Policy	Current Setting
Minimum password length	8 characters	?
Password history retained	5	?
Maximum password age (days)	365	?
Password complexity	Enabled	?
Account lockout threshold	5	?
Account lockout duration (min)	10	?
Reset account lockout counter (min)	10	?

- For Mac users, a local accounts should be created for the user when the computer is assigned the device.
- The local account should be removed when the computer is transferred to another user.
- A local administrative account (agent) is created for administrative use by Technology Services. This account has a common password across all Macs.

- CEHD faculty or staff may request to be a local administrator for their computer. If this request is granted by the Dean of the CEHD, then a local account will be created for them to use to manage their computer.

Not Fully Implemented

Service Accounts

Policy Type	CEHD Policy
Minimum password length	16 characters
Maximum password age (days)	Unlimited
Password complexity	Random

- Service accounts are ones created to run automated computer-to-computer processes.
- These can be on linux, Windows, or OS X computers.
- For Windows computers, the local SYSTEM account should be used when possible.
- Service Account passwords should be stored within Team Password[2].

Not Fully Implemented

Other System Specific Accounts

Policy Type	CEHD Policy
Minimum password length	16 characters
Maximum password age (days)	Unlimited
Password complexity	Enabled

- For other systems that require a shared administrative password (e.g., a default admin account), the password should be generated following the above policy.
- These accounts/password should be stored in Team Password and accessible by at least two people.
- The vendor default password shall be changed.

Not Fully Implemented

[1]TAMU Security Catalog AC-2 Account Management
http://cio.tamu.edu/Risk_Management_Policy/IT_Policy_Compliance/PDFs/AC2_Account_Management.pdf

[2]Team Password
Team Password (teampassword.com) is a web based product for managing group passwords.

Revised February 27, 2017