CEHD IT Security Procedures

Computer Configuration

This document outlines the minimum requirements for all computers owned by CEHD. A list of general exceptions will be included at the end of this document.

1. A computer must require unique login IDs for anyone to use the computer.
2. When feasible, the computer should be configured to allow access via the A&M NetID. For these login accounts, password policy is enforced by the university and no additional configuration is required.
3. For unique login IDs that are not tied to the A&M NetID, the computer must enforce the following policies.
   - Passwords must be at least eight characters long with operating system complexity rules enabled and must be changed at least once a year OR a password must be at least sixteen characters with complexity enabled with no password expiration. In either case, a password should be changed if the user believes the password has been compromised.
   - Accounts should be locked after no more than seven failed attempts (auto-unlock cannot occur until at least 15 minutes)
4. Login credentials that pass through the network must be passed in an encrypted state.
5. The computer must have anti-virus installed and configured. Virus definitions should be regularly checked and updated at not more than a one week interval.
6. Security-related operating system and software patches must be kept up-to-date. In particular, updates should be applied within one month of issue.
7. Firewall technology must be employed to prevent unauthorized communication to the computer. Firewall port openings can be made as needed based on services running on the computer.
8. Each computer must have an operating system for which security updates are still issued. That is, no computer can have an operating system that has passed its "End-of-Life."
9. Logs use internal system clocks for timestamps.
10. Security logs must be maintained on all computers for at least thirty days. Logs must be regularly monitored for unauthorized or inappropriate use.
11. Software is only installed if the appropriate licensing exists.
12. The computer must display an approved system use notification message or banner before granting access.

    Approved Notification Message:

    Welcome to the College of Education and Human Development

    WARNING: Unauthorized use of this system is prohibited. Such use may result in administrative or legal action or both against the user. You have no expectation of privacy except as otherwise provided by applicable privacy laws. This warning is required by the Texas Administrative Code (TAC), Title 1 Administration Part 10 Department of Information

Resources and the Information Resources Management ACT (IRMA). By clicking "Ok" you hereby agree to comply with the terms listed above.

Minor changes to wording of last sentence is allowed to tailor message to an individual system.

13. *Special considerations for systems containing confidential information*
14. (Linux based systems) System must be configured to disallow remote-root login.
15. Administrative rights on computers are limited to Technology Services personnel unless a faculty or staff member completes the Admin Rights form and takes responsibility for the computer. This includes ensuring that all of the above requirements are met.
16. Every effort should be made to implement all of these procedures on all computers. However, some situations may require exceptions. Requests for exceptions to these procedures must be sent to the CEHD ISO and must include
    - list of AMU asset numbers or serial number of the devices requested to be exceptions
    - procedures for which requesting exemptions;
    - duration of the exemption (e.g., for a summer camp or for the life of the device);
    - reasons each procedure cannot be practically implemented; and,
    - if approved, this information will be included in the documentation and must be re-evaluated annually to determine if exemption still required.

CEHD Managed Systems

Additional configuration requirements for CEHD managed systems. Any exception must be documented.

1. Windows computers shall be joined to the ED domain.
2. Linux computers shall be managed by CEHD's Puppet management system.
3. All servers (physical and virtual) shall be monitored by CEHD's GrayLog implementation.

General Exceptions

These situations are exempted from the above procedures. There is not need to request exceptions for these cases.

- Smart phones and limited use tablets (e.g., iOS, Android) used exclusively by an individual. Each device has it own security and each owner is encouraged to take advantage of those options. Otherwise, CEHD does not have specific requirements for these devices at this time. (This does not include other small form factor computers that have a full operating system such as the Microsoft Surface. Such devices should follow then general procedures in this document.)

Definitions

Computer. For the purpose of these procedures, a computer is any general purpose computing device that includes everything from mobile devices up to large servers.

This document addresses the following questions on the NIST Low Application Assessment required by Texas A&M University

NIST-R0002-AC-03.02
NIST-R0007-AC-07
NIST-R0008-AC-08
NIST-R0056-IA-02a
NIST-R0060-IA-06.01
NIST-R0161-SI-02
NIST-R0027-AU-08

The CEHD ISO as of April 2016 is Arlen Strader, IT Manager

Approved By: ____ Date: ________________

Next scheduled review: 2/1/2018