DHHS Securing Hardware and Software Standard

Issue Date: October 1, 2013
Effective Date: October 1, 2013
Revised Date:

Number: DHHS-2013-001-A

1.0 Purpose and Objectives

The Department of Health and Human Services (DHHS) requires appropriate administrative, physical, and technical controls be incorporated into all hardware and software that store or process any DHHS information, commensurate with its information classification. This includes all DHHS-supported or branded applications, web services, and websites hosted by third parties. The purpose of this standard is to provide guidance to DHHS Information Systems and Technology (IS&T) teams and related third parties on the security requirements for hardware and software that store, process, or have access to DHHS electronic information.

2.0 Scope and Applicability

The scope of this standard applies to all DHHS personnel, contractors, temporary employees, volunteers, vendors and business partners (hereinafter "Staff") with access to DHHS IT resources.

This standard includes all application and system hardware or software that:

a. Reside within the DHHS infrastructure

b. Store, process, or access DHHS Confidential or Highly Restricted data

c. Are hosted by third-party organizations on behalf of DHHS

2.1 Reviews and Enforcement

The DHHS Information Security Officer (ISO) and IS&T will initiate periodic reviews to ensure compliance with the defined hardware and software standards.

The DHHS ISO is responsible to establish a schedule for review and inspection of hardware and software compliance, and shall minimally meet these requirements:

1. All desktop, server, and network device configuration standards shall be reviewed and updated on an annual basis.
2. Inspections for compliance with hardware and software standards shall be performed annually, or more frequently as circumstances dictate. All results will be documented and secured.
3. The DHHS ISO shall maintain a Plan of Action with Milestones (POA&M) that reflects all outstanding security gaps, mitigation and remediation action plans, and corresponding timelines.

4. Documentation of change management meetings shall be maintained and will include descriptions or reference to the changes requested and all approval or non-approval decisions.

Should a violation of this standard occur, it is the responsibility of management for the area in violation to mitigate or remediate the violation in a timely manner. Violation of this standard, as it includes compliance with federal and state regulations, may result in criminal and monetary penalties for DHHS and Staff found violating these standards. Any Staff who committed the violation will be personally responsible for their own actions and any reasonably foreseeable consequences of those actions. Lack of knowledge or familiarity with this standard shall not release an individual from their responsibilities.

Any Staff found to have violated this standard may be subject to disciplinary action, as defined in DHHS-2013-001 *DHHS IT Security Policy.*

3.0 Standards

3.1 Server Hardening Standard

DHHS depends on servers to deliver data in a secure, reliable fashion. DHHS requires assurance that key servers will maintain information confidentiality, integrity, and availability. One step to attain this assurance is to ensure that servers are installed and maintained in a manner that prevents unauthorized access and disruptions in service. All servers that may store, process, or have access to Confidential or Highly Restricted data (sensitive servers) are required to be hardened according to these DHHS standards. In addition, these servers shall have a published configuration management plan that must be as defined below and approved by the DHHS IS&T Management.

1. Servers may not be connected to the DHHS network until approved by IS&T Management. This approval will not be granted for sensitive servers until these hardening standards have been met.
2. The Operating System must be installed by IS&T authorized personnel only, and all vendor supplied OS patches must be applied.
3. All unnecessary software, system services, accounts and drivers must be removed.
4. Audit logging will be enabled. Audit logs will be secured and only accessible to accounts with privileged access.
5. Security parameters and file protection settings must be established, reviewed, and approved by IS&T.
6. Default passwords and default accounts must be disabled or changed.

7. Security patches will be applied as defined by the Change Management Process. Priority setting of vulnerabilities will be based on impact to DHHS and as referenced in the National Vulnerability database (HTTP://nvd.nist.gov).
8. Hardened servers will be scanned on a monthly basis for unauthorized software or unauthorized changes to the configuration baselines.
9. Hardened servers will be monitored with active intrusion detection, intrusion protection, or end-point security monitoring that has been approved by IS&T and DHHS ISO. This monitoring shall have the capability to alert IS&T administrative personnel within 24 hours.
10. Servers shall be loaded from standardized processes and software as defined in the Technical Services Document Library. These processes and software shall be appropriately configured and protected, with integrity controls to ensure only authorized and documented changes are possible.
11. Remote management of hardened servers shall be performed over secured channels only. Protocols such as telnet, VNC, RDP, or others that do not actively support approved encryption should only be used if they are performed over a secondary encryption channel, such as SSL or IPSEC.
12. IS&T shall perform a penetration test of all hardened servers on an annual basis under the direction of the DHHS ISO.

In addition to the configuration management standards listed in section 3.1, all servers designated as "Hardened" are required to have a Hardened Server Configuration Management Plan. This plan will be managed by IS&T and reviewed annually or prior to any change to the hardened server baseline. This plan shall include, at a minimum:

1. Cover page clearly marked "Confidential"
2. Roles and responsibilities
3. Inventory of server(s) and description of purpose, including business departments using the server
4. Location of server within the DHHS infrastructure, including network diagrams
5. Detailed inventory of software authorized to reside on server(s), number of users anticipated
6. Detailed inventory of server(s) hardware, manufacturer, model and serial numbers, configuration settings, and hardware specifications.
7. Emergency server change procedures.
8. Hardened Server Change Request Process.
9. Impact analysis and summary report
10. System Security Plan and Contingency Plan updates
11. Schedule of scanning for authorized software and settings

12. Change request process, and where resulting information will be stored.
13. All servers that are required to meet hardening standards are required to have all change, maintenance and repair activity recorded, including summaries of the activity, and who performed the activity and when.

3.2 Server Security Standards

Improperly configured servers are at risk to have their systems compromised. Without proper adherence to these server security standards, DHHS is at increased risk to have data lost, stolen, or destroyed. This standard is necessary to protect DHHS from the liability of illegal data or activity residing or occurring on DHHS equipment. It is also necessary to reduce the likelihood of malicious activity propagating throughout DHHS networks or launching other attacks. All DHHS managed servers are required to meet these standards. The DHHS Technical Services team is responsible for maintaining these standards and for configuring and managing the hardware and software and imaging processes for managed servers. As server hardware and software may change, see the Technical Services Document Library for specific details for each type of DHHS server.

3.3 Change Management Standards

DHHS change management standards address requirements for managing changes to the DHHS IT infrastructure (which includes all hardware, system software, and network assets) and application software that use data classified as Confidential and Highly Restricted (which include commercial off the shelf data applications and DHHS in-house developed data application software).

The change control process may differ between the change controls for the IT infrastructure and application software, but the underlying requirements are the same. All IT infrastructure and application development changes are required to follow a change management process to ensure the change is approved for release.

3.3.1 IT Infrastructure - The following standards are required to be followed for all IT infrastructure. This is in addition to any above referenced hardening standards for specifically identified hardware and software.

1. DHHS has established a change management process with assigned responsibilities to ensure all changes to DHHS hardware, system software, and network infrastructure is authorized. This process will include representation from IS&T, Information Security, and application development (when application changes impact or are impacted by IT infrastructure changes) and will require meeting on a periodic basis with sufficient frequency to meet demands for changes to the DHHS environment.

2. The Infrastructure Change Control Group will keep records and documentation of meetings, decisions made, and rationale. All decisions made at the change control group will be documented and securely stored for audit purposes. The agenda for this meeting should address a review of the following:
    a. Change summary, justification and timeline
    b. Test plans and results
    c. Security review and impact analysis
    d. Documentation and baseline updates
    e. Implementation timeline , and recovery plans

3. DHHS is required to maintain baseline configuration documentation in use throughout the infrastructure. These baseline configuration documents shall be categorized as confidential information, and secured appropriately. The baseline documents must be reviewed and updated on an annual basis or after any significant changes to the baseline have been installed.

4. As part of the infrastructure configuration baseline, IS&T will maintain an inventory of all authorized (system and application) software components. As software is added or removed, the software inventory will be updated.

5. All changes to the DHHS production infrastructure are required to be made by authorized personnel only, using access credentials assigned to that individual. Actions performed by these user credentials will be logged when possible.

6. DHHS shall disable all ports, services, protocols, etc. on all technology that is not needed to support DHHS business. This information shall be documented, and the ISO will initiate a review of the environment on an annual basis to ensure that only necessary and required ports, services, protocols, etc. remain enabled.

7. DHHS will maintain an inventory of hardware, software, networks, and system components that include manufacturer, model numbers, serial numbers, licensing information, version numbers, physical and logical locations, and other applicable information. This inventory will be secured and auditable, and will be kept updated and current with the DHHS infrastructure.

3.3.2. Application Development – The following standards are required to be followed for DHHS application software systems that create, process, or store Confidential and Highly Restricted data.

1. DHHS must establish application change management processes with assigned responsibilities to ensure all changes to appropriate DHHS application software are approved and documented. Change management teams will include appropriate application development staff and appropriate staff to represent DHHS Information Security.

2. The change management processes may vary depending on the data application size and configuration, however all processes must include formal procedures with tools to support the documentation, review and approval for each change request.

3. The change management processes will retain a documented history of the change process as it passes through the SDLC with documentation securely stored for audit purposes. Documentation should address a review of the following:
    a. Change summary, justification, and timeline
    b. Test plans and results
    c. Security review and impact analysis
    d. Documentation and baseline updates
    e. Implementation timeline and recovery plans

4. Changes to software applications must be controlled and production installations shall be made by personnel assigned to update production libraries.

5. Changes to production libraries should not be the same personnel who made the application changes unless documented procedures are in place which ensure the confidentiality, integrity, and availability of the data maintained in the production library.

6. Application development changes that impact DHHS IT infrastructure must be submitted to the Infrastructure Change Control Team for review, approval, and implementation.

3.4 Workstation Security Standards

Improperly configured workstations are at risk to have their systems compromised. Without proper adherence to these workstation security standards, DHHS is at increased risks to have data lost, stolen, or destroyed. This standard is necessary to protect DHHS from the liability of illegal data or activity residing or occurring on DHHS equipment. It is also necessary to reduce the likelihood of malicious activity propagating throughout DHHS networks or launching other attacks. All DHHS managed workstations that connect to the DHHS network are required to meet these standards. The DHHS Technical Services team is responsible for maintaining these standards and for configuring and managing the hardware, software, and imaging processes for all managed workstations. As workstation hardware and software may change frequently specific workstation standards are maintained in the Technical Services Document Library. In addition to adherence to the required images, the following standards are defined for all workstations that connect to the DHHS network. The degree of protection of the workstation should be commensurate with the information classification of the resources stored, accessed, or processed from this computer.

1. Endpoint security (anti-virus) software, approved by IS&T and ISO, must be installed and enabled.

2. The host-based firewall must be enabled if the workstation is removed from the DHHS internal network.

3. The operating system must be configured to receive automated updates.

4. The system must be configured to enforce password complexity standards on accounts.

5. Application software should only be installed if there is an expectation that it will be used.

6. Application software not in use should be uninstalled.

7. All application software must have security updates applied as defined by patch management standards.

8. Shared login accounts are prohibited unless approved in advance and configured by IS&T. Shared login accounts are only acceptable if approved through the policy exception process and alternate mechanisms or access layers exist to ensure the ability to individually identify personnel accessing non-public information.

9. Shared login accounts are forbidden on multi-user systems where the manipulation and storage of Confidential or Highly Restricted information takes place.

10. Users need to lock their desktops when not in use. The system shall automatically lock a workstation after 15 minutes of inactivity.

11. Users are required to store all Confidential or Highly Restricted information on IS&T managed servers, and not the local hard drive of the computer. Local storage can only be used for temporary purposes when the data stored is not sensitive, and where loss of the information will not have any detrimental impact

on DHHS. All DHHS laptops with the ability to store data must be fully encrypted using IS&T approved technology.

12. All workstations shall be re-imaged with standard load images prior to re-assignment.

13. Equipment scheduled for disposal or recycling shall be cleansed following DHHS media disposal guidelines.

3.5 Network Device Security Standards

DHHS encourages the use of its electronic communications infrastructure in support of its mission. However, this infrastructure must be well-managed and protected to ensure the security of DHHS information. Therefore, all network devices that connect to the DHHS network are required to adhere to the following standards:

1. All publically accessible devices attached to the DHHS network must be registered and documented in the IS&T Inventory system. Publically accessible devices must reside in the DHHS DMZ unless approved by IS&T and the Information Security Officer for legitimate business purposes.

2. All publically accessible devices must be located in an access-controlled environment, and access credentials must be managed by IS&T authorized personnel.

3. All devices that contain or process Confidential or Highly Restricted data must be secured with a password-protected screen saver that automatically locks the session after 15 minutes of inactivity.

4. All devices that are connected to the DHHS network shall be continually executing IS&T approved anti-virus scanning, spyware protection, or other automated security scanning technologies, as applicable to the device.

5. Network scanning is prohibited, unless prior approval is obtained by the Information Security Officer and IS&T management. If approved, scanning must be restricted to authorized and registered IP addresses only, and conducted by authorized personnel only.

6. No person at DHHS shall monitor network traffic unless this activity is approved in advance by the DHHS ISO, DHHS Human Resources, DHHS Legal, or the scanning activity is part of their normal job duties. IS&T shall implement measures to restrict scanning to authorized personnel only.

7. Devices that include native host-based firewall software in the operating system shall have the firewall activated and properly configured, unless the active

firewall software compromises the usability of critical applications, or lessens the posture of other security systems.

8. Passwords and SNMP community names may not be sent in clear text over open networks. All devices must use IS&T authorized encryption for access authorization to the internal network. Access to the DMZ applications is exempt from this requirement.

9. All encryption must be approved by IS&T.

10. Any device that has been compromised may be disconnected from the DHHS network without prior warning. The DHHS ISO will be notified within 1 hour of any suspected security incident.

11. The DHHS network shall have an annual verification of all open ports for publically accessible systems. The system shall have an external penetration test conducted annually. Self-assessments and tests are acceptable every other year. Any requests for public IP addresses or for additional open ports must be approved by the IS&T Network Management.

12. Network devices will follow approved change control and configuration management procedures, as defined by IS&T.

13. Services and applications that will not be used must be disabled.

14. Patches and hot-fixes recommended by hardware or software vendors must be installed as soon as practical, following the DHHS standards for patch and vulnerability management.

3.6 Application Development Security Standards

This standard applies to all software applications that are being developed or administered by DHHS personnel. It also applies to all software that resides on DHHS infrastructure and software that stores, processes, or accesses DHHS Confidential or Highly Restricted data. This standard is intended to increase the security of applications and help safeguard DHHS information technology resources. The following items are required to be implemented into all application software within the scope of this standard:

1. All applications are required to maintain up-to-date documentation that includes an assessment of security threats and impacts, and a detailed description of the data handling with its accurate classification.
2. Applications that provide user interfaces shall have a Confidentiality Banner displayed, applicable to the data being accessed (i.e., HIPAA).
3. Application credentials, where possible, should be inherited from the DHHS Managed Authentication Source. If that is not possible, credentials should have the same level of management and approval as other DHHS access credentials.

4. Confidential or Highly Restricted data must be encrypted when transmitted outside the DHHS internal network.
5. Application Development and Implementation must follow a change management process, which includes Security oversight at specific handoff points of the SDLC - such as going from requirements definition to a design stage. All applications must be thoroughly tested before release to a production state.
6. Testing should use artificial or de-identified data. If that is not possible or practical, then the testing environment shall be secured to a level adequate to meet all policies to protect the information commensurate with its information classification.
7. Applications that process Confidential or Highly Restricted data must have a security plan defining critical service levels that is reviewed and approved by the IS&T Management Team.
8. Application software must be managed in a secured environment. Changes shall occur in non-production environments and then migrated to production state after authorized approvals. DHHS shall maintain at least three versions of application software, and all versions shall maintain audit trails.

3.7 Security Standards for Web Application and Services

DHHS Internet-facing systems are diverse in order to meet a multitude of different needs. Therefore, information exposures by these systems differ, as do threats. Security controls should be implemented to mitigate meaningful risks to an application. Because every system is different, the web application developer is the most knowledgeable about the system and the risks it faces.

This standard establishes a baseline of security requirements for all DHHS websites, web services, and all third-party supported or hosted web applications. All applications that are Internet-facing are required to securely maintain documentation and evidence of compliance levels with this standard.

This standard is based on the research and recommendations from the SysAdmin, Audit, Network, and Security (SANS) Institute and the Open Web Application Security Project (OWASP).

1. Consider the threats and risks to your application. If you are unsure, follow the Threat Risk methodology published by OWASP. http://www.owasp.org/index.php/Threat_Risk_Modeling

2. Consider and implement additional security controls to ensure the Confidentiality, Integrity, and Availability of the information based on the unique threats that face your application.

3. Implement error-handling in a manner that denies processing on any failure or exception.

4. All input fields must be validated before accepting. Input should be checked to prevent the program from executing malicious code. Input length must be validated to determine if it is within the predetermined minimum and maximum ranges. Input values should be screened for valid data types (e.g., number or character only, no special characters).

5. Output fields must be sanitized to ensure the output does not reveal too much information that could be used by malicious intent (e.g., default system-generated messages should be translated by the application). If invalid user input is encountered, the error message should not reveal the specific component which caused the error. Messages should be general in nature, and not reveal anything more than what is necessary.

6. The identity of the user must be authenticated, and all user credentials and passwords must meet the DHHS policy requirements for strength, change, and history. User access and capability must be limited to the functions required for the authorized access level only.

7. The requesting and granting of user accounts must include an approval process that validates the user and the minimum necessary access levels.

8. Establish secure default settings commensurate with the type of access.

9. All external systems (including web services), which require access to the application, must be authenticated and permissions checked before the external system becomes trusted.

10. All password entry fields should not "echo" the password in readable text when it is entered. Auto-complete of password fields should be disabled.

11. All sessions should be invalidated when the user logs out of the system.

12. If a web application needs to store temporary or session-related information that is Confidential or Highly Restricted outside of the secured DHHS internal network, that information must be encrypted in all cases – whether stored or in transit. Encryption technology must be approved by IS&T.

13. All web applications are required to have a security scan and test of the application on a recurring basis as determined by the DHHS ISO. Higher risk or impact applications should be tested annually. This test shall be coordinated and supervised by the ISO and IS&T management. Some packaged web applications where the package's architecture inherently protects the application from

security risks, may have reduced testing requirements versus other web applications.

Other application security recommendations and development guides can be reviewed at the OWASP or SANS websites:

https://www.owasp.org/index.php/Category:OWASP_Guide_Project

http://www.sans.org/top25-software-errors/

3.8 Security Requirements for Cloud Services and Cloud Service Providers

All Cloud Service Providers (CSP's) must have an official FedRAMP certification by an accredited third-Party Assessor Organization (3PAO), or alternatively, the following conditions must be met or addressed via contractual agreement before engaging any cloud service providers or third-party hosting for DHHS when that cloud service may store or process any Confidential or Highly Restricted data:

1. The Cloud Service Provider or third-party host (CSP/3PH) must provide evidence of secure storage of access credentials that are at least equal to that of DHHS internal systems.
2. Access to the cloud service will require multi-factor authentication based on data classification levels.
3. De-provisioning of credentials must occur within two (2) hours of de-provisioning of the internal system credentials.
4. Information will be encrypted using IS&T approved technology for information in transit as well as information stored or at rest.
5. Encryption key management will be controlled and managed by DHHS unless explicit approval for key management is provided to CSP/3PH by IS&T. This may require an escrow service for key storage.
6. All equipment removed from service, information storage areas, or electronic media that contained DHHS information must have all DHHS information over-written, sanitized, and data destruction verified by DHHS before allowing that equipment, information storage space, or media to be destroyed or assigned for reuse.
7. CSP/3PH will provide vulnerability scanning and testing on a schedule approved by the DHHS ISO. Results will be provided to DHHS as needed.
8. Patch management of hardware and software at the CSP/3PH are required to meet the same standards that are required at DHHS.
9. CSP/3PH will meet all DHHS requirements for chain of custody and PHI or PII breach notification in the event that DHHS requires forensic analysis. CSP/3PH will maintain an incident management program that notifies DHHS within one (1) hour of a breach.

10. CSP/3PH will provide evidence of audit and assessment of the security of the service environment, and will agree to reasonable inspection of such security by DHHS-authorized parties.
11. CSP/3PH is required to advise DHHS on all geographic locations of DHHS information. CSP/3PH will not allow DHHS information to be stored or accessed outside the USA without explicit approval by DHHS. This includes both primary and alternate sites.
12. Privileged access roles at the CSP/3PH are required to meet the same vetting standards of privileged access personnel at DHHS, such as background checks, etc.
13. Contracts with CSP/3PH's shall have SLAs in place that clearly define security and performance standards. Contracts will address how performance and security will be measured, monitored, and reported. Contracts will also establish an enforcement mechanism for SLA compliance.
14. CSP/3PH will provide assurance of compliance with the Privacy Act, HIPAA regulations, and IRS 1075 regulations. CSP/3PH will provide adequate security and privacy training to its associates, and provide the DHHS security officer with adequate evidence of this training.
15. CSP/3PH will provide DHHS with the ability to conduct a reasonable search to meet Nebraska Public Records Law.
16. Before contracting with a CSP/3PH, DHHS shall have proactive records planning in place to ensure the ability to have timely and actual destruction of records in accordance with DHHS record retention policies.
17. CSP/3PH will provide documentation, evidence, or reasonable access by IS&T and ISO to ensure compliance with these standards.

4.0 Revision History

Legal Review – 09-09-2013
Policy Approved – 09-30-2013

Signature:

Date: 9/30/2013

Eric Henrichsen
Information System & Technology Administrator
Nebraska Department of Health & Human Services