DHHS Information Technology (IT) Security Policy

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

Number: DHHS-2013-001

1.0 Purpose and Objectives

All State of Nebraska Department of Health and Human Services (DHHS) personnel have an obligation to protect the Information Technology resources they handle from intentional or accidental misuse or damage. DHHS IT Resources referred to in this document include but are not limited to computer hardware, software, data storage, portable digital devices, network communication infrastructure, network access, Internet/Intranet/Extranet access, and electronic communication (i.e., email, instant messaging, and data exchange).

The purpose of this policy is to define the administrative, technical, and physical safeguards that are required for the protection of the Confidentiality, Integrity, Availability, and Privacy of the State of Nebraska DHHS information and all Information Technology (IT) resources administered and managed for DHHS by the Information Systems & Technology (IS&T) Division.

This policy describes the minimum required safeguards and procedures necessary to maintain a secured environment commensurate with the classification level and follow all applicable state and federal privacy/security safeguard requirements.

The primary objectives of this policy are to:

- Provide clear direction to all Staff on their obligations to safeguard information, and procedures to follow to minimize the risk of security incidents.
- Establish clear accountability and authority for developing, administering, and ensuring compliance with security policy across all of DHHS.
- Ensure a focus on security and privacy exists at key touch points throughout DHHS, so that security becomes an institutionalized and integrated function.
- Establish a secure, resilient, and controlled information technology infrastructure and environment.
- Ensure that all administrative, physical, and technical safeguards remain in compliance with all applicable regulatory, legislative, and DHHS mandates.
- Ensure adequate and appropriate planning is in place in the event of a security incident or event affecting business continuity and recoverability.
- Promote and increase the overall awareness of information security throughout DHHS.

- Establish effective management of risk, commensurate with the sensitivity of information at hand and potential impact of information loss, damage, or exposure.

2.0 Scope and Applicability

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

This policy applies to all DHHS and State IT resources owned, leased, or supported by DHHS or any outside entity that has signed a Third Party or Business Partner Agreement with DHHS.

This policy outlines the requirements and expectations that all Staff are expected to follow to ensure the confidentiality, integrity, and availability of information in the State's care, while providing the appropriate level of information stewardship to our State's citizens.

Staff granted access to DHHS IT resources are required by this policy to abide by all safeguards listed in this policy and in the defined standards and procedures associated with this policy. Staff will cooperate fully with IS&T in carrying out the safeguards.

2.1 Policy

It is DHHS policy that electronic and physical security safeguards must be implemented as defined in this policy and appropriate to meet a defined level of risk and updated as required by state and federal statutes and changes in technology.

This policy, and all related standards, procedures, strategies, and plans are required to be compliant with all Nebraska Information Technology Commission (NITC) security policies and requirements. It is the responsibility of the DHHS Information Security Officer (ISO) to ensure appropriate review of compliancy occurs on a regular basis.

2.2 Policy Enforcement

Should a violation of this policy 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 policy, 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 working directly for DHHS found to have violated this policy may be disciplined in accordance with the applicable workplace policies and labor contracts administered by DHHS Human Resources. Such discipline may include termination of employment.

Any Staff working directly for a business partner under contract with DHHS to provide services to or on behalf of DHHS who is found to have violated this policy may be disciplined in accordance with state and federal laws and penalty provisions as defined in the service contract. Such discipline may include termination of the service contract.

2.3 Policy Exception Process

It is recognized that at times, business requirements dictate short term solutions that are contrary to the Security Policy, and may require policy exceptions. All requests for exceptions to this policy will be made in writing and include a risk and impact analysis and a plan for mitigation of the risk of the policy exception. Exceptions must be approved in advance by the CIO of DHHS. Specific details and procedures for requesting a policy exception are included in the DHHS Information Technology Policy Exception Procedure.

3.0 Security Authority and Responsibilities

3.1 DHHS Information Security Officer

DHHS will assign an Information Security Officer who will have oversight responsibility to ensure appropriate and adequate policy, process, and procedures are in place to protect the confidentiality, availability, and integrity of information throughout the DHHS environment.

It is the responsibility of the DHHS ISO to effectively manage the overall security program and to continually monitor, review, assess, and improve the technical, physical, and procedural safeguards to a level that is adequate and appropriate for the information being protected.

The DHHS ISO will have the authority to conduct IT audits, reviews, and assessments to determine the level of compliance with DHHS IT Security Policy. The DHHS ISO will also draft and submit for approval all new or changed security policies, standards, and procedures necessary to maintain appropriate levels of security to the DHHS Agency CIO.

3.2 DHHS CIO

The Agency CEO has authorized the DHHS Agency CIO to serve as the authority to establish and ratify Security Policy. DHHS Human Resources will have the authority to enforce compliance with DHHS Policy. The DHHS CIO will serve as the Security activity

approval authority, with recommendation from the DHHS ISO and consideration from IS&T Management. This includes the authority to establish the standards and procedures necessary to follow in order to comply with Security Policy while staying aligned with ongoing IT strategies. DHHS IS&T is charged with the responsibility for implementing and maintaining adequate and appropriate security safeguards that comply with the Security Policy.

The DHHS CIO will have the authority to grant policy exceptions when warranted, and when presented by the DHHS ISO.

3.3 DHHS Agency Wide Support Department Management

It is the responsibility of DHHS Agency Wide Support Department leadership to visibly endorse and enforce this policy. Department management will establish detailed standards and procedures, aligned with this policy, for Staff to follow in performing their assigned duties in a secure manner. Exceptions to this policy must be formally submitted as described in the DHHS IT Security Policy Exception Procedure. Agency wide support departments include:

- Communications and Legislative Services
- Legal Services
- COO / Operations
- Information Systems and Technology (IS&T)

3.4 DHHS Division Senior Management

It is the responsibility of the Division Leadership Team within the six key divisions of DHHS to incorporate and enforce compliance with this policy into their division operational procedures. These divisions include:

- Behavioral Health
- Children and Family Services
- Developmental Disabilities
- Medicaid and Long Term Care
- Public Health
- Veteran's Homes

This policy will serve as governing policy and standard to any division-level security policies. Any exceptions to compliance with this policy will follow the formal DHHS IT Security Policy Exception Procedure.

4.0 Security Oversight and Compliance

It is the responsibility of the DHHS CIO and the DHHS ISO to ensure an appropriate level of Security oversight is occurring at all potential exposure points of DHHS systems and operations so that the State has reasonable assurance that the overall security posture continuously remains intact. The DHHS ISO has the responsibility to ensure the security program meets state and federal statutes as they apply to DHHS and DHHS IT resources.

It is DHHS Policy that the DHHS ISO will establish and manage an entity-wide oversight and compliance function. This will include, at a minimum, appropriate information security oversight at key points within the Technology Acquisition Process, Hardware and Software Change Management Process, and the Contract Management Process when changes involve access to or potential exposure of Confidential or Highly Restricted information.

4.1 Acceptable Use

DHHS-provided technology, such as individual computer workstations or laptops, computer systems, networks, email, and Internet software and services are intended for authorized business purposes only. All Staff will be required to review and comply with the DHHS-2013-002 *DHHS IT Acceptable Use Policy* and annually sign an Acknowledgement of Understanding of the DHHS IT Acceptable Use Policy DHHS-2013-002.

4.2 Right to Monitor

DHHS is responsible for servicing and protecting the DHHS equipment, networks, information, and resource availability and therefore may be required to access and/or monitor electronic communications. This can include emails, Internet usage, telephone calls, instant and text messaging, and other electronic communications. This monitoring is also necessary to perform optimization of IT resources, troubleshooting and repair of technical problems, analysis for capacity and performance planning, and detecting patterns of abuse or illegal activity.

4.3 Security in Contracts, Agreements, RFP's/RFI's, and SOW's

All contracts, business partner agreements, RFP's/RFI's, statements of work, or other third-party arrangements that involve Confidential or Highly Restricted information will include an acknowledgement and agreement for the business partner to meet security policy and other minimum security requirements of DHHS. This agreement will include provisions to allow for compliance review or assessments ensuring minimum security requirements of DHHS are continually managed. All contracts must include appropriate DHHS IT Security language provided by the DHHS ISO and approved by IS&T.

Business Partners will be required to notify DHHS of any security incidents affecting or involving Confidential or Highly Restricted DHHS information in a timeframe and manner commensurate with the information classification, magnitude of exposure, and

potential impact to DHHS or Citizens of the State of Nebraska. Incidents that involve or could potentially involve Confidential or Highly Restricted data must be reported immediately as defined in DHHS-2013-001-E *DHHS IT Incident Management Standard.*

4.4 Auditable Events

DHHS will maintain logging of certain events, as detailed in DHHS-2013-001-F *DHHS Information Technology Audit Standard.* Logs will be treated as Confidential or Highly Restricted information and secured appropriately with sufficient capacity to meet audit log retention requirements. DHHS will periodically review audit log records for indications of inappropriate or unusual activity, and report findings to designated DHHS officials.

5.0 Security Planning

It is DHHS policy that appropriate planning occur to ensure information security is adequately addressed, staffed, and funded to stay at an appropriate level for the protection and compliance of the DHHS environment.

5.1 Recurring Security Plans

DHHS ISO will prepare a System Security Plan and Safeguard Activity Plan and Report on an annual basis. These plans will reflect the current and planned state of Security at DHHS, and will be consistent with DHHS strategic architecture. The DHHS Information Security team will prepare a Security Plan of Action and Milestones (POA&M) which will be reviewed by the IS&T Management team on a monthly basis. All security plans will be considered Confidential Information, and will follow the requirements and procedures as outlined in DHHS-2013-001-D *DHHS IT Security Reporting Standard.* DHHS-2013-001 *DHHS IT Security Policy* and all applicable standards and procedures will be reviewed on an annual basis and updated as necessary.

5.2 Security Reviews

DHHS ISO will prepare a plan for review and assessment of policy compliance within the various divisions of DHHS. This plan will include consideration of the level of risk within the DHHS divisions, and will be updated on an annual basis, or when significant change of technology or information handling changes within the DHHS divisions. DHHS ISO will perform an annual FISMA assessment as defined in DHHS-2013-001-F *DHHS IT Audit Standard.*

5.3 Record Keeping

The DHHS ISO will keep records of plan updates and versions. All records will be treated as confidential information and will be appropriately secured and retained according to DHHS record retention procedures.

6.0 Information Classification

It is DHHS Policy that in order to maintain appropriate levels of information confidentiality, integrity, and availability, all information, whether electronic or printed, must be classified into one of four classification levels:

1. PUBLIC
2. INTERNAL USE ONLY
3. CONFIDENTIAL
4. HIGHLY RESTRICTED

This policy applies to all information in any form, including: online, email messages, printed material, FAX, digital messages, voice mail, and personal conversations.

All Staff, regardless of their position, recognize and appropriately categorize any information they access, use, or are exposed to into one of these categories. It is the policy of DHHS to implement technical, physical, and administrative safeguards to protect the Confidentiality, Integrity, and Availability of all State information in a manner that is commensurate with its classification level.

PUBLIC applies to information that has been explicitly approved by official State channels for release to the public, or information that is already in the public domain.

Examples include but are not limited to:

- Job openings and postings
- Information on the Nebraska.gov website
- Advertisements
- Public Records

Safeguards for PUBLIC information include, at a minimum:

- Mechanisms to ensure the integrity and accuracy of the information
- Procedures to ensure the recovery of the information in the event of loss or damage

INTERNAL USE ONLY applies to information that is not intended for Public Release.

Examples include, but are not limited to:

- Information NOT approved for release to the Public
- Documentation and instruction manuals
- Building Security and Disaster Recovery Plans
- Software technical specifications
- Items protected by Non-Disclosure Agreements
- Policies, standards, and procedures

Safeguards for INTERNAL USE ONLY information include, at a minimum, all the safeguards defined for Public information AND:

- Mechanisms to ensure the confidentiality and availability of the information
- Access will be restricted to authorized personnel only

CONFIDENTIAL applies to information that is restricted to individuals who have approved access to this information, and require this access in order to perform their assigned duties.

Examples include, but are not limited to:

- Personally identifiable information (PII)
- Protected health information (PHI)
- Employee HR records, including performance ratings and payroll information
- Social Security numbers
- Attorney/Client privilege information

Safeguards for CONFIDENTIAL information include, at a minimum, all the safeguards defined for Internal Use Only information AND:

- Storage of information will be secured behind DHHS-managed firewalls
- Access will be limited to individually identifiable accounts
- Information will be encrypted per DHHS standards when in transit outside of the internal network (such as in emails)
- Information will not be stored on removable or portable media (such as laptops, thumb drives, or smartphones) unless encrypted using DHHS-approved encryption tools Remote access to Confidential Information must be configured using DHHS-controlled, managed, or approved methods.

HIGHLY RESTRICTED applies to critical and sensitive information that is restricted to a very small subset of individuals who have explicit approved access to this information, and require this access in order to perform their assigned duties. This information typically has additional technical protection requirements or unique protection regulations that must be adhered to beyond what is required for Confidential Information.

Examples include, but are not limited to:

- Privileged account credentials (i.e., ADMIN accounts) and log information
- Attorney/Client privilege information
- Federal tax information (FTI)

Safeguards for HIGHLY RESTRICTED information include, at a minimum, all the safeguards defined for CONFIDENTIAL information AND:

- Enhanced logging and auditing will be enabled
- Remote access to HIGHLY RESTRICTED information will require multi-factor authentication

7.0 Controlling Access to Information and Systems

It is DHHS Policy that appropriate access control safeguards be implemented and maintained to protect IT resources from unauthorized access. Access controls include unique identification and authentication of users before access is granted to protected IT resources. Configuration settings for automatic enforcement, logging, locking, and expiration of user accounts is detailed in DHHS-2013-001-B *DHHS IT Access Control Standard*.

Periodic reviews will be performed on IT resources storing or accessing DHHS information. Such reviews will be a joint venture between Information Security and the DHHS department, division, or program area being audited The review will include an assessment of access credentials, authorization of access, and a review to ensure that only the minimum necessary access to perform assigned duties is granted to the reviewed group.

7.1 User Accounts and Minimum Necessary Access

Any Staff authorized to access any DHHS IT resources that have the potential to update, modify, or access non-public information must be assigned a unique identification (ID) with the MINIMUM NECESSARY access required to perform their duties. Staff are responsible for, and can be held accountable for, the actions conducted by their user ID and are required to secure their ID's from unauthorized use. It is the responsibility of management to ensure that only minimum necessary access is provided to their Staff, and each user requiring access to the DHHS network with the potential to update, modify, or access non-public information has an individual user ID issued to them.

7.2 Passwords

Passwords are considered Highly Restricted information, and should be guarded against unauthorized or accidental disclosure.

It is DHHS Policy that password standards and controls include auto locking, password strength, password composition, and previous usage. These password standards and controls must be automatically enforced.

All password standards and required controls are defined in DHHS-2013-001-B *DHHS IT Access Control Standard*.

7.3 Remote Access

Remote access is defined as: Access to the DHHS information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Remote access to the DHHS Internal Network containing Confidential or Highly Restricted information will only be permitted from DHHS-controlled, managed, or approved methods or arrangements that have been approved through the policy exception process. Procedures for controlling remote access devices are defined in DHHS-2013-001-B *DHHS IT Access Control Standard*. All remote access must have prior authorization before remote access to the internal network is established. Staff approved for remote access must sign an acknowledgement and agreement of requirements and responsibilities before remote access to the internal network is established. Remote access will be logged and periodically audited. Remote access to Confidential or Highly Restricted information will require multi-factor authentication using IS&T approved technology before remote connection is granted.

7.4 Account Termination

Accounts that have been inactive for 180 consecutive days will be automatically disabled. Accounts that have been inactive for 13 months will be automatically deleted. Temporary accounts for any contractors, consultants, or business partners will be terminated or renewed annually, and records will be kept on this activity. Staff that has terminated DHHS employment will have their credentials disabled within 24 hours of their departure, or immediately on departure if due to cause.

7.5 Privileged Access Accounts

Accounts with privileged access, such as administrator or root access accounts, will have activity logging enabled, following DHHS-2013-001-F *DHHS IT Audit Standard*. DHHS will perform a quarterly review of privileged access accounts. All privileged access accounts must be assigned to an individual with a documented business need for the privileged access. These accounts will not be shared. Privileged access through remote channels will be allowed for emergency maintenance or support only, and usage must be documented and approved. Privileged Accounts management will follow the procedures as outlined in DHHS-2013-001-B *DHHS IT Access Control Standard*.

8.0 Secure Handling of Information

It is DHHS policy that all information will be handled in a secure manner commensurate with the classification level of that information. This includes all Staff of DHHS, all systems that process or store information, and all business partners who have authorized access to any DHHS information.

8.1 Portable Media

If Confidential or Highly Restricted data must be stored on portable media, it is DHHS policy that the media storing the Confidential or Highly Restricted data must be fully encrypted using IS&T approved technology. Refer to the Technical Services Document Library for specifics.

Portable media is defined as any device that can store data electronically and is portable or removable including, but not limited to: laptops, portable hard drives, CD's, DVD's, thumb drives, smartphones, and PDA's.

8.2 Email and Messaging

All DHHS email accounts, email messages, text messages, instant messages, video conferences, and any other messaging received or transmitted using DHHS resources are the property of DHHS and may be monitored for appropriate usage. Any electronic transmission, including email, messaging, or video containing Confidential or Highly Restricted data will not be sent over any open networks (such as the Internet) unless transmitted using IS&T approved encryption technology. Acceptable use of the DHHS email system is detailed in DHHS-2013-002 *DHHS IT Acceptable Use of Technology Policy*.

8.3 Encryption

Encryption solutions must be approved in advance by the DHHS ISO before deployment to any DHHS technology or information database. Any encryption technology must be FIPS 140-2 compliant and have a key management plan approved by IS&T and the DHHS ISO. Confidential or Highly Restricted Information will be encrypted, in transit and at rest, when this information is not resident within the DHHS internal network.

9.0 Risk Management

The DHHS ISO is required to implement an Information Security Risk Management program for DHHS. This will include periodic assessments of risk throughout the DHHS environment. These assessments will address both threats and vulnerabilities, and include an assessment of the adequacy of the confidentiality, integrity, and availability controls for information and DHHS resources surrounding the business process, commensurate with its information classification level. All findings will be documented, prioritized, and managed.

9.1 Risk Reviews and Assessments

It is DHHS Policy that scheduled and random risk assessments will be conducted on DHHS IT resources maintaining or accessing DHHS information.

Such risk assessments will evaluate the potential security risk a defined IT resource's vulnerabilities may have and the potential impact it may have on other DHHS IT

resources. The risk assessments will be a joint venture between IS&T and the DHHS division, department, or program area accountable for the IT resource included in a risk assessment.

The DHHS ISO will prepare an annual plan for business process risk assessments. This plan will take into consideration: previous reviews, audit findings of the business process, risk indicators surrounding the business process, probabilities and likelihood of security events affecting the business process, impacts to the State and its citizens should the business process have its security compromised, and other planned or active projects, tasks, and initiatives affecting the business process.

Random risk assessments will be performed at the discretion of the DHHS ISO or as directed by the DHHS CIO, typically when circumstances require additional oversight-such as after a security incident, increased security threat, or significant changes to the IT infrastructure.

Detailed procedures to be followed for risk assessments are defined in DHHS-2013-001-C *DHHS IT Risk Management Standard*.

9.2 Vulnerability and Patch Management

System software will be regularly evaluated and updated when appropriate. Updates will be managed and remediated through the Change Management Process. DHHS will perform vulnerability scanning of system software on a quarterly basis. All findings from the vulnerability scans will be documented, prioritized and mitigated or remediated according to the detailed procedures in DHHS-2013-001-A *DHHS Securing Hardware and Software Standard*.

9.3 Software Scanning

Internet exposed software developed by DHHS will be scanned for web application security flaws before being published into a production environment. Scanning must be performed by a qualified, independent process using authorized tools. All findings will be documented and addressed before release to production status.

Detailed procedures for this process are documented in DHHS-2013-001-A *DHHS Securing Hardware and Software Standard*.

9.4 HIPAA Risk Assessment

It is DHHS policy that all DHHS divisions, departments, and program areas who use, create, process, receive, transmit, or store electronic PHI (hereinafter referred to as "PHI Owner") will maintain a current HIPAA Risk Assessment for the handling and protection of PHI.

The HIPAA Privacy Officer and DHHS ISO (serving as the DHHS HIPAA Security Officer) will be jointly responsible for scheduling and managing HIPAA Risk Assessments. HIPAA Risk Assessments will be a joint venture between the HIPAA Security and Privacy Officers and the PHI Owner.

HIPAA Risk Assessments will be conducted:

- At minimum, once every five (5) years
- When significant changes to the protection of electronic PHI occur
- Before any new IT resource or data systems that may affect the handling or protection of PHI are implemented.

Detailed procedures for this process are documented in the DHHS-2013-001-C *DHHS IT Risk Management Standard*.

10.0 Incident Management, Contingency and Disaster Recovery Planning

10.1 Incident Management

DHHS will maintain a Security Incident Response Program that will be in effect 24 hours per day, 7 days per week. This program will define detailed procedures to follow for monitoring and responding to security incidents. It will identify a DHHS Crisis Management team and include procedures for assessing impact, reporting to authorities, repairing damage, and restoring normal operations. Detailed standards and procedures are included in DHHS-2013-001-E *DHHS IT Incident Management Standard*.

10.2 Contingency and Disaster Recovery Plans

DHHS business units are required to prepare a Contingency Plan that addresses: the criticality of the work being performed by Staff throughout DHHS, the designation of essential personnel, documentation of required information, alternate work procedures, and overall contingency procedures. These Contingency Plans will include procedures to be followed should information or systems become unavailable to Staff for a pre-determined period of time, and should be commensurate with the criticality, classification, and currency of information or system needs by DHHS business units.

DHHS IS&T is required to prepare a Disaster Recovery plan that meets recovery time objectives, recovery point objectives; and addresses equipment failure, alternate infrastructure facilities, and alternative network connectivity. These plans will be reviewed and updated annually, or anytime significant changes occur within the DHHS infrastructure or business units.

10.3 Testing

Incident management plans, business continuity plans, and disaster recovery plans will be tested on an annual basis. Test plans will be prepared in advance, and testing results will be documented. Action plans to resolve gaps identified during the testing will be established and managed.

11.0 Securing Hardware and Software

Only DHHS-authorized hardware or software is permitted within the DHHS Infrastructure. Requests for additional software must be submitted through authorized channels. Personal software is not allowed. Documentation of key systems within DHHS will be maintained and secured as Proprietary information. DHHS Staff is prohibited from downloading or installing software unless this activity is approved as part of Staff assignment and authorized by IS&T. Detailed standards and procedures for securing hardware and software are documented in DHHS-2013-001-A *DHHS Securing Hardware and Software Standard.*

11.1 Monitoring for Authorized Hardware and Software

DHHS will perform regular monitoring and tracking to ensure that only authorized hardware and software exist within the DHHS Infrastructure. This activity will be documented.

11.2 Server Hardening

All DHHS servers will be located within a secured facility that is approved by the DHHS ISO. Servers that access or store Confidential or Highly Restricted information will be "hardened" according to DHHS-2013-001-A *DHHS Securing Hardware and Software Standard*. DHHS will implement automated mechanisms to detect unauthorized changes to hardened servers.

11.3 Configuration and Change Management

IS&T Staff are required to follow Configuration and Change Management standards (as defined in DHHS-2013-001-A *DHHS Securing Hardware and Software Standard* when making any hardware or software change to the production baseline. Change Management must include, at a minimum, change approvals and change logging and tracking. Configuration Management must include, at a minimum, up-to-date documented configuration baselines for hardware and recoverable production software code.

11.4 Inventory

DHHS will maintain and secure an accurate inventory of all software, hardware and equipment authorized for use within DHHS including, but not limited to: system

software, servers, routers, firewalls, switches, desktop PC's, smart phones, portable digital devices, and laptops. This inventory will include appropriate and applicable licensing information, model and serial numbers, assignments, location, and documented schematics, wiring configurations, versions, and settings. This inventory will be maintained for accuracy and reviewed and audited periodically.

11.5 Change Management

All new enhancements or changes to software or hardware within the DHHS infrastructure must go through a formal change management and approval process before becoming operational. Detailed requirements for Change Management are documented in DHHS-2013-001-A *DHHS Securing Hardware and Software Standard.*

11.6 Hardware Reuse

It is DHHS policy that all information systems hardware storage media that have the potential of storing non-public DHHS information will be sanitized using approved mechanisms prior to disposal, release from DHHS, or release for reuse. This activity will be tracked and recorded.

12.0 Securing Communications and Networks

12.1 Firewalls

DHHS will maintain a tightly controlled and secured firewall that denies all traffic by default using stateful inspection. All firewall maintenance (hardware or software) will include detailed logs of changes, and these logs will be classified as Confidential Information and kept in a secure location.

12.2 Foreign Equipment

Equipment not managed, controlled, or authorized by DHHS will not be allowed to access the DHHS internal network areas that contain Confidential or Highly Restricted information. Confidential or Highly Restricted information will not be stored on any device not owned, managed, or authorized by DHHS IS&T.

12.3 Remote Access

Remote or external connectivity to the DHHS internal network will require multi-factor authentication if accessing any Highly Restricted information. Any remote access to Confidential or Highly Restricted information will be restricted to DHHS-controlled access points. See DHHS-2013-001-B *DHHS IT Access Control Standard* for detailed instructions on remote connectivity requirements.

13.0 Security Education and Awareness

13.1 New Hire Training

All Staff are required to attend security training as part of their orientation. Staff will sign an acknowledgement of understanding of the security policy and their obligations to comply with the policy no later than 30 days after their hire date.

13.2 Annual Refresher Training

On an annual basis, all Staff of DHHS are required to complete a Security and Privacy training session. DHHS will maintain records of all attendance for New Hire and Refresher training.

13.3 Federal Tax Information (FTI)

All Staff who have access to Federal Tax Information (FTI) are required to complete special training and annual recertification on handling and disclosure of FTI prior to accessing this data. This includes any Staff who have potential exposure to FTI as an incidental result of their job duties.

14.0 Definitions & Reference

See DHHS Information Technology Dictionary for definitions and references identified in this policy.

15.0 Revision History

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

Signature:

Eric Henrichsen Date: 9/30/2013

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