Information Technology (IT) Security Policies and Standards

Revision History and required review:

DHHS IT Security Policies and Standards shall be reviewed and updated annually or as significant changes to policy, procedures, or standards occur. A full review and revision of DHHS IT Policies and Standards shall occur every three years.

Version	Approved/Reviewed By	Date Reviewed	Summary of Changes
1.0	Chris Hill	6/29/2018	New
1.0	Mark Nelson	9/30/2019	Review
1.0	Mark Nelson	9/30/2020	Review
1.0	Mark Nelson	9/30/2021	Review
1.1	Mark Nelson	12/01/2021	Updates
2.0	Mark Nelson	9/12/2022	Updates
2.1	Mark Nelson	1/30/2024	Updates

Recoverable Signature

X Mark Nelson

Mark Nelson
IT Manager
Signed by: 22e45306-58c7-4711-b913-bc463a1ebdf2

1.0 SCOPE

The DHHS IT Security Policy applies to all DHHS personnel, contractors, consultants, temporary employees, volunteers, vendors, and business partners (herein collectively referred to as “Staff”) with access to DHHS or State of Nebraska IT resources owned, leased or supported by DHHS, OCIO, or any outside entity that has a signed Third-party or Business Partner Agreement with DHHS. Staff granted access to DHHS IT resources are required to make themselves familiar with and abide by all safeguards listed in this policy and the standards and procedures associated with this policy.

The IT environment includes all IT resources administered and managed by DHHS Information Systems & Technology (IS&T) and the State of Nebraska Office of the Chief Information Officer (OCIO). Implemented safeguards should be commensurate with the classification level required to protect the confidentiality, integrity, and availability of DHHS information.

DHHS Information Technology Policies and Standard are written and implemented to provide guidance on requirements, use, and reporting for the IT resources used in the Agency’s day-to-day operations.

2.0 PURPOSE

This policy provides guidance and define the minimum administrative, technical, and physical safeguards and procedures necessary to maintain a secured environment commensurate with the classification level required to protect the confidentiality, integrity, and availability of DHHS information and all IT resources administered and managed for DHHS by the Information Systems & Technology (IS&T) Division and the State of Nebraska Office of the Chief Information Officer (OCIO).

The DHHS IT Security Policy shall be reviewed and updated annually or as significant changes to policy, procedures, or standards occur. A full review and revision of DHHS IT Policy shall occur every three years.

3.0 POLICY

Policy Enforcement: Violation of the DHHS IT Policy may result in criminal and/or monetary penalties for DHHS and Staff determined to be in violation of these standards as it includes compliance with federal and state regulations.

3.1 If a violation of this policy and/or any associated policy standard occurs, the offending individual's supervisor or manager is responsible to mitigate or remediate the violation in a timely manner.

3.2 DHHS Staff found in violation of this policy and/or any associated policy standard shall be held accountable for their actions and any reasonable, foreseeable consequences of those actions. The staff member may be disciplined in accordance with the applicable workplace policies and labor contracts administered by DHHS Human Resources. Such discipline may include restitution for damages caused by improper use and termination of employment.

3.3 Staff working for a DHHS External Partner to provide services to or on behalf of DHHS found in violation of this policy and/or any associated policy standard 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.

3.4 Lack of knowledge or familiarity with this policy and/or any associated policy standard shall not release an individual from their responsibilities.

4.0 CONFLICTS

DHHS is required to comply with appropriate Federal regulations when using protected information such as PHI, FTI and Social Security information. If there is conflicting guidance, the more restrictive rules shall apply.

5.0 POLICY EXCEPTION

5.1 The Agency recognizes that business requirements may dictate long or short-term solutions contrary to DHHS or State of Nebraska IT Security Policies and Standards and may require policy exceptions. All requests for exceptions to this policy and/or any associated policy standard will be made in writing and include a risk and impact analysis and a plan for mitigation of the risk of the policy exception. The OCIO or DHHS must approve exceptions in advance.

5.2 Specific details and procedures for requesting a policy exception are included in the DHHS Information Technology Policy Exception Procedure.

5.3 Exceptions or waivers at the State of Nebraska enterprise level must be coordinated through the OCIO per NITC 1-103

6.0 POLICIES AND STANDARDS

Staff are required to review, understand and comply with State and Agency policies and standards. A brief description of DHHS IT Policy is contained in this section.

6.1 DHHS IT Security Policy (Section 1) is the base document and provides initial guidance. It also describes the Information Classification and required protection standards for all information used within the State of Nebraska network.

6.2 Securing Hardware and Software (Section 2) outlines the methodology and requirements for inventory control, test, implementation, and maintenance required to apply the necessary configuration settings on all hardware and software used to create, receive, store, process, access or transmit data owned by DHHS or hosted by third-party organizations on behalf of DHHS. It includes software development standards and describes the procedures to follow when hardening servers, network devices, and workstations. Configurations are based on security controls prescribed by the most current versions of federal guidance, to include, but not limited to: the National Institute of Standards and Technology (NIST) Special Publications (SP), Federal Information Processing Standard (FIPS) 140-2, and IRS Publication 1075. This standard also provides direction to ensure that servers, infrastructure, and workstations deployed at DHHS are inspected for compliance with this standard at least annually and as prescribed by applicable regulatory compliance.

6.3 Access Control (Section 3) defines requirements for UserID, passwords, minimum necessary permissions for Staff based on job requirements, separation of responsibilities, protection of access controls, and requirements for remote access to the DHHS network environment.

6.4 Risk Management (Section 4) defines requirements by DHHS to implement policies, standards, and procedures to detect, contain, correct or prevent security deficiencies. This standard also provides guidance in conducting risk analysis and management to ensure adequate resources are in place to ensure compliance with appropriate DHHS and Federal guidance.

6.5 IT Security Reporting (Section 5) gives the AISO an avenue to provide DHHS leadership with appropriate information in a consistent format to support fact-based decision-making and allocation of future funding, as well as ensuring compliance with Federal Agency requirements for systems containing sensitive client information. Consistent reporting standards will also help to ensure that information security controls are consistent across the enterprise, meet all necessary requirements, and are appropriate for the levels and types of risk facing DHHS and its information assets. Formal reporting helps keep the information security mission consistent, well understood and continually progressing as planned.

6.6 IT Incident Management (Section 6) includes multiple processes throughout DHHS and IS&T. This Standard identifies key steps for promptly reporting and responding to security incidents and establishes formal reporting requirements for all such instances to the AISO, DHHS Privacy Officer, State officials, and DHHS customers. It also includes a number of operational and technical components, which provide the necessary functions in order to support all the fundamental steps within the Incident Management Life Cycle, including Preparation, Identification, Containment, Communication, Eradication, Recovery, and Root Cause/Remediation. It is a necessary component to Information Technology strategy and long term planning. State and Agency policy, the Federal Information Security Management Act (FISMA), HIPAA, CMS, SSA and IRS regulations require incident management policy and procedures.

6.7 IT Auditing (Section 7) provides direction and assurance that DHHS maintains and retains audit log records according to policy. It also defines State of Nebraska, DHHS and Federal Agency document retention requirements. Further, this policy standard defines requirements for the Agency to maintain audit logs as evidence that may be necessary for investigations, forensics, or legal discovery purposes.

6.8 IT Security Education and Awareness Training (Section 8) provides guidance on required and recommended training necessary to ensure Staff are provided with necessary information so they are apprised, and remain aware of current and pending data security and privacy requirements.

6.9 IT Media Protection and Disposal (Section 9) provides guidance for ensuring all forms of media (e.g., internal and external storage devices, print media, etc.,) are protected through encryption and secure storage. It also provides high-level direction for properly disposing of media when it is no longer serviceable or required.

6.10 IT Acceptable Use Policy (Section 10) provides authorized users with guidance for the proper use of DHHS IT resources, to include internet, applications, DHHS data, and secure e-mail.

6.11 IT Contingency Planning (Section 11) provides framework for identifying roles and responsibilities, prioritization, implementation, training, and exercising agency plans, policies, standards, and procedures in the event of a contingency. The Agency must have a Business Continuity/Disaster Recovery plan that integrates all agency activities, to include Operations and IT functions, as well as any external dependencies, should an event affect one or more business areas.

6.12 Acronyms and Definitions provide the most common acronyms and terminology with associated definitions used by the Agency.

THIS PAGE INTENTIONALLY LEFT BLANK

Section 1 - DHHS Information Technology (IT) Security Policy

7.0 INTRODUCTION

All State of Nebraska Department of Health and Human Services (herein referred to as 'DHHS' or 'the Agency') personnel have an obligation to protect the Information Technology (IT) resources they handle from intentional or accidental misuse or damage.

DHHS provides diverse services across a wide geographical area. Contractual relationships required to fulfill the Agency's missions, policies, standards, procedures and appropriate safeguards must be implemented to meet State and Federal security and privacy regulations and ensure a secure computing environment that meets the unique business requirements of the Agency.

DHHS IT Resources include, but are not limited to: computer hardware, software, data storage (to include removable media such as USB flash drives, writeable DVDs and external hard drives), portable digital devices (e.g., smart phones, tablet computers, etc.), network communication infrastructure, network access, Internet/Intranet access, and electronic communication (i.e., email, instant messaging, and data exchange), as well as any data created, received, stored, processed or transmitted by the Agency.

DHHS IT policies and associated policy standards are written to complement the Nebraska Information Technology Commission (NITC) policies and standards and place emphasis on the Agency's unique requirements.

Additionally, Agency policies, standards, and procedures are used to relay and enforce appropriate Federal guidance as provided by the Internal Revenue Service (IRS), Centers for Medicare and Medicaid Services (CMS), Social Security Administration (SSA), and the Health Insurance Portability and Availability Act (HIPAA), to name a few. DHHS IT Policy also serves as guidance to support any division-level security policies.

7.1 Purpose and Objectives.

7.1.1 This policy and associated standards provide guidance and define the minimum administrative, technical, and physical safeguards and procedures necessary to maintain a secured environment commensurate with the classification level required to protect the confidentiality, integrity, and availability of DHHS information and all IT resources administered and managed for DHHS by the Information Systems & Technology (IS&T) Division and the State of Nebraska Office of the Chief Information Officer (OCIO).

7.1.2 The primary objectives of this policy are to:

7.1.2.1 Provide clear direction to all Staff on their obligations to safeguard information, and procedures to follow to minimize the risk of security incidents.

7.1.2.2 Establish clear accountability and authority for developing, administering, and ensuring compliance with security policy across all of DHHS.

7.1.2.3 Promote a focus on security and privacy existing at key touch points throughout DHHS so security and privacy become institutionalized and integrated functions.

7.1.2.4 Establish and maintain a secure, resilient, and controlled information technology infrastructure and environment.

7.1.2.5 Ensure administrative, physical, and technical safeguards are compliant with all applicable Federal, State, and Agency mandates.

7.1.2.6 Ensure adequate and appropriate planning is in place in the event of a security incident or an event affecting business continuity and recoverability.

7.1.2.7 Establish effective risk management commensurate with the sensitivity of information used and potential impact of information loss, damage, or exposure.

7.2 Information Classifications (categorization)

Information shall be categorized (classified) based on content and the level of protection required to ensure its security. Information classification shall apply to all information in any form, including, but not limited to: web-based data, email messages, printed material, facsimile (fax), digital messages, voice mail, and personal conversations.

DHHS is required to implement appropriate technical, physical, and administrative safeguards to protect the confidentiality, integrity, and availability of all Agency information in a manner commensurate with its classification level.

7.2.1 All Staff must be able to recognize and appropriately categorize the information they access, use, or are exposed to, into one of the following categories to maintain appropriate levels of information confidentiality, integrity, and availability.

7.2.1.1 PUBLIC information is approved by official State or Agency 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 State of Nebraska public-facing websites
- 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

7.2.1.2 INTERNAL USE ONLY information is not intended or approved for public release and requires additional protection. It is not sensitive to the extent that it contains CONFIDENTIAL or RESTRICTED information. Examples include, but are not limited to:

- Agency 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:

- Implementation of security safeguards to ensure the confidentiality and availability of the information
- Access is restricted to authorized personnel only

7.2.1.3 CONFIDENTIAL information is restricted to individuals who have approved access to this information and require access to perform their assigned duties. Examples include, but are not limited to:

- Personally identifiable information (PII)
- Protected health information (PHI)
- Employee Human Resources (HR) records, including performance ratings and payroll information
- Social Security numbers
- Attorney/Client privilege information
- System configurations and system-specific disaster recovery procedures

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

- Information will be segregated and maintained in secured environments
- Access is limited to individually identifiable accounts with appropriate minimum necessary permissions to access data
- Information will be encrypted per DHHS and State of Nebraska standards when in transit outside of the internal network (such as email)
- Information stored on removable or portable media (such as laptops, USB flash drives, or smartphones) must be encrypted using approved technology.
- Remote access to CONFIDENTIAL Information requires multi-factor authentication

7.2.1.4 RESTRICTED information is any critical and sensitive information to which access is limited to a very small subset of individuals requiring access 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)
- System log information
- Attorney/Client privilege information

- Federal tax information (FTI)

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

- Enhanced logging and auditing

8.0 POLICY

8.1 POLICY STATEMENT

8.1.1 Electronic and physical security safeguards must be implemented as defined in this policy and associated standards, as well as applicable state and federal guidance, and meet an acceptable level of risk. Updates to safeguards will be tested and implemented in accordance with state and federal statutes.

8.1.2 This policy and all related standards, procedures, strategies, and plans are designed to complement all Nebraska Information Technology Commission (NITC) security policies and standards. It is the responsibility of the DHHS (Agency) Information Security Office (AISO) to ensure appropriate review of compliance occurs on a regular basis.

8.2 ROLES AND RESPONSIBILITIES

8.2.1 DHHS Chief Information Officer (CIO)

8.2.1.1 The Agency CEO has authorized the DHHS Agency CIO to serve as the authority to establish and ratify Security Policy. The Agency CIO is a full-time equivalent (FTE) position hired and funded by the Agency.

8.2.1.2 The DHHS CIO will serve as the Security activity approval authority, with recommendation from the AISO 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.

8.2.1.3 DHHS IS&T is charged with the responsibility for implementing and maintaining adequate and appropriate security safeguards that comply with the Security Policy.

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

8.2.2 DHHS (Agency) Information Security Officer (AISO)

8.2.2.1 DHHS will assign an Agency Information Security Officer (AISO) who will have oversight responsibility to ensure appropriate and adequate IT policies, processes, and procedures are applied to protect the confidentiality, integrity and availability of information in the DHHS environment.

8.2.2.2 The AISO is responsible for effectively managing the Agency's overall security program and will 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.

8.2.2.3 The AISO is authorized to conduct IT audits, reviews, and assessments to determine the level of compliance with DHHS IT Security Policies and Standards. The AISO 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.

8.2.3 DHHS Division Senior Management

8.2.3.1 The DHHS Division senior Leadership shall incorporate and enforce compliance with DHHS IT policies and associated standards into their Division's operational procedures. DHHS divisions include:

- Behavioral Health
- Children and Family Services
- Developmental Disabilities
- Medicaid and Long Term Care
- Operations
- Public Health

8.2.4 DHHS Agency-Wide Support Department Management

8.2.4.1 DHHS Agency-Wide Support Department leadership is responsible 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:

- Accounting and Finance
- Communications and Legislative Services
- Human Resources
- Information Systems and Technology (IS&T)
- Internal Audit
- Legal Services
- Procurement

8.2.5 DHHS Security Administrator

8.2.5.1 DHHS Security administrators are comprised of:

- Staff assigned an additional duty of security administrator.
- Sponsors of external entities.
- Supervisors.

9.0 SECURITY OVERSIGHT AND COMPLIANCE

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

The AISO 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 RESTRICTED information.

9.1 Acceptable Use

9.1.1 DHHS-provided technology, such as individual computer workstations or laptops, computer systems, networks, email, and Internet software and services, is intended for authorized business purposes only. All Staff will be required to review and comply with the DHHS IT Acceptable Use Policy.

9.2 Consent to Monitor

DHHS is responsible for servicing and protecting DHHS equipment, networks, information, and resource availability. As such, Staff use of DHHS IT resources is subject to monitoring by the Agency and OCIO. This includes, but is not limited to emails, Internet usage, telephone calls, instant and text messaging, or other electronic communications.

9.2.1 Monitoring is necessary to perform optimization of IT resources, troubleshooting and repair of technical problems, analysis for capacity and performance planning, and for detecting patterns of unauthorized activity.

9.2.2 Staff are provided a ‘Consent to Monitor’ statement prior to logging in to certain resources or applications. By accepting the terms of the statement, the staff member understands and agrees that their activities are monitored and logged. Terms of the statement must be accepted before being presented with the logon screen.

9.3 Security in Contracts, Agreements, RFPs/RFIs, and SOWs

9.3.1 All contracts, business partner agreements, Requests for Proposal, Requests for Information, Statements of Work, or other third-party arrangements that involve CONFIDENTIAL or RESTRICTED information shall include an acknowledgement and agreement by the business partner to meet security policy and minimum-security requirements of DHHS. This agreement shall include provisions to allow for compliance reviews or assessments to ensure security requirements of DHHS are continually managed. All contracts must include:

9.3.1.1 Appropriate DHHS IT Security language provided by IS&T and approved by the DHHS Legal department.

9.3.1.2 Appropriate Federal entity (e.g., IRS, CMS or SSA) security language as required if a contracted service will be storing or maintaining sensitive client information such as PHI or FTI.

9.3.2 Business Partners are required to notify DHHS of any security incidents affecting or involving CONFIDENTIAL or RESTRICTED DHHS information in a timeframe and manner commensurate with the information classification, magnitude of exposure, and potential impact to DHHS or clients. Incidents involving or with the potential to involve CONFIDENTIAL or RESTRICTED data must be reported immediately as defined in DHHS-IT-001E DHHS IT Incident Management Standard.

10.0 SECURITY PLANNING

Appropriate planning must occur to ensure information security is adequately addressed, staffed, and funded to stay at appropriate levels for the protection and compliance of the DHHS environment.

10.1 Recurring Security Plans

The AISO will prepare a System Security Plan on an annual basis. This plan 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 quarterly basis. All security plans will be considered CONFIDENTIAL Information, and will follow the requirements and procedures as outlined in DHHS-IT-001D DHHS IT Security Reporting Standard.

10.2 Security Reviews

The AISO 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-IT-001F DHHS IT Audit Standard.

10.3 Record Keeping

The AISO will keep records of Security plan updates and versions. All records will be treated as CONFIDENTIAL information and will be appropriately secured and retained according to State of Nebraska and DHHS record retention requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

Section 2 - DHHS Information Technology (IT) Securing Hardware and Software

11.0 INTRODUCTION

DHHS uses sensitive information such as PII, PHI, and FTI on a regular basis. The foundation of protecting information lies in the security of the Agency's network infrastructure. State and Federal regulations require DHHS to incorporate appropriate administrative, physical, and technical controls commensurate with appropriate information classification levels into all hardware and software used to store or process any DHHS information.

11.1 Purpose and objectives

Improperly configured network components (servers, workstations, routers, applications, etc.,) are at risk to compromise, increasing the potential to have data lost, stolen, improperly accessed, modified, or destroyed. This standard provides guidance to DHHS IS&T teams and related third parties on security requirements for hardware and software used to store, process, or access DHHS electronic information, to include all DHHS-supported or branded applications, web services, and websites hosted by third parties.

11.2 Roles and Responsibilities

Roles and responsibilities for appropriate levels of DHHS Staff and/or management are identified in the DHHS Information Technology Security Policy. Additional roles and responsibilities are as follows:

11.2.1 Information Systems and Technology

11.2.1.1 Identify authorized personnel who will perform required maintenance on Agency systems

11.2.1.2 Coordinate with the OCIO to ensure State of Nebraska network infrastructure is secure, and that enterprise-level configurations allow the full functionality of agency-specific applications.

11.2.1.3 Coordinate changes within the agency and identify any potential network security risks of those changes.

12.0 STANDARDS

Standards are necessary to provide additional guidance as an effort to help protect DHHS from the liability of unauthorized data or activity residing or occurring on DHHS equipment. Properly applied configuration standards are also necessary to help reduce the likelihood of malicious activity propagating throughout DHHS networks. The State is responsible for implementing these standards through the proper configuration and management of DHHS hardware, software, and imaging processes. All other DHHS staff are responsible for reporting anomalous behavior of computers, servers and applications.

The Technical Services Document Library (restricted access) contains specific details for each type of DHHS server or application used or accessed by DHHS Staff. This library is updated as hardware and software requirements change.

Use the following guidance to identify, test, implement, and maintain appropriate security controls for DHHS hardware and software. Applicable guidance may include, but is not limited to:

- National Institute of Standards and Technology (NIST) Special Publications

- Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- Center for Internet Security (CIS) benchmarks
- Internal Revenue Service Publication 1075
- Federal Information Processing Standards (FIPS) 140-2

12.1 Authorized Personnel

12.1.1 Only authorized personnel with appropriate accounts and permissions may perform maintenance on Agency IT resources.

12.1.2 The Agency shall maintain a list of authorized system maintenance personnel.

12.1.3 Although authorized personnel may not have direct access to Federal Tax Information (FTI), authorized personnel accessing systems containing FTI must complete an appropriate background check (to include fingerprinting) per IRS requirements, as well as identity proofing conducted by Human Resources.

12.1.4 Third-party vendors contracted to perform maintenance must have signed confidentiality or other appropriate non-disclosure agreements with DHHS.

12.2 Encryption Standards

12.2.1 When configuring systems used to create, access, process, or store CONFIDENTIAL or RESTRICTED data, use FIPS 140-2 standards or an equivalent level of protection, for encrypting:

12.2.1.1 Data at rest;

12.2.1.2 Transfer of data (to include secure e-mail);

12.2.1.3 Applications (to include web applications); and

12.2.1.4 Laptop computers (full-disk encryption);

12.2.2 Encryption key management will be controlled and managed by DHHS. This may require an escrow service for key storage.

12.3 Server Hardening Standard

DHHS depends on properly configured servers to deliver data in a secure, reliable fashion and requires assurance that key servers will maintain information confidentiality, integrity, and availability.

12.3.1 Systems Administrators shall install, configure, and maintain servers in a consistent manner to prevent unauthorized access or disruptions in service. Harden all servers with the potential to store, process, or access CONFIDENTIAL or RESTRICTED data according to these standards and appropriate NIST, Internal Revenue Service, Social Security Administration, Centers for Medicare and Medicaid Services and other applicable federal guidance.

12.3.1.1 Use standardized and appropriately configured software baselines to load and configure hardened servers prior to deployment. These processes and software shall be protected with integrity controls to ensure only authorized and documented changes are possible.

12.3.1.2 DHHS maintains and operates several disparate systems and applications; as such, automatic patching may cause system or application failures. As a compensating control, test and apply security patches 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).

12.3.1.3 Remove or disable unnecessary default software, system services, ports, protocols, accounts and drivers if doing so will not negatively affect the overall operation of the server or DHHS applications. If this is not possible, identify any compensating controls and document the configuration plan accordingly.

12.3.1.4 Change all default passwords. Create and periodically change passwords using the guidance of the DHHS IT Access Control Standard and system/application requirements. Ensure passwords are securely stored.

12.3.1.5 Enable audit logging to provide a running history of activity on the servers. Audit logs will be secured and only accessible to accounts with privileged access (refer to the Audit standard). Audit logs shall be maintained in accordance with the DHHS IT Audit Standard and applicable Federal guidance.

12.3.1.6 Security parameters and file protection settings must be established, reviewed, and approved by IS&T, as well as OCIO.

12.3.1.7 Servers shall not be connected to the DHHS network until hardening standards are met and approval to connect is granted by IS&T Management.

12.3.1.8 Servers shall have approved and current antivirus, intrusion detection and protection, and/or end-point security monitoring software installed and activated. Active monitoring software shall have the capability to alert IS&T administrative personnel of anomalous activity within 24 hours.

12.3.1.9 Maintain Servers in facilities offering multiple layers of physical protection, to include being installed in locked cabinets.

12.3.1.10 Sanitize or destroy equipment scheduled for disposal or recycling following appropriate federal media disposal guidelines.

12.3.2 In addition to the configuration management standards listed in section 12.3.1, all servers designated as “Hardened” shall have a Hardened Server Configuration Management Plan. The configuration management plan shall be marked as CONFIDENTIAL and protected accordingly. IS&T will review and update this plan annually or prior to any significant change to the hardened server baseline. This plan shall include, at a minimum:

12.3.2.1 Cover page clearly marked “CONFIDENTIAL”

12.3.2.2 Roles and responsibilities of IS&T Staff.

12.3.2.3 Location of server(s) within the DHHS infrastructure, including network diagrams

12.3.2.4 Detailed inventory of authorized software residing on server(s) and the number of users anticipated

12.3.2.5 Detailed inventory of server hardware, manufacturer, model and serial numbers, configuration settings, and specifications. Include description of purpose, business departments using the server(s) and the anticipated number of users.

12.3.2.6 Emergency server change procedures.

12.3.2.7 Hardened Server Change Request Process and the location where resulting information will be stored.

12.3.2.8 Security impact analysis and summary report

12.3.2.9 System Security Plan and Contingency Plan updates

12.3.2.10 Schedule of scanning for authorized software and settings

12.4 Workstation Security Standards

Agency managed workstation hardware and software are subject to change based on agency requirements; specific workstation standards are maintained in the Technical Services Document Library. The degree of workstation protection should be commensurate with the information classification of the resources stored, accessed, transmitted or processed. Use the following guidance when configuring workstations:

12.4.1 Authorized maintenance personnel shall install, configure, and maintain workstations in a consistent manner to prevent unauthorized access or disruptions in service. Configure workstations with the potential to store, process, or access CONFIDENTIAL or RESTRICTED data according to these standards and appropriate NIST or other applicable federal guidance.

12.4.1.1 Use standardized and appropriately configured software baselines as defined in the Technical Services Library to load and configure all workstations and laptop computers prior to deployment. These processes and software shall be protected with integrity controls to ensure only authorized and documented changes are possible. Standard workstation loads shall be documented and updated as required to ensure the most current security settings are implemented.

12.4.1.2 Automatic patching of workstations may cause system or application failures. As a compensating control, security patches shall be tested and applied as defined by the Change Management Process. Base priority setting of vulnerabilities on impact to DHHS and as referenced in the National Vulnerability database (HTTP://nvd.nist.gov).

12.4.1.3 Change all default passwords. Blank or default system passwords are vulnerable to compromise and can allow unauthorized access of deployed network systems.

12.4.1.4 Configure systems to enforce password complexity standards on accounts. This may be achieved through group policy.

12.4.1.5 Remove or disable unnecessary software, services, ports, protocols, accounts and device drivers if doing so will not adversely affect the overall operation or performance of the computer or DHHS applications. Implement and document reasonable and appropriate compensating controls to reduce the risk of unauthorized access or use of software, services, accounts or drivers that cannot be removed or disabled.

12.4.1.6 Application software may be installed if there is a valid business requirement AND if it is approved, licensed, and secured. Applications shall receive security updates as defined by patch management standards.

12.4.1.7 Approved intrusion detection, endpoint security and antivirus software must be installed and enabled.

12.4.1.8 Host-based firewalls must be enabled if the workstations are removed and operated independently from the DHHS internal network.

12.4.1.9 Workstations shall automatically lock after 15 minutes of inactivity.

12.4.1.10 Sanitize or destroy equipment scheduled for disposal or recycling following appropriate federal media disposal guidelines.

12.4.1.11 All DHHS owned or managed portable devices (e.g., laptops) must be full-disk encrypted using approved technology. Encryption technology will be provided or approved by IS&T and must be FIPS 140-2 compliant or have an equivalent level of protection implemented.

12.4.1.12 All publicly accessible devices (e.g., agency-managed kiosks, etc.) connected to the DHHS Network must be:

12.4.1.12.1 Physically located in a monitored environment; and where applicable, access credentials must be managed by authorized personnel

12.4.1.12.2 Registered and documented in the DHHS Inventory.

12.4.1.12.3 Logically connected in the DHHS DMZ unless approved by IS&T management to connect to the DHHS LAN for legitimate business purposes.

12.5 Network and portable Device Security Standards

DHHS encourages the use of the State of Nebraska electronic communications infrastructure to support its mission. This infrastructure must be well managed and protected to ensure the security of DHHS information. Therefore, all devices that connect to the DHHS network must adhere to the following standards:

12.5.1 Secure all devices with a password-protected screen saver that automatically locks the computer or terminates the session after 15 minutes of inactivity.

12.5.2 All devices connected to the DHHS network shall have approved anti-virus, spyware protection, or other automated security scanning technologies installed and fully operational, as applicable to the device.

12.5.3 Devices (i.e., laptops) 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 security posture of other systems.

12.5.4 Do not send passwords and SNMP community names in clear text over open networks. All devices must use authorized encryption methods for access to the internal network. Access to systems and applications in the DMZ applications is exempt from this requirement.

12.5.5 Follow approved change control and configuration management procedures to make recommended configuration changes or install patches and hot-fixes. All changes must be thoroughly tested prior to implementation.

12.5.6 Based on impact to DHHS systems, prioritize vulnerability mitigation strategy as referenced in the National Vulnerability database (HTTP://nvd.nist.gov).

12.5.7 Remove or disable unnecessary software, services, ports, protocols, accounts and device drivers if doing so will not adversely affect the overall operation or performance of the computer or DHHS applications. Implement and document reasonable and appropriate compensating controls to reduce the risk of unauthorized access or use of software, services, accounts or drivers that cannot be removed or disabled.

12.5.8 Network infrastructure (routers, hubs, switches, etc.,) should be maintained in facilities offering multiple layers of physical protection, to include being installed in locked cabinets.

12.5.9 Collaborative computing devices and software (e.g. networked white boards, cameras, and microphones) are not permitted to access FTI.

12.5.10 Discussing FTI over a VoIP network is not permitted.

12.6 Application Development Security Standards

This standard applies to all software applications developed, maintained or administered by DHHS personnel and to all software residing on DHHS infrastructure used to create, store, process, or access DHHS CONFIDENTIAL or RESTRICTED data to help increase the security of applications and safeguard DHHS IT resources. The following items are required in all application software within the scope of this standard:

12.6.1 Maintain current documentation to include an assessment of security threats and impacts and a detailed description of data handling with its accurate classification.

12.6.2 Applications that provide user interfaces shall display an appropriate warning banner applicable to the data being accessed (i.e., HIPAA or FTI), and appropriate warning notifications on each screen containing such information.

12.6.3 Application credentials, where possible, should be inherited from a DHHS Managed Authentication Source. If that is not possible, credentials should have the same level of management and approval as other DHHS access credentials.

12.6.4 Application development and implementation must follow the change management process, which includes security oversight at specific handoff points of the SDLC such as going from requirements definition to a design stage. Document any security implications of application changes. Thoroughly test all applications before release to the production network.

12.6.5 Use artificial or de-identified data for testing. If using artificial or de-identified data is not possible, secure the testing environment to a production-class level to meet safeguarding requirements necessary to protect the information. NOTE: Use of live FTI for testing must be approved by the IRS prior to testing.

12.6.6 Applications that process CONFIDENTIAL or RESTRICTED data must have a security plan defining critical service levels. The plan must be reviewed and approved by an appropriate level of Agency management.

12.6.7 Manage application software in a secured environment. Make changes in a non-production environment. After successful testing and approval, changes may then be migrated to the production environment. DHHS shall maintain at least three versions of application software, and all versions shall maintain audit trails.

12.7 Security Standards for Web Application and Services

To meet a multitude of different needs, DHHS public facing systems are diverse. Therefore, information exposures by these systems differ, as do threats. To reduce the risks from public-facing systems, ensure appropriate security controls are implemented. Because every system is different, the web application developer is the most knowledgeable about the system and its associated risks.

This standard establishes a security requirement baseline for all DHHS websites, web services, and all third party supported or hosted web applications. Maintain appropriate configuration documentation for all public-facing applications as evidence of compliance 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).

12.7.1 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

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

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

12.7.4 Validate all input fields before accepting. Check inputs to prevent the program from executing malicious code. Validate input length to determine if it is within the predetermined minimum and maximum range. Screen input values for valid data types (e.g., number or character only, no special characters).

12.7.5 Mask output fields to ensure the output does not reveal too much information that could be used for malicious intent (e.g., default system-generated messages should be translated by the application). Invalid user inputs should generate error messages that do not reveal the specific component causing the error. Messages should be general in nature, and not reveal any more information than necessary.

12.7.6 Authenticate the identity of the user. All user credentials and passwords must meet DHHS policy requirements for uniqueness, strength, change, and history. Limit user access and capability to the functions required for the authorized access level.

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

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

12.7.9 All external systems (including web services) requiring access to the application must be authenticated and permissions checked before the external system becomes trusted.

12.7.10 Mask password entry fields so passwords entered are not displayed in clear text. Disable auto-complete of all fields. Logon credentials may not be stored on the website

12.7.11 Disconnect all sessions when the user logs out of the system, closes the web browser, or after a pre-determined time.

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

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

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

12.8 Security Requirements for Cloud Services and Cloud Service Providers

All Cloud Service Providers (CSPs) must have an official FedRAMP certification by an accredited third-Party Assessor Organization (3PAO), or alternatively, the following conditions must be 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 RESTRICTED data:

12.8.1 The CSP or third party host (3PH) must provide evidence of secure storage of access credentials that are at least equal to that of DHHS internal systems.

12.8.2 Access to the cloud service requires multi-factor authentication based on data classification levels.

12.8.3 De-provisioning of credentials must occur within two (2) hours of de-provisioning of the internal system credentials.

12.8.4 Encrypt Information using IS&T approved technology for information in transit.

12.8.5 Encrypt Data at rest using FIPS 140-2 or equivalent standards.

12.8.6 All equipment removed from service that contained DHHS information must be sanitized and verified by DHHS before allowing that equipment, information storage space, or media to be destroyed or assigned for reuse. Destruction certificates must be provided to the Agency.

12.8.7 CSP/3PH will conduct vulnerability scanning and testing on a schedule approved by the AISO. Results will be provided to DHHS.

12.8.8 Patch management of hardware and software at the CSP/3PH are required to meet or exceed the same standards required at DHHS.

12.8.9 CSP/3PH will meet all DHHS requirements for chain of custody and 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 identifying a real or suspected breach.

12.8.10 CSP/3PH will provide evidence of audit and assessment of the security of the service environment, and will agree to reasonable inspection by DHHS-authorized parties.

12.8.11 CSP/3PH is required to advise DHHS on all geographic locations of DHHS information. CSP/3PH shall not allow DHHS information to be stored at, or accessed from primary or alternate operating locations outside the United States without explicit approval by DHHS. Per IRS Publication 1075 requirements, FTI may not be stored at or be accessible from locations outside of United States. To maintain consistency of information security requirements, no other sensitive DHHS information (e.g., PHI) may be stored at or accessed from offshore locations.

12.8.12 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.

12.8.13 Contracts with CSP/3PH's shall have service level agreements (SLAs) and/or business associate agreements in place that clearly define security and performance standards. Contracts shall also have appropriate verbiage for the level of information maintained (e.g., IRS, Publication 1075, exhibit 7 language for systems or functions accessing FTI). Contracts will address how performance and security will be measured, monitored, and reported. Contracts will also establish an enforcement mechanism for SLA compliance.

12.8.14 CSP/3PH will provide assurance of compliance with applicable federal and state privacy and security regulations. CSP/3PH will provide adequate security and privacy training to its associates, and provide the AISO with adequate evidence of this training.

12.8.15 CSP/3PH will provide DHHS with the ability to conduct a reasonable search to meet Nebraska Public Records Law.

12.8.16 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.

12.8.17 CSP/3PH will provide documentation, evidence, or allow reasonable access by Agency officials to ensure compliance with these standards.

12.9 Open source software

Open source software has source code that is publicly available under a license that allows users the ability to modify and distribute to meet their requirements. Due to the nature of the coding, additional restrictions may apply. Open source software must be:

12.9.1 Approved for use;

12.9.2 Obtained and legally licensed through a known, reputable vendor;

12.9.3 Documented and tracked by the agency;

12.9.4 Thoroughly tested for malware and compatibility with existing systems and applications prior to implementation;

12.9.5 Configured and secured to meet state and federal requirements for use on agency systems; and,

12.9.6 Patched using vendor provided updates after the patches have been thoroughly tested. Update procedures shall follow the agency's change management process.

12.10 System Maintenance, testing and reviews

12.10.1 Use the Change Management standards to schedule and perform system maintenance.

12.10.2 Use approved tools to scan servers monthly for vulnerabilities, unauthorized software and unauthorized changes to the configuration baselines. Address any findings affecting security posture as soon as practical.

12.10.3 Periodically conduct security scans and tests on web applications. Test high risk or impact applications at least annually or when significant changes are made. Tests shall be coordinated and supervised by the OCIO, AISO 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.

12.10.4 Authorized personnel performing server maintenance from a remote location must use an approved, secure method using multifactor authentication to access the servers. 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.

12.10.5 Conduct penetration tests of all hardened servers annually under the direction of the AISO or SISO. Record results and take appropriate action to remediate findings.

12.10.6 Record all change, maintenance and repair activity, to include a summary of the activity, the individual performing the change and the change completion date.

12.10.7 Network scanning is prohibited unless prior approval is obtained from the AISO, SISO and IS&T management. If approved, network scanning is conducted by authorized personnel only, and restricted to authorized and registered IP addresses.

12.10.8 No person at DHHS shall monitor network traffic unless the AISO, SISO, DHHS Human Resources, or DHHS Legal approve this activity in advance or the network monitoring activity is part of their normal job duties. IS&T shall implement measures to restrict network monitoring to authorized personnel only.

12.10.9 The AISO and IS&T are responsible for establishing a schedule for periodic review and inspection of hardware and software to ensure compliance with defined hardware and software standards. Minimum requirements include:

12.10.9.1 Annually review configuration standards for all desktop and laptop computers, servers, and network devices.

12.10.9.2 Annually perform compliance inspections of hardware and software standards. Inspections may occur more frequently as circumstances dictate. Document and secure all results.

12.10.9.3 The AISO shall maintain a Plan of Action with Milestones (POA&M) that reflects all outstanding security gaps, mitigation and remediation action plans, and corresponding timelines of agency-specific systems.

12.10.9.4 Maintain documentation of change management meetings, to include descriptions or reference to requested changes, and all approval or non-approval decisions.

12.10.9.5 Review and update ports, services and protocols annually or as requirements change to ensure that only required ports, services, protocols, etc. remain enabled. The AISO may initiate a review of the environment as necessary.

12.10.9.6 Verify all open ports on publicly accessible systems at least annually. These systems shall have an external penetration test conducted annually. Any requests for public IP addresses or for additional open ports must be approved by IS&T Network Management.

12.10.10 Notify the AISO within 1 hour of any suspected security incident. Any compromised device may be disconnected from the DHHS network without warning.

12.11 Change Management Standards

Change management standards address requirements for making modifications to the DHHS IT infrastructure (which includes all hardware, system software, and network assets) and application software used to access CONFIDENTIAL and RESTRICTED (which include commercial off the shelf data applications and DHHS in-house developed data application software) data. Such processes are required to ensure all changes are tracked, authorized, tested and approved for release. All changes affecting DHHS IT infrastructure, to include hardware, system software, and applications, must be submitted to the Change Control Group for review, approval, and implementation.

12.11.1 IT Infrastructure – the following standards are required:

12.11.1.1 The change management review process includes representation from IS&T, Information Security, and application development (when application changes impact or are impacted by IT infrastructure changes) and will meet with sufficient frequency to meet demands for changes to the DHHS environment.

12.11.1.2 The Infrastructure Change Control Group will keep records and documentation of meetings, decisions made, and rationale. All meeting records shall be securely stored for audit purposes. The agenda for this meeting should address a review of the following:

12.11.1.2.1 Change summary, justification and timeline

12.11.1.2.2 Test plans and results

12.11.1.2.3 Security review and impact analysis

12.11.1.2.4 Documentation and baseline updates

12.11.1.2.5 Implementation timeline, and recovery plans

12.11.1.3 Maintain baseline configuration documentation. Baseline configuration documents are CONFIDENTIAL, and must be secured appropriately. Review and update the baseline documents annually or after making any significant changes to the baseline.

12.11.1.4 Only authorized personnel using assigned credentials (e.g., privileged accounts) may make changes to the DHHS production infrastructure. The actions performed under privileged user credentials must be logged. IS&T shall maintain a current list of authorized individuals.

12.11.1.5 Document and disable all unnecessary software, services, ports, protocols, accounts and device drivers on all technology supporting the Agency if doing so will not adversely affect operations. Those that cannot be removed or disabled must have documented compensating controls or a mitigation plan.

12.11.1.6 Maintain a current inventory of all 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, auditable and kept current with the DHHS infrastructure.

12.11.2 Application Development – Use the following standards for DHHS application software systems that create, process, or store CONFIDENTIAL and RESTRICTED data.

12.11.2.1 DHHS must establish and maintain application change management processes with assigned responsibilities to ensure all changes to DHHS application software are approved and documented. Change management teams include appropriate applications development, systems administration and information security staff to address compatibility and security issues. 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. Documented processes must be reviewed annually or whenever significant process changes occur

12.11.2.2 Document the change management process as it passes through the system development life cycle (SDLC) with documentation securely stored for audit purposes. Documentation should address a review of the following:

12.11.2.2.1 Change summary, justification, and timeline

12.11.2.2.2 Test plans and results

12.11.2.2.3 Impact analysis to security and privacy

12.11.2.2.4 Documentation and baseline updates

12.11.2.2.5 Implementation timeline and recovery plans

12.11.2.2.6 End of life or decommissioning plans as required

12.11.2.3 Changes to software applications must be controlled. Only authorized personnel may perform production installations.

12.11.2.4 Changes to production libraries should not be the same individuals who made the application changes in test and development. If this is not possible, document procedures to reduce conflicts of interest; and separate privileged accounts with appropriate permission sets should be maintained to segregate test and production environment access.

12.12 Printers and Multifunction devices (MFDs)

Printers and multifunction devices (all-in-one printer/scanner/copier/fax machines) are designed to input information to, or generate information from computers. Such devices may be connected to the network or have internal memory or hard drives. These devices must be securely configured to reduce the risk of sensitive information disclosure.

12.12.1 Do not use MFDs to process sensitive data. Faxing of FTI is prohibited.

12.12.2 Remove or disable all unnecessary software, services, ports, protocols, and accounts that do not adversely affect device operation or business functions.

12.12.3 Enable full-disk encryption and the capability to purge scan/print job data from memory on all MFDs.

12.12.4 Printers and MFDs must have an assigned (static) IP address.

12.12.5 Change default passwords. Password strength shall be in accordance with DHHS-IT-001B, DHHS Access Control Standard.

12.12.6 Change user passwords in accordance with the DHHS IT Access Control Standard.

12.12.7 Devices with internal hard drives that are relocated to another business unit or removed from service must have the internal hard drive sanitized or replaced prior to being moved.

12.12.8 Use of MFDs for scanning to e-mail is restricted to internal DHHS recipients only. Delete manually entered e-mail addresses as personnel leave. Review and update the MFD address book at least annually.

THIS PAGE INTENTIONALLY LEFT BLANK

Section 3 - DHHS Information Technology (IT) Access Control

13.0 INTRODUCTION

Securing and protecting DHHS IT resources is a critical responsibility of every individual with access to those resources. DHHS policy is to provide the minimum access permissions necessary for Staff to perform their assigned duties.

13.1 Purpose and Objectives

This standard establishes guidelines for creating Unique User Identification (User ID, also referred to as UserID), strong passwords, minimum necessary access permissions based upon assigned job duties, protection of access controls, and requirements for remote access to the DHHS network environment.

14.0 ROLES AND RESPONSIBILITIES

The accounts management process is multi-faceted. All DHHS staff are responsible for ensuring accounts are authorized, properly requested, implemented, maintained and terminated timely and consistently.

14.1 The DHHS Supervisor is responsible for:

14.1.1 Identifying all appropriate resources required for their staff to perform assigned functions.

14.1.2 Coordinating with their designated DHHS IT Security Administrator to request access to DHHS IT resources on behalf of assigned staff based upon the minimum necessary criteria for the performance of assigned job activities. Each request must include system, applications, and level of access.

14.1.3 Ensuring Staff are sufficiently trained in appropriate use and management of assigned UserIDs, as well as security and privacy requirements of each application Staff will be using.

14.1.4 Annually reviewing access roles for assigned staff to determine if the assigned access permissions are reasonable and appropriate for currently assigned job duties.

14.1.5 Reporting all staff changes or terminations through their Security Administrator.

14.2 The DHHS Security Administrator is the designated point-of-contact (POC) for each DHHS Division, Service Area or local office location and is responsible for:

14.2.1 Coordinating with the Customer Service Help Desk to request staff IT access changes, including new access, transfers, name changes, permissions changes, and staff terminations.

14.2.2 Coordinating with any external entity for any external applications/systems the staff member may require access to for the performance of required tasks.

14.2.3 Coordinating with the Customer Service Help Desk and AISO for any policy exception requests, to include special UserIDs

14.3 The Customer Service Help Desk is responsible for:

14.3.1 Creation, modification, and deletion of accounts as requested by the DHHS Security Administrator.

14.3.2 Ensuring appropriate permissions are assigned to the Staff domain and application accounts.

14.3.3 Facilitating password changes as requested/required by staff.

14.3.4 Periodically auditing account activity for inactive (stale) accounts and taking appropriate actions to disable or delete inactive accounts.

14.4 DHHS business units are responsible for:

14.4.1 Providing an Agency sponsor to represent external entities requesting access to DHHS resources.

14.4.2 Coordinating and maintaining any business agreements with external entities.

14.4.3 Coordinate with Customer Services Help Desk and/or systems administrators to ensure appropriate permissions are established and provided to external user accounts.

14.4.4 Annually coordinating with external entities to ensure accounts are valid and necessary, and taking appropriate action for any necessary changes.

14.4.5 Reviewing audit reports for non-use of accounts and taking appropriate action to validate, disable or delete unused accounts.

14.5 All DHHS users are responsible for

14.5.1 Using and protecting their individually assigned credentials, to include UserIDs, passwords, challenge question responses, certificates, and PINs.

14.5.2 Reporting actual or suspected account compromise upon discovery

14.5.3 Changing their passwords on regular intervals.

14.6 The Agency Information Security Office (AISO) is responsible for:

14.6.1 Developing and disseminating information concerning recommended safeguards, and the potential security threats and concerns of remote access of DHHS automated information and systems;

14.6.2 Ensuring that all personnel are aware of this policy and incorporating it into access control briefings and training programs;

14.6.3 Promptly notifying the DHHS CIO and appropriate DHHS Management of computer security incidents (or suspected incidents) resulting from improper access.

14.6.4 Ensuring that information security notices and advisories are distributed to appropriate personnel and that vendor-issued security patches are installed on DHHS software.

14.6.5 Coordinating with DHHS Sponsors to perform a periodic review of the External Partners' account validations, security settings and protocols to ensure compliance with the contract arrangement or applicable federal, state, or agency policy and standards.

14.6.6 Requesting a risk assessment be performed for any vendors or contractors who require remote access to CONFIDENTIAL or RESTRICTED information. If a risk assessment is required, it must be completed before the vendor or contractor is allowed connectivity to DHHS systems.

15.0 UNIQUE USER IDENTIFICATION (USERID) STANDARD

Unique DHHS UserIDs and passwords are key to securely performing activity on the State network. The UserID owner is responsible for protecting the integrity of the logon credentials assigned to them.

Requests to the Customer Service Help Desk must be provided by the Security Administrator to ensure Staff are not independently requesting additional permissions or application access not required or authorized.

Only authorized DHHS Customer Service Help Desk Administrators may assign or make changes to UserIDs. If Staff suspects their logon credentials (UserID and/or password) have been compromised, report the incident to the DHHS Help Desk as soon as possible.

Security safeguards covered under this standard apply to Unique User Identification and Password Management and are designed to enhance the requirements of the DHHS IT Security Policy.

15.1 User IDs (UserIDs)

15.1.1 Every staff member accessing a DHHS IT Resource must have a unique User ID (UserID) assigned. Generic accounts or sharing of UserIDs are not allowed on any system capable of making changes or updates to DHHS information resources or applications capable of accessing CONFIDENTIAL or RESTRICTED information (e.g., any DHHS client data). Use of a UserID not specifically assigned to that individual is a violation of this standard unless additional levels of authentication or mechanisms to ensure individual accountability, such as increased logging, for information access are in place. Staff who improperly share UserID and passwords may have their account access suspended or removed, and/or other adverse actions based on the level of information accessed.

15.1.2 Shared login accounts are prohibited on multi-user systems where CONFIDENTIAL or RESTRICTED information is processed or stored.

15.1.3 Shared login accounts for any other system 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 (e.g., enhanced audit logging) or access layers exist to ensure the ability to individually identify personnel accessing non-public information.

15.1.4 Special UserIDs may be requested to meet unique requirements (e.g., mainframe batch job processing, system maintenance requirements, training IDs, etc.,) and must be approved through the AISO. Special UserIDs must be:

15.1.4.1 Assigned to a specific account owner who is directly accountable for activities performed using the Special UserID;

15.1.4.2 Terminated or reassigned when the responsible DHHS employee terminates or transfers;

15.1.4.3 Terminated immediately when no longer required;

15.1.4.4 Subject to the same password requirements as all other accounts; and,

15.1.4.5 Subject to increased audit and logging requirements.

15.1.5 All accounts (internal and external) must be reviewed annually to ensure the need for the accounts and their corresponding permissions are still valid.

16.0 INACTIVE ACCOUNTS

Inactive ("stale") accounts are those accounts that have not been accessed for a pre-determined period and pose a security risk to the network environment. Inactive accounts, if UserIDs and passwords are known or guessed, provide an avenue for unauthorized access to DHHS network resources, increasing the risk for unauthorized disclosure. The following shall apply for all accounts to reduce this risk:

16.1 Monitor agency accounts at least monthly for login activity. Accounts not accessed shall be disabled or deleted using the following standards.

16.1.1 Any account inactive for 60 consecutive days from the last logon date will be disabled. The account owner will be required to reset the password before accessing the account.

16.1.2 Any account inactive for 120 consecutive days from the last logon date will be disabled per paragraph 16.1.1 and requires the staff member to contact the Customer Service Help Desk to have the account reactivated.

16.1.3 Any account inactive for 13 consecutive months from the last logon date shall be automatically deleted. The Supervisor and Security Administrator must validate reinstatement of the account. Confidentiality agreements must be re-accomplished.

16.2 External accounts pose additional risk and undergo additional reviews.

16.2.1 Monthly reports shall be generated to search for accounts inactive for more than 30 consecutive days.

16.2.2 The DHHS Sponsor shall contact the External Entity regarding any account inactive for over 30 consecutive days to ensure the account is still required. If the entity does not respond, the Agency may take action to disable or delete the account.

16.2.3 External users whose accounts are deleted for inactivity shall require approval from the Agency sponsor and complete all required confidentiality agreements before a new account will be created.

16.2.4 External users found to be sharing accounts shall have access suspended. Repeated violations of account sharing shall result in account revocation. Re-establishing accounts require approval from the agency sponsor and completion of required confidentiality agreements.

16.2.5 External Entity shall notify DHHS Sponsor of account termination(s) within 15 calendar days of the termination.

16.2.6 All other actions as defined for internal accounts shall apply to external user accounts.

16.3 Exception:

16.3.1 Staff on extended (more than 30 days) absence for a documented reason (e.g., extended medical leave or administrative furlough) may have their accounts suspended (i.e., disabled, but not deleted) for the duration of the absence period. Route requests for account suspension through Human Resources, the staff member's supervisor, the appropriate Security Administrator and the Customer Service Help Desk. Help Desk should annotate the account to reflect an extended absence.

16.3.1.1 Notifications for suspending the account should be made BEFORE the extended absence begins.

16.3.1.2 The designated Security Administrator will contact the Customer Service Help Desk to restore access upon the Staff member's return.

17.0 PASSWORDS

Passwords are an important aspect of computer security and a front line of protection for individual user accounts. Passwords are used for various purposes at DHHS (e.g., LAN access, web accounts, email accounts, and user-level application access). Poorly created passwords that are easily guessable increase the risk of network compromise. All staff with access to DHHS systems are responsible for taking the appropriate steps, as outlined in this standard, to create secure passwords and keep them protected.

Account owners are responsible for any activity performed using their UserID and password. This standard establishes guidelines for creation of strong passwords, the protection of those passwords, and the frequency for changing passwords.

17.1 Password creation standards

Due to the diversity of DHHS applications, the password standard is divided into two sets of guidelines. The first set applies to all DHHS applications housed on the state mainframe computer utilizing mainframe security safeguards. The state mainframe safeguards are defined and managed by the State of Nebraska Office of the Chief Information Officer (OCIO) and employ the password standards listed in this document. All other DHHS IT resources and applications must meet the Network/Application password guidelines as defined in their respective user guides and this document. The following table is an illustration of best practices for password generation and applies to every system.

DO	DON'T
Use a pass phrase or multiple random words instead of a single word. For example: "The quick brown fox jumped over the lazy dog" can become T!6fj071d!	Use standard dictionary words
Use a mix of UPPERCASE or lowercase letters, numbers (1,2,3…) and special characters (!,@,#...) if the system allows it	Use family member, pet, car, sports team or other common name or item that can be directly associated to the user
Replace letters in the password with numbers or special characters. For example: - O can become 0 (numeric 'zero') Lower case 'L' can become 1, !, capital 'i' (I), /, \, or | ("pipe" symbol)	Use birthdays, anniversary or other significant dates that can be directly associated to the user
Select password characters from both ends of the keyboard (If a user is left-handed, the tendency may be to use the dominant hand (left) side of the keyboard)	Use Repeating characters. Examples include: - AAaa@@@@ - AAbb11!!
Change passwords as required by policies programmed into the network enterprise group policy or individual applications password policy	Keyboard "walk" (selecting character keys that are immediately adjacent to each other on the keyboard). Even though these passwords may meet the characteristic requirements, they can be easily compromised. Examples include: - Q2w3e4r% - QWERty7* - ZAQ!2wsx

17.1.1 Mainframe Password Guidelines.

17.1.1.1 Mainframe strong passwords consist of a minimum of six (6) and maximum of eight (8) characters in a combination of alpha (letters), numeric (numbers), and special characters. The combination must consist of:

- At least one alpha character (A-Z or a-z)
- At least one numeric value (0-9)
- May include special characters (#$@)

17.1.1.2 Resource Access Control Facility (RACF) account passwords follow the below guidance.

17.1.1.2.1 Standard user passwords must be changed at least every 90 days.

17.1.1.2.2 Accounts with elevated permissions must change passwords at least every 60 days.

17.1.1.2.3 RACF administrators shall change passwords monthly (mainframe setting is 31 days).

17.1.1.3 Passwords cannot be reused for 24 password generations. (i.e., 24 password change cycles must occur before the first password may be reused

17.1.1.4 Accounts are disabled after three (3) consecutive unsuccessful logon attempts.

17.1.1.5 Refer to system requirements for additional guidance.

17.1.2 Network/Application Password Standards:

17.1.2.1 Strong passwords consist of at least eight (16) characters in a combination containing three (3) of the following four (4) characteristics.

- At least one UPPER CASE alpha character (A-Z)
- At least one lower case alpha character (a-z)
- At least one Numeric value (0-9)
- At least one special character (~!@#$%^&*()_+-=<>?;':\)

17.1.2.2 Passwords must be must be changed at least every 60 days. Once a password has been changed, staff must wait at least one day before changing the password again.

17.1.2.3 Passwords cannot be reused for 24 password generations.

17.1.2.4 Accounts are disabled after three (3) consecutive unsuccessful logon attempts.

17.1.2.5 Refer to system requirements for additional guidance.

17.2 Password Protection Standards

Account owners are responsible for protecting the logon credentials (UserID and Password) assigned to them. Account owners must comply with the following protection standards:

17.2.1 Do not use the same password for DHHS accounts used for other non-DHHS accounts (e.g., personal ISP account, email, and benefits).

17.2.2 Where possible, do not use the same password for various DHHS access needs. For example, best business practice is to select one password for the LAN Access and a separate password for application access.

17.2.3 All passwords should be treated as CONFIDENTIAL DHHS information. Do not share passwords with anyone. Supervisors or managers requiring access to staff's accounts must contact the DHHS Help Desk for assistance.

17.2.4 Do not reveal a password over the phone. Exception: Password may be shared by an account owner WHO INITIATES THE CONTACT with the Customer Services Help Desk staff or DHHS Support staff to resolve an issue. Immediately after resolution of the incident, the password shared with support staff must be changed.

17.2.5 If anyone demands a password or an account reset for an account that is not theirs, refer him or her to this document or have them call the DHHS Help Desk.

17.2.6 Do not use the "Remember Password" feature on applications, to include any web-based application.

17.2.7 Do not write passwords down or store them where they may be lost, stolen, or otherwise compromised. Do not store passwords in a file on ANY computer system (including a PDA or similar devices) without encryption (see section 12.4 regarding “KeePass”).

17.2.8 If an account or password compromise is suspected, immediately change the password and report the incident to the DHHS Help Desk as soon as possible.

17.3 Application Development Standards

Application developers must ensure either their programs contain the following security precautions, through the application code itself or through boundary protections that require authentication that meets these standards prior to accessing the application:

17.3.1 Aligns with all DHHS standards and procedures; and does not degrade the security posture of the underlying infrastructure on which the application runs.

17.3.2 Aligns with the minimum password guidelines detailed in this document.

17.3.3 Supports authentication of individual users, not groups.

17.3.4 Does not store passwords in clear text or in any easily reversible form.

17.3.5 RACF passwords – Applications using RACF must meet the strongest password guidelines in force and supported by the OCIO.

17.4 KeePass

17.4.1 KeePass is an application tested and used by DHHS for encrypted storage of a Staff member’s UserIDs and passwords. Staff may use the application to create a password-protected file for storing their login credentials (UserID and Password).

17.4.2 Use of KeePass is optional, but recommended if the Staff member maintains multiple passwords. Staff members using this application should update entries as their passwords change. WARNING: if the Staff member forgets the password set for their encrypted KeePass file, the contents cannot be recovered.

17.5 Password Station

Avatier Password Station ("PassMan") is an application tested and used by DHHS as a self-service tool to unlock accounts or reset Staff Members' password for domain-level applications (Network logon and e-mail). Initial access to the Password Station requires staff to create and answer at least three challenge questions. The challenge question answers are necessary for subsequent access to the application.

18.0 PRIVILEGED ACCOUNT MANAGEMENT STANDARDS

Privileged accounts have elevated permissions and include administrator accounts, embedded system accounts to interconnect systems, and accounts used to run service programs. These accounts are used by systems and personnel to access sensitive files, execute software, load and configure policies and configuration settings, and set up or maintain accounts.

Disclosure of privileged accounts passwords could be catastrophic, as it would enable an intruder to impersonate any privileged user. Damage to the credential vault or loss of access to this database would create an operational disaster across the entire organization, since administrators could potentially be locked out of every system. As such, privileged account owners should exercise extra diligence in securing these credentials.

18.1 Due to the elevated access levels, DHHS requires the following standards and procedures to minimize the risk of incidents caused by these accounts:

18.1.1 Privileged access requests follow the normal access request process but shall have an additional approval authority level from either the DHHS CIO, IS&T Management, or the AISO.

18.1.2 Anonymous activity by privileged accounts is prohibited. All activity performed by privileged accounts must be performed using a named UserID and password.

18.1.3 Privileged access accounts shall be assigned to an individual or system in a manner that maintains a separation of duty from audit and compliance functions (e.g., audit reviews cannot be performed by the same person who administers access credentials).

18.1.4 Privileged accounts may not be shared; the assigned individual or system owner shall be held accountable for the actions conducted through the use of the privileged account.

18.1.5 Privileged accounts shall comply with all standards for password strength and expiration. ANY exceptions must be explicitly approved and documented through the AISO

18.1.6 Logging of privileged access activity is required and takes priority over other auditable events. IS&T shall ensure that appropriate storage is available to meet capacity requirements. Logs shall be retained as defined in the DHHS IT Audit Standard

18.1.7 Staff should authenticate to the network or system through their standard user logon prior to requesting, approving or gaining access to a privileged account. This ensures additional accountability for changes made using that account. Privileged accounts may not be used for day-to-day activities not requiring elevated privileges.

18.1.8 Remote access for privileged functions shall be permitted only for compelling operational needs, strictly controlled, and explicitly authorized in writing by the DHHS CIO or his/her designated representative.

18.1.9 The DHHS CIO is required to approve any changes or exceptions to the privileged account management infrastructure, operations, or procedures.

19.0 EXTERNAL USERS

External partners are entities with a current contract and/or business associate agreement with DHHS. Examples of these partners include but are not limited to: Medicaid and Long Term Care (MLTC) waiver contractors, Employment First contractors, Child Support Enforcement contractors, Public Health contractors, CFS Out of Home Care contractors, and Tribal Nations. The following standards apply to DHHS External Partners:

19.1 The agency must provide a business unit liaison (sponsor) who will be the primary points of contact (POCs) for the external entities. In turn, the external entities must provide POCs authorized to request accounts for their respective organization (i.e., security administrator). Requests for access must be routed and documented through the Agency sponsor.

19.2 Include contract language that provides for the appropriate protection of DHHS information commensurate with DHHS policies and standards.

19.3 Connect through a DHHS approved configuration. If connecting through a non-approved configuration, then the external partner must submit a detailed description of the remote connectivity mechanisms and security protocols employed to maintain the security of the DHHS information system and receive approval before the connection will be allowed.

19.3.1 Ensure the external partners' remote access connection complies with DHHS Security Policy, paying particular attention to the protection of FTI, PHI and PII.

19.3.2 Split-tunneling is not permitted at any time while remotely connected to the DHHS network.

19.4 External Partners must use their organization's authorized email system or State of Nebraska assigned e-mail account (as applicable) when conducting business on behalf of DHHS. Use of personal email accounts (e.g., Hotmail, Yahoo, Gmail, etc.) or other external resources to conduct Nebraska DHHS business is prohibited. This ensures that: 1) official business is never confused with personal business; and 2) any confidential information transmitted is not stored on a non-secure, cloud-based e-mail system.

19.4.1 The external partners' e-mail system must be able to send or receive protected information through encrypted email

19.5 External User accounts

19.5.1 Access profiles must be pre-determined and coordinated with systems administrators based on minimum necessary requirements for the business activities performed by the external entity on behalf of DHHS.

19.5.2 External account users are subject to federal, state, and agency policies, procedures and standards for appropriate use, and security and privacy requirements.

19.5.3 External user accounts are subject to periodic audits by the Agency.

19.5.4 The agency sponsor shall annually coordinate and validate user accounts with the external entity. This requirement does not release the external entity of compliance with existing agreements, to include timely notification of account access terminations.

19.5.5 The Agency may disable or terminate external user account access for any reported or identified misuse of DHHS resources (e.g., sharing of logon credentials, improper access, unauthorized disclosure, etc.). In accordance with signed agreements, the external organization will be requested to investigate the incident and report findings and remediation or mitigation strategy before the account will be reinstated.

19.6 Any information created, processed, stored or transmitted by the external entity on behalf of the DHHS is the property of the Agency. The external users shall not access, modify, process, download, store, or otherwise use DHHS data in a manner inconsistent with established Agency policies, standards, procedures or agreements.

20.0 REMOTE ACCESS STANDARDS

Remote Access is defined as access to any DHHS information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet). This Standard defines requirements and procedures for connecting to the DHHS network from any host connected using the Internet. These standards do not apply to DHHS web applications or systems designed for public access.

Remote access to the DHHS network containing CONFIDENTIAL or RESTRICTED information will only be permitted from DHHS-controlled, managed, or approved methods or if arrangements have been approved through the policy exception process. Remote access to FTI is only available through VDI. Remote users and administrators are prohibited from accessing FTI from non-agency owned information systems or devices.

Mobile devices such as PDA’s, smartphones, tablets and other consumer devices must use IS&T managed connection and configuration to access anything other than web-based applications. Personal devices that meet NITC Access standards and specifically approved by the OCIO may connect and synchronize to the state email system.

All remote access servers shall be kept fully patched and managed by authorized systems administrators. Remote access servers shall be placed at the network perimeter (such as a DMZ environment) and must be isolated from servers with DHHS network access, separated by boundary protection (such as firewalls) and intrusion detection monitoring.

This Standard does not apply to remote work (telework) arrangements when telework does not involve access to the DHHS network.

20.1 Roles and Responsibilities.

20.1.1 Supervisors and managers must ensure that:

20.1.1.1 An appropriate Management/Employee Agreement is signed by all staff approved for remote access.

20.1.1.2 Their teams have been trained concerning their security responsibilities, including the need to report any computer security incidents (or suspected incidents), when remotely accessing DHHS information and systems.

20.2 Remote Access Standards and Requirements

The following standards apply to all DHHS Staff approved to connect to DHHS IT resources through the Internet. This includes all approved work-from-home arrangements requiring access to DHHS systems and DHHS office locations that use the Internet to access the DHHS network.

Remote access for DHHS Staff must be requested and have prior authorization by their Supervisor or Division Management.

20.2.1 Nebraska DHHS Staff with remote access privileges must ensure that their DHHS-owned or personal computer or workstation, when remotely connected to the DHHS network, is not connected to any other network at the same time - with the exception of personal networks that are under the complete control of the user.

20.2.2 DHHS Staff with remote access privileges to the DHHS network must only use assigned State of Nebraska accounts to conduct DHHS business.

20.2.3 External access from a computer not owned or supported by DHHS may only access DHHS network resources via an authorized and appropriately configured connection

20.2.4 DHHS IS&T will authorize, document, and monitor all remote access capabilities used on the system

20.2.5 Multi-factor authentication (unique UserID and an appropriate hardware or software token) is required for remote access to CONFIDENTIAL or RESTRICTED data. Authentication will be controlled by centralized Key Management Centers/Security Management Centers with a backup at a separate location and shall employ IS&T approved cryptography during the entire session when connected to the DHHS network.

20.2.6 Remote sessions shall be locked or terminated after 15 minutes of inactivity. The user must re-establish access with the appropriate credentials and authentication procedures.

20.2.7 Staff approved for remote connectivity using non-DHHS equipment must have up to date anti-virus protection, active firewalls, and appropriate security patch levels equivalent to those provided for DHHS equipment. All users may be subject to random inspection by IS&T or the AISO and are required to sign an annual acknowledgement of understanding of responsibilities to protect information when connected to the DHHS network through a remote session.

20.2.8 Remote access sessions shall be logged. IS&T shall perform periodic monitoring of remote access sessions and random inspection of the user security settings and protocols to ensure compliance with policies and standards.

20.2.9 All remotely accessible information systems containing CONFIDENTIAL or RESTRICTED data must employ mechanisms to ensure sensitive information cannot be downloaded or stored to non-agency devices.

20.2.10 Remote access logon failures shall be logged. Credentials shall be disabled after three (3) consecutive failed logon attempts.

20.2.11 No DHHS information other than PUBLIC information may be stored on a personal device.

20.3 Account Termination and access changes

Remove all agency network and application accounts or access permissions no longer required by an individual user.

20.4 Notification

Supervisors and Security Administrators are in the best position to know when an individual is leaving the agency (either termination or transfer), transferring to another position within the Agency, or changing job requirements. As such, Supervisors and Security Administrators are responsible for making timely notifications to Human Resources AND the Customer Service Help Desk.

20.4.1 Make notifications of account termination or access change requirements as soon as practical, but no later than one (1) business day of a staff member's departure or change in responsibilities.

20.4.2 If a staff member provides advance notice, the Security Administrator may create a Request for Personnel Action (RPA) into the appropriate system (e.g., OnBase, Workday, etc.,) prior to the staff member's last business day of work. The Security Administrator should identify all Agency applications to which the departing member has access. The RPA will allow a ticket to be created in advance, allowing the Customer Service Help Desk to perform the account action at the appropriate time.

20.5 Processing of terminations

20.5.1 Customer service shall maintain procedures for the processing of accounts. NOTE: Best business practice for processing the RPA is within three (3) business days of staff departure.

20.5.2 Customer Service Help Desk must make a reasonable effort to ensure all accounts associated with a staff member are deleted from the systems. This includes all DHHS-specific applications (e.g., CHARTS, N-FOCUS, MMIS, NTRAC, etc.,) and e-mail to ensure no residual information relating to the individual remains on the system.

20.6 State Agency Transfers

20.6.1 Notification requirements of section 20.4 shall be met.

20.6.2 To reduce the risk of unauthorized access to or disclosure of DHHS client information, all accounts, including agency-specific application access, home directories and e-mail of the transferring staff members should be deleted.

20.7 Reusing UserIDs

Reusing a UserID is not good business practice and is strongly discouraged. Reuse may result in inadvertent assignment of incorrect permissions and reestablishment of e-mail accounts or file structures for the new user, resulting in improper access and inadvertent disclosure.

20.7.1 A deleted UserID may not be reused for 12 months.

20.7.1.1 Create a new account and provide a qualifier such as a number or middle initial (e.g., John.Public, John.Q.Public, jpublic, jqpubli, jpubli1, etc.) for subsequent accounts.

THIS PAGE INTENTIONALLY LEFT BLANK

Section 4 - DHHS Information Technology (IT) Risk Management

21.0 INTRODUCTION

Risk management is an essential function that is a perpetual focus within the DHHS systems development and maintenance practices. In order to have effective risk management, IS&T and the DHHS ISO are required to plan for the use of technology, assess the risks associated with technology, decide how to securely implement the technology and establish processes to measure and monitor risk.

Protecting and ensuring the Confidentiality, Integrity, and Availability for all DHHS information and information systems is a fundamental objective of DHHS Information Security. This Standard is a critical component of ensuring that all DHHS information is protected appropriately.

21.1 Purpose and Objectives

This standard describes requirements and procedures to be followed throughout the DHHS infrastructure to ensure information owned, controlled, or managed by DHHS is protected commensurate with its information classification, and that business areas are in compliance with Federal, State and DHHS policies and standards. The ISO is required to perform periodic reviews, inspections, and assessments of the security posture in place throughout DHHS. This standard describes the reviews conducted, and the format in which these reviews will take place.

21.2 Reference documents

Use the following reference documents as guidance for completing risk assessments:

- NIST SP 800-30 Standards for Risk Analysis
- NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.
- 45 CFR Part 164, Subpart C, “Security Standards for the Protection of Electronic Protected Health Information (ePHI),” (Heath Insurance Portability and Availability Act (HIPAA) Security Rule)

22.0 SCOPE AND APPLICABILITY

This standard applies to all DHHS Staff, DHHS business areas, physical locations and IT resources that process or handle non-public information subject to review and inspection. Business unit and IS&T Management shall work with the AISO to establish review schedules as requested, accommodate business schedules within reason, and make all personnel, information, physical areas, records, and historical documentation available to facilitate these reviews. The ISO is required to establish schedules and priorities based upon known or likely levels of security risks to DHHS information or services.

22.1 Enforcement

This standard includes compliance with federal and state regulations. Violations may result in criminal and monetary penalties for individuals found violating these standards. Any staff member found to have violated this policy may be subject to disciplinary action, as defined in DHHS-IT-001 DHHS IT Security Policy.

23.0 STANDARDS

DHHS is required to implement policies, standards, and procedures to prevent, detect, contain, and correct security deficiencies. DHHS is also required to implement risk analysis and risk management to ensure adequate resources, policies, and procedures are in place and compliant with Federal, State, and DHHS standards and procedures.

23.1 Key elements of the DHHS Risk Management Program

23.1.1 Operational Planning identifies and assesses risk exposure to ensure policies, procedures and controls remain effective. Risk reviews and assessments should address Confidentiality, Integrity, and Availability of systems, controls, and foreseeable internal and external threats. DHHS business owners need to consider the results of risk assessments when overseeing operations.

23.1.2 Ongoing Data Collection: Understanding the systems environment is critical to an effective risk management program. Several sources of information provide valuable input into the DHHS Risk Management Program. The ISO shall validate and review:

23.1.2.1 IS&T Strategic and Tactical Plans

23.1.2.2 Disaster Recovery

23.1.2.3 IS&T Help Desk tickets and tracking reports

23.1.2.4 Self-assessments on security controls

23.1.2.5 Reported security incidents

23.1.3 Risk Analysis: DHHS business owners and the ISO shall use information collected on IT assets to analyze the potential impact of risks on system and business functions. The analysis should identify vulnerabilities, events or threats that could negatively affect the system strategically or operationally. The ISO shall evaluate the likelihood of various events and rank the possible impact.

23.1.4 Inspection and Monitoring: The ISO shall perform reviews and inspections of DHHS systems and business processes. The ISO and business owners shall monitor risk mitigation and remediation activities to ensure appropriate progress is being made. Record any mitigation and remediation action findings in the DHHS Plan of Action and Milestones (POA&M) process.

23.2 Risk assessments and reviews evaluate potential security risks because of an IT resource's vulnerabilities and the potential impact on other DHHS IT resources. 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. DHHS has established three levels of scheduled reviews with an intention of addressing risk from three perspectives:

23.2.1 Business Process Review - reviewing risk from the individual business perspective

23.2.1.1 The intent of the Business Process Risk Assessment is to validate that DHHS departments are compliant with DHHS-001 DHHS IT Security Policy, particularly where the highest level of risks exist to DHHS information. This review focuses specifically on the individual business process, and includes a review of all information input, processing, and output. It will review all touch points, exposure points, and information flow to ensure information is protected commensurate with its classification.

23.2.1.2 Because of the large volume of business processes throughout DHHS and the various levels of information handled by these departments, it is not practical to review all business areas on a regular basis. In fact, it is more likely that higher-risk business processes may be reviewed multiple times before lower-risk processes are reviewed. The AISO shall prepare an annual schedule of Business Process reviews, with input from the DHHS Privacy Officer and other DHHS and IS&T management. These reviews shall occur at least four (4) times per year (quarterly), and all findings shall be recorded and tracked in the POA&M process. The schedule of reviews shall be based on priorities that are determined using the following considerations:

23.2.1.2.1 Classification level of the information used within the business process

23.2.1.2.2 Evaluation of key risk indicators and their related factors

23.2.1.2.3 Evaluation of threats that are imminent or unique to the business process

23.2.1.2.4 Past performance, previous incidents or exposures, past audit or review findings

23.2.1.2.5 Impact analysis to DHHS of a security breach within the business process

23.2.1.2.6 Management discretion, concerns, or advice

23.2.2 HIPAA Focus reviews risks associated with the security of Protected Health Information.

23.2.2.1 All DHHS divisions, departments, and program areas (hereinafter referred to as “PHI Owner”) who use, create, process, receive, transmit, or store electronic Protected Health Information (ePHI) will maintain a current HIPAA Risk Assessment for the handling and protection of PHI. The intent of this review is to focus primarily on the areas of DHHS who handle PHI. These program areas must ensure all PHI is secured with an appropriate level of administrative, physical, and technical safeguards per the HIPAA Security Rule.

23.2.2.2 The AISO, in coordination with the DHHS HIPAA Privacy Officer will be responsible for scheduling and managing HIPAA Risk Assessments. HIPAA Risk Assessments will be a joint venture between the HIPAA Security Officer and the PHI Owner. Conduct HIPAA Risk Assessments:

23.2.2.2.1 at least once every five (5) years;

23.2.2.2.2 when significant changes to the protection of electronic PHI occur; or,

23.2.2.2.3 before implementing any new IT resource or data system that may affect the handling or protection of PHI.

23.2.2.3 The AISO shall perform this review using the steps below, as adapted from the approach outlined in NIST SP 800-30 Standards for Risk Analysis:

23.2.2.3.1 Identify Scope and Boundaries of the analysis

23.2.2.3.2 Gather data through interview, testing, observation, and review

23.2.2.3.3 Identify and document potential threats and vulnerabilities

23.2.2.3.4 Assess the current security posture, measures, and mitigations

23.2.2.3.5 Determine the likelihood of a threat occurrence

23.2.2.3.6 Determine the potential impact of a threat occurrence

23.2.2.3.7 Determine the level of risk

23.2.2.3.8 Identify security measures, recommendations, or mandates, and finalize documentation in the POA&M

23.2.3 Federal Information Security Management Act (FISMA) Review assesses risk from infrastructure and organizational perspectives

23.2.3.1 The NIST 800-53 framework makes up the fundamental security and privacy requirements. As such, DHHS is required to conduct an annual review of the DHHS infrastructure to ensure compliance with these standards. The format and approach for this review is based on FISMA requirements. The security controls inspected are organized into 17 control families within three classes (management, operational, and technical), and aligned with the security control areas specified in FIPS 200, Minimum Security Requirements for Federal Information and Information Systems.

23.2.3.2 The AISO shall perform an annual FISMA assessment. Each assessment should cover at least 1/3 of the control areas, and all controls should be assessed over a three-year period.

23.2.3.3 To meet federal agency requirements, an independent and certified third party must perform a full FISMA assessment at least once every three years.

23.2.3.4 This review shall be conducted for each major system used within DHHS, and shall include all infrastructure and peripheral processes that are used by DHHS. Guidebooks and review templates can be found at: http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html

23.2.3.5 Some Controls, Enhancements, Implementation Standards and Guidance, or portions thereof, only pertain to narrowly-defined types of data, such as PHI, Personally Identifiable Information (PII) or Federal Tax Information (FTI). Additionally, some requirements may only apply within specific implementation scenarios. The approved migration of data into a FedRAMP-approved Cloud Service Provider (CSP) for instance, may require the unique application of specific Controls, Enhancements, Implementation Standards or Guidance that are only applicable in this specific scenario. These specialized requirements are referenced and clearly documented in guidance material.

23.3 Random Risk Assessments

23.3.1 Random risk assessments will be performed at the discretion of the AISO, typically when circumstances require additional oversight, such as after a security incident, increased security threat, or significant changes to the IT infrastructure. These assessments are flexible and intended to review specific elements identified as exception-based or high priority. These reviews can also be performed to validate the appropriate remediation or mitigation of a previous finding.

23.3.2 The AISO shall document the business area, reason for the random review, scope of inspection, dates of the review and all findings and results will be documented in the POA&M.

THIS PAGE INTENTIONALLY LEFT BLANK

Section 5 - DHHS Information Technology (IT) Security Reporting

24.0 INTRODUCTION

Consistent reporting standards will help ensure DHHS information security controls are uniformly implemented across the enterprise, meet all necessary regulations and requirements, and are appropriate for the level of risks facing DHHS and its information assets. Formal reporting helps keep the information security mission consistent, well understood and continually progressing as planned.

24.1 Purpose and objectives

This standard provides guidance ensure DHHS leadership is given current and appropriate information in a consistent format to support fact-based decision-making and allocation of future funding.

25.0 SCOPE

DHHS is required to produce the following standards and reports to reflect the current and planned state of information security at DHHS:

25.1 Agency

25.1.1 Information Security Strategic Plan for DHHS

25.1.2 Information Security Annual Report

25.2 Federal reporting requirements are defined in section 26.2.

26.0 REPORTS AND STANDARDS

26.1 Agency requirements

26.1.1 DHHS must properly plan to ensure the most appropriate projects are funded and supported. Planning for information protection will be given the same level of executive scrutiny at DHHS as planning for information technology changes. This plan shall be updated and published on an annual basis, and should include a 5-year projection of planned technology implementation and forecasted costs. It should include an educated view of emerging threats and protections, and an analysis of the potential impacts to DHHS information resources. This plan is necessary to ensure that information security is viewed as a strategic priority, and is included as part of the overall DHHS and Information Systems and Technology (IS&T) Strategic planning process.

26.1.2 Contents of the Strategic Plan:

26.1.2.1 Summary of the state of information security, mission, scope, and guiding principles

26.1.2.2 Analysis of the current and planned technology and infrastructure design for DHHS, and the corresponding changes required for Information Security to stay aligned with these plans.

26.1.2.3 Summary of the overall DHHS Information Risks Assessments and current risk levels. Detailed descriptions of significant security risks, and plans to mitigate or remediate those risks.

26.1.2.4 Assessment of the current information security posture related to the future targeted posture, identified gaps, and high-level timeline necessary to close or mitigate those gaps.

26.1.2.5 Summary of the Policies, Standards, and Procedures for DHHS Information Security, and projected changes necessary to stay current and relevant.

26.1.2.6 Summary of the Information Security Education and Awareness Program, progress, and timeline of events.

26.1.2.7 Summary of Disaster Recovery and Business Continuity activity and plans.

26.1.2.8 Analysis of the regulatory and contractual compliance environment, including potential new regulations or pending contractual requirements that will affect DHHS Information Security.

26.1.2.9 Proposed five year timeline of events

26.1.2.10 Line item cost projections for all information security activity is itemized by:

- Steady State Investments: The costs for current care and maintenance of the information security program.
- Risk Management and Mitigation: The line item expenses necessary to mitigate or resolve security risks for DHHS, in a prioritized order.
- Future Technology: The line item expenses and timelines necessary to support emerging or changing technology, and to be ready for new and emerging threats to DHHS information.
- Regulatory: The line item expense necessary to meet all regulatory and contractual compliance requirements.

26.2 Agency Plan of Action and Milestones Report (POA&M)

The POA&M report is a result from a quarterly management process that outlines weaknesses and delineates the tasks necessary to mitigate them. The DHHS Information Security POA&M process will be used to facilitate the remediation of DHHS Information Security and system-level weaknesses, and will provide a means for:

- Planning and monitoring corrective actions
- Defining roles, responsibilities, and accountabilities for weakness resolution
- Assisting in identifying the security funding requirements necessary to mitigate weaknesses
- Tracking and prioritizing resources
- Ensuring appropriate progress and priorities are continually addressed
- Informing decision makers

The POA&M process provides significant benefits to DHHS. It is a dynamic management tool useful for ongoing efforts to address programmatic and system-specific vulnerabilities. It assists in essential decision-making activities, facilitating and helping to ensure the oversight and mitigation of security weaknesses and the cost-effective use of mitigation resources. To function effectively, a POA&M must be continually monitored and diligently updated. The ISO is responsible for maintaining the POA&M and for providing quarterly updates to the IS&T Management team.

26.3 Federal Reporting Requirements

26.3.1 Center for Medicaid Services Requirements Safeguard Security Report (SSR) for FTI information

26.3.1.1 System Security Plan (SSP) is the overarching security plan that provides a system and boundary description, and addresses all applicable NIST control for that system. Required for the DHHS system connecting to and receiving Federal Data Services Hub information.

26.3.1.2 Security Control Assessment Attestation – annual requirement to validate the controls are applied as required. Independent review is required every three years.

26.3.1.3 Information System Risk Assessment (ISRA) – annual requirement to identify any potential risks that may exist within the system. Risks may or may not be correctable. Correctable risks are identified and tracked in the POA&M.

26.3.1.4 Privacy Impact Assessment (PIA) – annual requirement to identify how the agency accesses, processes, uses, or stores federal Hub data and any potential impacts to client privacy. Correctable impacts are identified and tracked in the POA&M.

26.3.1.5 Plan of Action and Milestones (POA&M) – tracking tool used to identify any significant correctable gaps in the security posture of a system. Submission to CMS is required quarterly.

26.3.2 Internal Revenue Service Requirements

26.3.2.1 Security Safeguard Review (SSR) - The SSR shall be prepared annually and is a collection of information required by the IRS for systems used in the handling of FTI. DHHS shall submit the SSR using the template provided by the IRS Office of Safeguards and meets all IRS requirements as defined in IRS Publication 1075. Much of the content is taken from other reports and formatted to meet IRS requirements.

26.3.2.2 Corrective Action Plan (CAP) is generated as a result of an IRS on-site visit which identifies deficiencies in the Agency's and its supporting entities' security postures. The on-site review is conducted every three years. The agency and supporting entities must review and attempt to take corrective action against open CAP items, document then return the CAP to the IRS for adjudication every six months.

26.3.2.3 Notifications of change is done as prescribed in the IRS Publication 1075 and is required for any changes to the network or application environment that affects how the agency manages FTI.

26.3.3 Social Security Administration

26.3.3.1 The Security Design Plan (SDP) is created as significant changes to the network or system of record occur that may affect how the agency manages SSA information. The SDP may be accompanied by a site visit from SSA to validate responses, and review physical controls.

26.3.3.2 The Security Evaluation Questionnaire (SEQ) is a less intensive version of the SDP and is required every three years. It is accompanied by a site visit from SSA to validate responses.

THIS PAGE INTENTIONALLY LEFT BLANK

Section 6 - DHHS Information Technology (IT) Incident Management Standard

27.0 INTRODUCTION

Computer systems are subject to a wide range of mishaps: corrupted data files, viruses or other malware, insider threats, or natural disasters. Mishaps can occur at any time and without warning. Many mishaps are remediated through day-to-day operating procedures; while more severe mishaps are addressed in other ways (e.g., Continuity of Operations (COOP) plans). In some cases, incident-handling actions cannot be performed by a single person or on a single system. Incident responses can range from re-education to recovering compromised systems to the collection of evidence for the purpose of criminal prosecution.

A formally documented and coordinated incident response capability is necessary in order to rapidly respond to detected incidents, minimize loss and destruction, remediate and mitigate exploited weaknesses and restore computing services. It prepares DHHS to efficiently and effectively respond, protect systems and data, and prevent disruption of services across multiple platforms and between all agencies across the State and DHHS network.

27.1 Purpose and Objectives

27.1.1 The DHHS IT Incident Management Standard and Procedures includes multiple processes throughout DHHS and Information Systems and Technology (IS&T). It includes a number of operational and technical components necessary to support all the fundamental steps within the Incident Management Life Cycle - including Preparation, Identification, Containment, Communication, Eradication, Recovery, and Root Cause/Remediation.

27.1.2 This standard is also a necessary component to Information Technology strategy and long term planning. DHHS policy, as well as Federal Information Security Management Act (FISMA), Health Insurance Portability and Accountability Act (HIPAA), and Internal Revenue Service (IRS) regulations require the establishment and maintenance of a computer security incident response capability that is in effect 24x7.

27.2 This document identifies key steps for promptly reporting security incidents and establishes formal reporting requirements for all such instances to the DHHS Information Security Officer (AISO), DHHS Privacy Officer, State officials, and DHHS customers. All security incident reports shall contain the facts and information needed to make informed management decisions and assist in coordinating and managing resolution(s).

28.0 SCOPE AND APPLICABILITY

This standard applies to all DHHS personnel, contractors, temporary employees, volunteers, vendors and business partners (hereinafter “Staff”) with access to DHHS IT resources; and to all access into the DHHS network or any system owned, leased, or supported by DHHS that stores protected DHHS information.

DHHS acknowledges and will comply with NITC 8-401, Incident Response and Reporting Procedure for State Government Standard.

28.1 Roles and Responsibilities

28.1.1 All DHHS Personnel

28.1.1.1 If the security incident involves Federal Agency (e.g., IRS, CMS, SSA, etc.), follow that Agency's reporting standards (i.e., within 24 hours of discovery). For FTI, this would include reporting findings to the appropriate Special Agent-in-Charge, TIGTA, and the IRS Office of Safeguards.

28.1.1.2 Report security incidents to the immediate supervisor, ISO or the DHHS Help Desk immediately, but not later than one hour of any suspected security incident.

28.1.1.3 Assist ISO and IT Team with remediation and reporting.

28.1.1.4 Follow instructions from ISO or IS&T before taking action.

28.1.1.5 Do NOT communicate information regarding the incident unless authorized.

28.1.2 Senior DHHS Management

28.1.2.1 Coordinate with ISO, Legal (HIPPA Office), and DHHS Privacy Office and communicate reportable breaches of PHI, PII, and FTI as required by regulation within one (1) hour of awareness.

28.1.2.2 Provide support and resources necessary to contain and remediate incidents.

28.1.2.3 As required, provide command and control of the event.

28.1.3 DHHS Legal

28.1.3.1 Work with ISO to triage and assess reportable conditions.

28.1.3.2 Draft communications for customers, government officials and the public in the event of a reportable breach.

28.1.3.3 Report Breaches of PHI and PII within required periods.

28.1.3.4 Ensure all third party agreements contain requirements to comply with DHHS Incident Management requirements.

28.1.4 DHHS Privacy Office

28.1.4.1 Work with ISO to triage and assess reportable conditions.

28.1.4.2 Draft communications for customers, government officials and the public in the event of a reportable breach.

28.1.4.3 Report privacy Breaches of PHI and PII to appropriate agencies within required periods.

28.1.4.4 Ensure all third party agreements contain requirements to comply with DHHS Incident Management requirements.

28.1.5 DHHS (Agency) Information Security Officer (AISO)

28.1.5.1 Facilitates liaison with the incident response team assembled by the agency CIO.

28.1.5.2 Ensures senior leadership is apprised of the current status of security incidents and follow-up activity.

28.1.5.3 Supports IS&T Management and technical staff to perform analysis and triage of incident impact and reportable conditions.

28.1.5.4 Communicates IS&T Incident Response Plan content and activities with DHHS Management.

28.1.5.5 Work with IS&T teams to prepare remediation and countermeasures.

28.1.5.6 Finalize Security Incident Reports.

28.1.5.7 Reviews requests for release of security incident information.

28.1.5.8 Determines follow-up activity and conducts root cause analysis, long- term mitigation, and awareness.

28.1.5.9 Perform review and inspection of business partners and their ability to meet requirements with this standard.

28.1.5.10 Perform education and training of this standard to all applicable DHHS personnel

28.1.5.11 Test the Incident Management Process annually.

28.1.6 DHHS CIO

28.1.6.1 Contact all appropriate individuals who will comprise the incident response team

28.1.6.2 Provide command, control, and oversight of information security incident triage, containment, remediation, and communication activity

28.1.6.3 Determine impact and priority of security incidents.

28.1.6.4 Issue an order of action if security incident is not controlled in a timely manner.

28.1.6.5 Review all requests for the release of security incident information and make determinations with regard to its release.

28.1.7 DHHS Incident Response Team

28.1.7.1 Composition of the Incident Response Team will be dependent on the nature and location of the event.

28.1.7.2 Agency divisions shall identify key personnel in their incident response plans who may be tasked to serve as members of the DHHS Incident Response Team. These personnel should be knowledgeable of agency operations and able to rapidly respond to, manage, and support any suspected incident to minimize damage to DHHS information system(s), network(s) and data by identifying and controlling the incident, properly preserving evidence, and reporting to appropriate State and Federal entities.

29.0 STANDARDS

A completed Security Incident Report is classified as RESTRICTED Information. Limit sharing or distribution of the information to only those individuals with a valid need-to-know. The Agency Chief Information Officer (CIO), with consultation from the AISO and IS&T management, will review all requests for the release of security incident information and make determinations with regard to its release, ensuring that it is consistent with applicable policies, regulations, and external customer requirements. Overall questions regarding this procedure should be directed to the AISO.

29.1 Incident Components

Incident handling procedures consist of four major components: Identification, procedure, analysis, and recovery. The goal of this standard is to respond to each incident consistently, effectively and as close to real time as possible to protect DHHS information assets.

29.1.1 Identification

Identification is formal acknowledgement that an incident has occurred. Depending on who received the initial notification of an incident, triage shall be conducted by the AISO, DHHS Help Desk, HIPAA Office, DHHS Privacy Official or IS&T Management to understand the impact of the incident and initiate appropriate action. Once an incident has been identified and reported, the AISO will assume oversight of the incident response and will continually assess the incident conditions and determine if escalation of response actions is appropriate. Prevention of damage shall have priority over forensics of incident source. Therefore, the AISO and DHHS CIO reserve the right to quarantine any potentially threatening system and terminate any threatening activity using all means necessary.

29.1.2 Procedure

Procedures spell out the actions required to resolve the security incident. At a minimum, DHHS internal procedures require minimization of damage from the incident. The first priority is to shut off or terminate any potential threat. This action should be performed in a manner that allows for preservation of evidence, but if there is ANY doubt, all DHHS personnel, whether employees or contractors, are required to disable the threat immediately. Following the assessment and termination of the threat, the next priority is containment followed by recovery actions, damage determination, report documentation, lessons learned, and identification of corrective actions. Distribution and/or notification will include coordination of the ISO, DHHS CIO, Legal, DHHS Privacy Officer, and Communications and Legislative Services. These are the only parties who will communicate to customers or Senior Leadership of DHHS. All outsourced support, including any IT Support, will communicate with parties necessary for responding to the incident, and the ISO or IS&T management only.

29.1.2.1 Reportable conditions, such as the breach of PII, PHI, or FTI, require notification by the Agency to the appropriate federal agency within specific timeframes of DHHS becoming aware of an incident, as defined by federal regulations.

29.1.2.2 As soon as an incident is detected, personnel qualified and designated to respond shall be notified to take immediate action, determine incident impact, file a ticket, or prepare a report.

29.1.2.3 The AISO will track all Agency-reported security incidents. DHHS Staff who observe, experience, or are notified of a security incident, should immediately report the situation to the AISO and the DHHS Help Desk. All contracted support personnel are required to notify their DHHS sponsor or appropriate DHHS leadership immediately of any suspected security incident or breach.

29.1.2.4 If the incident appears to have ANY client information compromised, including any PHI, PII, or FTI, immediate notification to the AISO, Legal, Privacy Officer, or DHHS CIO is REQUIRED. The Privacy Officer or DHHS CIO will notify Senior State officials and will determine the level of contact with DHHS customers and government agencies. DHHS Senior Management or designee will oversee and coordinate all communication actions.

29.1.2.5 DHHS Help Desk, AISO, or IS&T Management will conduct incident triage to establish the impact level and conduct corresponding notifications of officials and Incident Response Team.

29.1.2.6 The AISO or CIO will issue the order of action, if a security incident is not controlled in a timely manner (typically 12 hours).

29.1.2.7 Upon confirmation, the security incident response actions and remediation will be immediately implemented and documented by the AISO.

29.1.2.8 Any compromised or suspected to be compromised device may be disconnected from the DHHS network without warning

29.1.2.9 All incidents except those classified as ‘low’ impact are required to have an incident report completed. Documentation of information is critical in situations that may eventually involve authorities as well as provides documentation of the actions taken to resolve the event. A copy of the incident report form is available from the AISO.

29.1.3 Analysis

Analysis is examination of the incident to determine the impact to the agency, and the root cause of the incident. Initiate a damage analysis of security incidents immediately after assessment by the AISO, IS&T Management and their engineering and security teams as required. The AISO and IS&T will determine if the incident affects organizations outside of the DHHS internal network. DHHS Senior Management will be notified of analysis results and client impact immediately upon discovery, and shall be kept abreast of all analysis findings, impact assessments, and remediation progress.

In the event of a discovery of a breach of system security protections, an internal security investigation must be properly performed. The chain of custody steps that should be taken in the event of a security breach are as follows:

29.1.3.1 If possible, immediately remove compromised systems from network by disconnecting the network cable. DO NOT turn off the system unless that is the only way to stop the threat. Do NOT log in or change passwords if possible. Logging on to or turning off the system can result in temporary memory being overwritten or deleted, removing valuable evidence used to determine the root cause.

29.1.3.2 If the system cannot be taken off the network, take pictures and screenshots.

29.1.3.3 Notify the AISO immediately after initial steps, but NO LATER than 30 minutes after becoming aware of the possible incident.

29.1.3.4 Dump memory contents to a file.

29.1.3.5 Image (bit copy) the device hard drive before investigating (i.e., opening files, deleting, rebooting) to ensure as much forensic evidence as possible is retained.

29.1.3.6 Log all activities taken.

29.1.3.7 Label all evidence and be able to present an affidavit to ensure the chain of custody is maintained.

29.1.4 Recovery

Activities necessary to return to normal operations and implement long-term corrective actions to minimize the probability of recurrence. The DHHS Incident Response team, working with application and data owners, shall evaluate and determine when to return compromised systems to normal operations. Access to compromised systems shall be limited to authorized personnel until the security incident has been contained and root cause mitigated. Complete analysis and mitigation procedures as soon as possible, recognizing DHHS systems are vulnerable to other occurrences of the same type. Recovery procedures shall address:

29.1.4.1 The agency shall define and prioritize recovery requirements before returning affected or compromised systems to normal operations. Recovery strategies may include, but are not limited to:

29.1.4.1.1 Restoring compromised systems from a trusted baseline.

29.1.4.1.2 Restoring system user files, startup routines, or settings from trusted backups.

29.1.4.1.3 Validation of restored systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons.

29.1.4.2 Increasing Security Monitoring. DHHS shall heighten awareness and monitoring for a recurrence of the incident.

29.2 Post-mortem activities (After-Action)

Post-mortem activities may be required if the incident is severe and wide-spread enough to warrant further discussion. After action discussions should include lessons learned (strengths and areas needing improvement), any potential changes to policy and procedure, and Plans of Action and Milestones to implement or track any necessary changes.

29.3 Incident Management Training and Testing

DHHS shall provide training on incident recognition and reporting requirements to all staff. More in-depth training and awareness will be given to all applicable staff in incident response and recovery procedures and reporting methods. The AISO shall provide annual training and simulated incident response and recovery testing for the DHHS Security Incident Response team. The AISO and DHHS Incident Response Team shall also receive annual education and awareness of the various laws and regulations related to privacy and reporting of breaches of PHI, PII or FTI.

THIS PAGE INTENTIONALLY LEFT BLANK

Section 7 - DHHS Information Technology (IT) Auditing Standard

30.0 INTRODUCTION

Nebraska Department of Health and Human Services (DHHS) Policy requires the DHHS Information Security Officer (AISO) to establish and manage an entity-wide oversight and compliance function of Agency-specific applications and functions. This includes a managed review of auditing logs and records of security-related events to provide DHHS with assurance of policy compliance throughout DHHS.

30.1 Purpose and Objectives

This standard establishes requirements for DHHS to maintain log records according to policy and DHHS document retention requirements.

30.1.1 Audit log records shall be periodically reviewed for indications of inappropriate or unusual activity, and findings reported to designated DHHS officials. Audit log records pertaining to FTI access must be reviewed on a weekly basis.

30.1.2 Servers deployed at DHHS shall be configured according to DHHS policies and standards and inspected for compliance with this standard at least annually and as prescribed by applicable regulatory compliance.

30.1.3 Logs may be maintained for longer periods as required to provide evidence that may be necessary for investigations, forensics, or legal discovery purposes.

30.1.4 All logs shall be treated as CONFIDENTIAL information and appropriately secured and protected.

30.1.5 Systems shall have sufficient storage capacity to meet audit log retention requirements.

30.1.6 Automated mechanism shall be created for logs near capacity notification.

30.2 Scope and Applicability

30.2.1 This standard applies to all systems owned, leased, operated, or maintained by DHHS.

30.2.2 Audit and logging requirements also exist for business applications, such as disclosure of sensitive information (e.g., PHI, FTI, and PII) for business purposes or application security events. The requirements for auditing and logging of sensitive information disclosure or handling are not within scope of this standard. Disclosure log handling is covered in the Incident Response Policy Standard.

30.3 Enforcement

30.3.1 Enforcement of DHHS IT Policies and Standards is defined in the DHHS IT Security Policy.

31.0 STANDARD

All systems used to manage CONFIDENTIAL or RESTRICTED information, interconnect with other systems, or make access control (authentication and authorization) decisions, shall record and retain audit-logging information sufficient to answer the following questions:

- Who or what performed the activity, including the system and the activity performed (User or system account)?
- What activity was attempted or performed (add/delete/modify)?
- On what object (file, user account, device, etc.) was the activity performed?
- Date/Time stamp of when the activity was performed
- What tool(s) were used to perform the activity?
- What was the status (such as success/failure/result) of the activity?

31.1 Log Format, Storage, Failure notification and Retention

31.1.1 Systems should have the capability to support formatting and storing audit logs in a manner that ensures the log integrity and supports enterprise-level analysis and reporting. Some mechanisms known to support these goals are listed in the DHHS Audit Logging and Monitoring Procedures.

31.1.2 Sufficient audit log storage capacity must be allocated to ensure availability of log information to meet policy requirements. Log file capacity and utilization shall be regularly monitored and reported. Systems Administrators will take appropriate action to keep an appropriate level of free space available. IS&T shall perform annual capacity planning and trend analysis to reduce the likelihood of exceeding capacity.

31.1.3 Systems should have the capability to provide automated notification to appropriate IS&T personnel if

31.1.3.1 the capacity of log files reaches or exceeds defined threshold levels

31.1.3.2 an audit processing failure (e.g., shut down information system, unintended overwriting of the oldest audit records, stop generating audit records, etc.).

31.1.3.3 the audit logging system fails for any reason.

31.1.4 All system logs shall be sent to a central log review system which is protected from unauthorized access and backed up for availability and integrity purposes.

31.1.4.1 Access logs (domain logon, etc.,) should be kept for at least 90 days.

31.1.4.2 System logs may be kept up to one (1) year or longer if requested or as required for investigative or legal purposes. Events should be summarized and reported monthly, or on request.

31.1.4.3 Logs governed by Federal Privacy Regulations (such as IRS, SSA or CMS data handling) may have retention requirements that exceed these standards. Examples of longer retention requirements include:

31.1.4.3.1 Log files for access to FTI must be maintained for seven (7) years

31.1.4.3.2 Log files for access to PHI must be maintained for at least ten (10) years

31.1.4.3.3 Log files for access to SSA data must be maintained for at least six (6) years

31.2 System and Network Infrastructure Auditable Events

31.2.1 System and Network infrastructure are defined as “the LAN, WAN, Servers, firewalls, and Routers/Switches use to provide electronic communication and data /information processing”.

31.2.2 Security safeguard regulations require logging and reviewing events that are determined to have a level of risk above “low” as identified by DHHS Risk Management procedures. Auditable events may be incorporated into system auto logs and change management documents.

31.2.3 The following System and Network Infrastructure events should be logged and periodically reviewed, unless the risks of security incidents can be mitigated or reduced to acceptable levels through other security mechanisms:

- Successful or failed user access events (logon/log-off) to the DHHS domain
- Setting of system time
- Additions, deletions or changes to the audit settings or log files
- Privileged account activities such as account creation/deletion or other root or domain administrator level activities.
- System, Server, and Network startup and shutdown
- System, Network, or Services configuration changes, including installation of hardware, firmware or software patches and updates, or other installed software changes
- Initiation, acceptance, or rejection of a network connection
- Grant, modify, or revoke system access privileges, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, and user password changes
- Modification of Firewall rules or other boundary protection settings
- Detection of suspicious/malicious activity from an Intrusion Detection or Prevention System (IDS/IPS), antivirus system, or anti-spyware system.
- Physical access to secured and restricted areas or facilities where application, system and network infrastructure reside (may require manual entry logs subject to retention and review requirements)

31.2.4 Audit Log Contents

Logs shall contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. At a minimum, the logs should contain the following elements:

- Date/time stamp the action was performed, obtained from internal system clocks, including relevant time-zone information if not in Coordinated Universal Time (UCT).
- Type of action: Examples include authorize, create, read, update, delete, and accept network connection.
- Subsystem performing the action: Examples includes process or transaction name, process or transaction identifier.
- Identifiers (as many as available) for the subject requesting the action: Examples include user name, computer name, IP address, and MAC address. Such identifiers should be standardized in order to facilitate log correlation.
- Success/failure of the action and the appropriate code provided by the access control mechanism.

31.3 Audit review, Monitoring, Findings, and Remediation

31.3.1 Security safeguard regulations require regular inspections of system audit logs for indications of inappropriate or unusual activity. These logs shall be reviewed by authorized personnel (representative of the data owner) to facilitate investigations of suspicious activity or suspected violations. All reports of findings shall be reported to appropriate officials who will prescribe the appropriate and necessary actions.

- Logs of system capacity and log integrity shall be reviewed on a daily basis.
- Logs used to determine anomalies in system or network utilization shall be reviewed on a daily basis
- Logs of privileged access account creation or modification shall be reviewed at a minimum of every two weeks
- All other logs shall be reviewed at a minimum of monthly

31.3.1.1 Other logs may be reviewed more frequently as required by state or Federal guidance.

31.3.2 Where possible, employ automated mechanisms to alert designated staff when inappropriate or unusual activities with security implications are discovered. Any automation used for log analysis must not change the underlying log structure. As long as original audit logs remain unchanged and secured, the use of log analysis tools to extract data for analytical review is acceptable.

31.3.3 All relevant findings discovered as a result of an audit may be listed in the DHHS tracking system or Information Security Plan of Action and Milestones (POA&M) process to ensure prompt resolution or appropriate mitigating controls. All results and findings generated by the audit or review process must be provided to appropriate DHHS management within one week of project/task completion. This report will be considered CONFIDENTIAL DHHS information.

31.4 Application Logging Review and Monitoring

DHHS requires application development or acquisition activity include applicable application logging for security events. Application logs are invaluable data for identifying security incidents, monitoring policy violations, establishing baselines, providing information about problems and unusual conditions, contributing additional application-specific data for incident investigation which is lacking in other log sources, and helping defend against vulnerability identification and exploitation through attack detection.

31.4.1 Application logging must be commensurate with audit and logging requirements prescribed by data sharing agreements or state and federal security regulations. Examples of oversight regulations:

- IRS Data Use Agreement:

IRS Publication 1075, Section 9.3.3.2 – Security-relevant events must enable the detection of unauthorized access to FTI data. Auditing must be enabled to the extent necessary to capture access, modification, deletion and movement of FTI by each unique user.

- HIPAA Security Standard - Information System Activity Review

Security Rule 45 CFR § 164.308(a)(1)(ii)(D) – “Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.”

31.4.2 Application logging may be used to record other types of events. Application logging content must be part of the overall system analysis and design activity, and should consider:

- Application process startup, shutdown, or restart
- Application process abort, failure, or abnormal end
- Significant input and output validation failures
- Business process monitoring (e.g., activity abandonment, transactions, connections, information requests)
- Audit trails (e.g., data addition, modification and deletion, data exports)
- Performance monitoring (e.g., data load time, page timeouts)
- Compliance monitoring and regulatory, legal, or court ordered actions.
- Authentication and authorization successes and failures;
- Session management failures
- Use of higher-risk functionality (e.g., addition or deletion of application credentials, changes to privileges, assigning users to tokens, adding or deleting tokens, submission of user-generated content - especially file uploads)
- Legal and other opt-ins (e.g., permissions for mobile phone capabilities, terms and conditions of use, personal data usage consent, permission to receive marketing communications)
- Suspicious, unacceptable or unexpected behavior

31.4.3 Application logs shall be reviewed weekly. Corrective actions to address application deficiencies will be managed through either the application development or the POAM process.

31.5 Audit and Logging Requirements for Business Partners

31.5.1 This standard may be adapted for use in DHHS procurement standards and RFP templates to ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

31.6 Audit Review and Scheduling

31.6.1 The AISO is responsible for maintaining an audit schedule detailing required periodic IT audits. The schedule will detail the yearly dates of each audit, what business unit or program area is responsible for completing the audit, and the date the audit is completed. This schedule at minimum will include:

31.6.1.1 Weekly RACF Report Review

31.6.1.2 Bi-annual Alter Access review for systems managing CONFIDENTIAL and RESTRICTED data

31.6.1.3 Annual Timely Termination Review

31.6.1.4 New-Hire and Annual Privacy & Security Awareness Training Review

31.6.1.5 Annual External Partner Account and Access Review

31.6.1.6 Periodic Physical Safeguard Site Review of DHHS Offices and Facilities

31.6.1.7 Daily, Weekly, and Monthly review of logs from auditable events

THIS PAGE INTENTIONALLY LEFT BLANK

Section 8 - DHHS Information Technology (IT) Security and Privacy Education and Awareness

32.0 INTRODUCTION

DHHS staff must know and understand IT security and privacy requirements related to the protection of DHHS IT resources and client information. Training in either online or classroom settings is necessary to relay or reinforce security and privacy requirements.

32.1 Purpose and Objectives

This standard identifies IT Security and Privacy Awareness training requirements for DHHS Staff to ensure training is completed and acknowledged within required time limits recommended by the supervisor or the Agency.

32.2 Scope and applicability

This standard applies to all DHHS personnel, contractors, temporary employees, volunteers, vendors and business partners (hereinafter "Staff") with access to DHHS IT resources who are required to receive periodic training on DHHS IT Policies, procedures, and standards.

33.0 TRAINING METHODS AND TRACKING REQUIREMENTS

Training may be conducted online (self-paced) or in a classroom environment (one or multiple-day training). Acknowledgement of completed training is required to provide a permanent record. Supervisors should have access to physical or online training logs for their respective work center. Staff are responsible for ensuring their training is current. Training records will be retained for a minimum of 5 years.

33.1 Online training should be conducted through the State of Nebraska provided training portal unless other methods are approved and means to provide proof of completion are available.

33.1.1 Staff should request online training modules and complete the training in a timely manner. Completion of training should have a minimal impact on work performance.

33.1.2 Supervisors should assign and/or approve the training required for the work center and the most appropriate means by which to complete the training.

33.1.3 Staff requesting training modules or certifications that require a fee should refer to their supervisor and State of Nebraska policies for payment or reimbursement.

33.2 Classroom training should be conducted in State of Nebraska facilities or in facilities made available by the state or Agency.

33.2.1 Supervisors should assign and/or approve the training requested or required for Staff and schedule the training to minimize impact on the business unit workload.

33.2.2 Staff requesting a training class or certification through a paid private vendor should refer to State of Nebraska policies for attendance requirements and reimbursement.

33.3 Staff should be provided time during their normal business hours to complete mandatory training. Outlying state offices and 24-hour facilities may have internal procedures for the completion of training. Mandatory training shall be tracked by the Agency or assigning individuals. Supervisors will be notified if training is not completed within the required time.

34.0 DHHS TRAINING MODULES

34.1 IT Security and Privacy Awareness Training for New Employees

34.1.1 All Staff are required to attend and/or complete IT Security and Privacy Awareness training as part of their orientation. Staff will sign an acknowledgement of understanding and obligation to comply with the security policy no later than 30 days after their employment start date. The Agency will maintain records of attendance and completion.

34.1.2 Staff transferring within the Agency are not required to re-accomplish this module if training is current.

34.1.3 Staff transferring to DHHS from other State of Nebraska agencies may not be required to complete initial IT Security Awareness training if they are in good standing with their previous Agency.

34.2 IT Security and Privacy Awareness Annual Refresher Training

34.2.1 On an annual basis, all DHHS Staff are required to complete IT Security and Privacy Awareness training. The Agency will maintain records of completion.

34.2.2 Staff transferring within the Agency are not required to re-accomplish this module if training is current.

34.2.3 Staff transferring to DHHS from other State of Nebraska agencies may not be required to complete the IT Security Awareness training if they are in good standing with their previous Agency, but will be required to complete the training in the next annual cycle.

34.3 Federal Tax Information (FTI)

All Staff with direct access to Federal Tax Information (FTI) or access to systems used to store or process FTI (i.e., DHHS, OCIO, or other contracted service provider systems administrators or applications developers) are required to complete initial training and annual recertification on handling and disclosure of FTI prior to accessing data. This requirement includes any Staff who have the potential for incidental exposure to FTI because of their job duties.

34.3.1 Training will be logged and monitored.

34.3.2 Supervisors will be notified if staff do not complete training within the allowable time frame.

34.3.3 Access to FTI or the systems used to store or process FTI will be suspended until the mandatory training is completed.

34.4 HIPAA training (use of protected health information)

All Staff with access to Protected Health Information (PHI) or access to systems used to store or process PHI (i.e., DHHS, OCIO, or other contracted service provider systems administrators or applications developers) are required to complete initial training and annual recertification on handling and disclosure of PHI prior to accessing this data. This includes any Staff who have the potential for incidental exposure to PHI because of their job duties. The Agency will maintain records of attendance and completion.

34.5 Other training

34.5.1 The Office of the Chief Information Officer has the option to periodically assign IT Security Awareness training modules to all State of Nebraska employees though the State of Nebraska website LINK – Employee Development Center (EDC). This training is considered mandatory and the Agency will maintain records of completion.

34.5.2 Additional training (online and classroom) requiring registration through LINK-EDC may require a fee and/or supervisor approval. Staff should discuss with their supervisor before making the request.

THIS PAGE INTENTIONALLY LEFT BLANK

Section 9 - DHHS Information Technology (IT) Media Protection and Disposal

35.0 INTRODUCTION

Disclosure of sensitive information through improper storage, disposal or re-use of digital and non-digital media presents a risk to the State of Nebraska. A plan for protection and proper disposal of media must be established to minimize this risk. Storage devices containing sensitive information such as hard disk drives, paper or other storage media (e.g. tape, diskette, CDs, DVDs, USB drives, cell phones, memory sticks, digital copiers/printers/scanners with data storage capabilities) regardless of physical form or format must be properly disposed of when the data contained on the device is no longer required or the device itself is no longer usable.

35.1 Purpose and Objectives

35.1.1 The purpose of this policy standard is to ensure media is properly secured, stored, labeled and disposed of based on the data categorization standard and the data owner. The level of security required for information system media is dependent on the security category of the information.

35.1.2 The minimum-security requirements that must be adhered to in order to establish a consistent baseline of security are identified in this standard. Depending on the needs of the Agency data owner, the type and categorization of the data processed, stored, or transmitted, or other federal or state statutory requirements, there may be more stringent security control requirements. In the event of conflicting guidance, the more stringent rules shall apply.

35.1.3 The following guidance should be used for media sanitization

35.1.3.1 NIST SP 800-88, Guidelines for Media Sanitization

35.1.3.2 NIST SP 800-53, Security Controls and Assessment Procedures for Federal Information Systems and Organizations

35.1.3.3 IRS Publication 1075, Tax Information Security Guidelines For Federal, State and Local Agencies

35.2 Definitions

35.2.1 Definitions and acronyms are found in at the end of this document.

36.0 SCOPE AND APPLICABILITY

36.1 This standard applies to all DHHS personnel, contractors, consultants, temporary employees, volunteers, vendors, and business partners (herein referred to as “Staff”) with access to DHHS or State of Nebraska IT resources owned, leased or supported by DHHS, OCIO, or any outside entity that has a signed Third-party or Business Partner Agreement with DHHS.

36.2 This standard also applies to DHHS or State of Nebraska IT resources owned, leased or supported by DHHS or OCIO with the ability to create, process, access, or store information in either digital or printed form.

37.0 ROLES AND RESPONSIBILITIES

37.1 Agency Information Security Office (AISO)

37.1.1 Develop and maintain DHHS IT Security policies, standards and procedures to protect agency information systems.

37.1.2 Ensures successful implementation of DHHS Information Security Policies.

37.2 IS&T

37.2.1 Works with Agency to approve physical and logical access to systems and applications

37.2.2 Facilitate sanitization or destruction of electronic media

37.3 Business Units

37.3.1 Appoint a security administrator responsible for the control/management of media storage devices in their work center.

37.3.2 Coordinate with IS&T for the acquisition and final disposition of removable media

37.3.3 Maintain a lockable storage area or other container for securing media devices when not in use.

38.0 STANDARDS

38.1 Encryption

38.1.1 Laptop computers shall be full-disk encrypted using approved methods and technology.

38.1.2 Peripheral devices (e.g., printers or Multi-function (printer/scanner/copier/fax)) with an internal hard disk drive shall have full-disk encryption AND the capability of overwriting data after each print job enabled.

38.1.3 All other electronic devices designed to be portable or removable must be fully encrypted.

38.2 Media Access

38.2.1 The Business Unit shall approve and authorize the use of, and access to, digital and non-digital media.

38.2.2 Controls to restrict access to digital and non-digital media to authorized users according to Business Unit requirement shall be implemented.

38.3 Media Marking

38.3.1 Business Units shall define removable Information System media and Information System output indicating the distribution limitations, handling caveats, and applicable security markings of the information as required.

38.3.2 Removable Information System media and Information System output shall be marked to indicate the distribution limitations, handling caveats, and applicable security markings of the information as required.

38.4 Media Storage

38.4.1 Digital and non-digital media may never be left unattended.

38.4.2 When not in use, digital and non-digital media must be stored in a secure area or locked container according to Federal, State, and Local policy and procedures.

38.4.3 Media shall be secured until it is destroyed or sanitized using approved equipment, techniques, and procedures.

38.4.4 Turn over unidentifiable or unattended electronic media to the AISO for disposition.

38.4.5 Dispose of unidentified/unattended paper media per office policy.

38.5 Media Transport

38.5.1 The Agency shall protect, control, document, and maintain accountability for digital and non-digital media during transport outside of controlled areas.

38.5.2 The Agency shall implement encryption via software and/or hardware mechanisms to protect the confidentiality, integrity, and availability of information stored on digital media during transport outside of controlled areas.

38.5.3 The Agency shall ensure that only authorized personnel transport Information System media in accordance with Business Unit requirements.

38.6 Personally-owned Media Use

38.6.1 USE OF PERSONALLY-OWNED MEDIA STORAGE DEVICES ON STATE OF NEBRASKA OR DHHS-OWNED INFORMATION SYSTEMS OR SYSTEM COMPONENTS IS PROHIBITED.

39.0 MEDIA SANITIZATION AND DISPOSAL

39.1 Serviceable electronic media may be reused.

39.1.1 Prior to reuse, the media must be overwritten a minimum of three times using an approved method.

39.2 Electronic media that is unserviceable (i.e., corrupted or physically damaged to the point where it cannot be restored to a usable status) or has extended past its normal service life (i.e., no longer supported by the vendor) shall be disposed of using one or more of the following methods:

39.2.1 Overwriting

39.2.2 Degaussing

39.2.3 Physical destruction by crushing, shredding, melting or otherwise dismantling a media device to the point where the storage platters or memory chip cannot be read.

39.3 Paper media must be kept in a locking shred container in a secure area until it can be destroyed using approved disposal methods.

39.3.1 Use of an approved shred vendor is allowable for paper media that does not contain FTI.

39.3.2 Any documents containing FTI must be kept separate from all other paper and shredded to a dimension prescribed by IRS Publication 1075.

39.3.3 Burning must reduce the print media to ash.

39.4 An attestation of the destruction of media must be provided. Destruction logs or certificates of destruction must be maintained in accordance with State of Nebraska data retention rules.

THIS PAGE INTENTIONALLY LEFT BLANK

Section 10 - DHHS Information Technology (IT) Acceptable Use

40.0 INTRODUCTION

The Nebraska Department of Health and Human Services (DHHS, also referred to as "the Agency") and State of Nebraska information technology (IT) resources are effective tools for DHHS staff, provided the resources are adequately protected and used for their intended purpose.

IT resources provided by DHHS and the State of Nebraska are for performing Agency business and are the property of DHHS and the State of Nebraska. Acceptable use of DHHS IT resources and the State Data Communications Network (SDCN) is limited to activity directly related to performing state business and encourages staff to add a personal layer of security to the protection of DHHS IT resources.

40.1 Purpose

The purpose of this policy is to:

40.1.1 Define acceptable use of DHHS and State of Nebraska IT resources

40.1.2 Promote effective and efficient use of information technology resources.

40.2 Scope and Applicability.

40.2.1 This policy applies to DHHS personnel, contractors, consultants, temporary employees, volunteers, vendors, and business partners (herein referred to as "Staff") with access to DHHS and State of Nebraska IT resources.

40.2.2 This policy shall also apply to all DHHS and State of Nebraska IT resources (as defined in section 42 of this policy) owned, leased, or managed by DHHS or the State of Nebraska.

40.3 Roles and responsibilities

40.3.1 All Users

40.3.1.1 Know and understand the acceptable use of DHHS IT resources, as well as any policy enforcement requirements.

40.3.1.2 Report any potential policy violations

40.3.2 Agency supervisors and management

40.3.2.1 Know and understand the acceptable use of DHHS IT resources

40.3.2.2 Provide training and reinforce the requirements for the acceptable use of IT resources.

40.3.3 Agency ISO (AISO)

40.3.3.1 Prepare, maintain, and disseminate IT Security Policies and Standards to Agency Staff

40.3.3.2 Provide periodic training on acceptable use

40.3.4 IS&T

40.3.4.1 Review audit logs for anomalous behavior

40.3.4.2 Provide audit log information to support investigation of acceptable use incidents.

40.3.4.3 Enforce policy and ensure staff is trained on acceptable use

40.3.4.4 Investigate and remediate policy violations in their respective work centers.

41.0 POLICY

This DHHS policy complements Nebraska Information Technology (NITC) policies, standards and guidelines and is focused on the Agency's responsibilities for acceptable use.

41.1 Acceptable Use Policy

41.1.1 All electronic information created, compiled, processed, stored, transmitted or used by Staff in the course of doing business is the property of DHHS. Such information is subject to Federal, State, Agency or business unit policies, procedures, privacy rules and regulations, and acceptable use guidelines.

41.1.2 Staff are responsible for the reasonable care and protection of DHHS and State of Nebraska IT resources and for meeting Federal, State, and Agency policies and standards governing their use.

41.1.3 Use of IT resources for any purpose other than conducting state business will be considered a violation of this policy.

41.2 Policy enforcement

This Policy is written to enforce State and Local policies and standards and complement Federal regulations regarding the confidentiality, integrity and availability of information. As such, violations of this policy and/or any associated DHHS IT policy standards may result in actions taken against DHHS Staff, pending the outcome of an investigation.

41.2.1 Violation of Federal laws (e.g., IRS, HIPAA, SSA, etc.,) may result in criminal or civil actions and any associated penalties and fines for DHHS and/or DHHS Staff involved.

41.2.2 If a violation of this policy and/or any associated DHHS IT policy or standard occurs, the offending area's management is responsible to investigate, mitigate and/or remediate the violation in a timely manner.

41.2.3 Any Staff working directly for DHHS found in violation of this policy and/or associated IT policy standards shall be held accountable for their actions and any reasonable foreseeable consequences of those actions. In addition to any Federal criminal or civil actions, Staff may be disciplined in accordance with applicable workplace policies and labor contracts administered by DHHS up to and including restitution for damages and termination of employment.

41.2.4 Any Staff working for a business partner under contract with DHHS to provide services to or on behalf of the Agency found in violation of this policy and/or associated IT policy standards may be disciplined in accordance with State and Federal laws and any penalty provisions as defined in the service contract up to and including termination of the service contract.

42.0 ACCEPTABLE USE OF IT RESOURCES

Acceptable use of IT resources is limited to activity necessary for the performance of State of Nebraska and DHHS business, or State-sponsored activities. IT resources are any hardware, software or data used by DHHS Staff to perform their assigned business activities. These resources must be owned, leased, managed or approved for use by the State of Nebraska and DHHS, and meet published specifications and requirements.

42.1 IT Devices

IT devices are any electronic devices used to create, store, process, or exchange information managed by DHHS. IT Devices include, but are not limited to: desktop, server, mainframe, laptop or tablet computers; personal digital assistants (PDAs); MP3 Players or other recording or playback device; printers, copiers and multifunction devices; routers; switches; portable storage devices (hard drives, USB flash drives, CD/DVD, etc.); digital cameras; cellular or smart phones (includes voice recording and camera features); or any other electronic device that may be used to create, store, process or exchange information managed by DHHS.

42.1.1 Authorized Home Office access to DHHS network, applications, email, and/or DHHS information is restricted to the use of desktop computers, laptops, remote access software, and procedures provided by or approved by IS&T.

42.1.2 Staff authorized to work from remote locations using personal devices may only access DHHS IT resources using a uniquely assigned DHHS account.

42.1.2.1 CONFIDENTIAL and RESTRICTED data owned by DHHS may only be accessed or processed using a DHHS-provided account.

42.1.2.2 CONFIDENTIAL or RESTRICTED data owned by DHHS, or accessed from a DHHS IT Device, shall not be stored on any IT Devices not owned, managed, or approved by IS&T.

42.1.2.3 Staff must ensure personal IT Devices approved to connect to the DHHS network are updated with current software patches and meet minimum-security safeguard and security software requirements as defined in the DHHS IT Securing Hardware and Software Standard (Section 2).

42.1.2.4 Wireless access devices (including but not limited to laptop computers, smartphones, tablet computers, and other mobile devices) used by Staff for business activities must:

42.1.2.4.1 be owned, leased, or approved by DHHS

42.1.2.4.2 meet state and agency specifications and requirements

42.2 DHHS Network

The DHHS network is the Local Area Network (LAN), Wide Area Network (WAN), Internet/Intranet/Extranet and DHHS Cellular or Broadband access owned, supported, contracted, or managed by DHHS or the State of Nebraska OCIO. Staff are responsible for the reasonable protection and use of the DHHS network access assigned to them and must follow the guidance of the DHHS IT Security Policies and Standards, as well as the NITC IT Security Policies and Standards.

42.2.1 No Individual may implement wireless technology to process any DHHS transactions without the review and approval of the IS&T.

42.2.2 Only authorized staff may install a wireless access device to the DHHS network connection jack, port, PC, or other devices connected to the DHHS network.

42.2.3 DHHS network access may not be used to perform any illegal activity such as:

42.2.3.1 trying to gain unauthorized access to restricted sites (hacking);

42.2.3.2 harassment of any kind;

42.2.3.3 creation of unauthorized Intranet sites or pages;

42.2.3.4 downloading or sharing of copyrighted material, such as music, videos or other imagery;

42.2.3.5 downloading, installing, or sharing of unlicensed software;

42.2.3.6 the production of any material that may be deemed offensive; or,

42.2.3.7 deliberately attempting to spread malware of any kind.

42.2.4 The DHHS network operates on the SDCN managed by the OCIO. The following are acceptable uses as published in NITC 7-101, Acceptable Use Policy:

42.2.4.1 For conducting state business.

42.2.4.2 For state government sponsored activities.

42.2.4.3 For use by state Staff and officials for emails, text messaging, local calls, and long-distance calls to children at home, teachers, doctors, daycare centers, baby-sitters, family members, or others to inform them of unexpected schedule changes, and for other essential personal business. Any such use for essential personal business shall be kept to a minimum and shall not interfere with the conduct of state business. State Staff or officials shall be responsible for payment or reimbursement of charges, if any, that directly result from any such communication. [Neb. Rev. Stat. § 81-1120.27(1)]

42.2.4.4 Essential personal business does not include use of the SDCN for personal financial gain or campaigning for or against the nomination or election of a candidate or the qualification, passage, or defeat of a ballot question. [Neb. Rev. Stat. § 49-14,101.01(2) and § 49-14,101.02(2)]

42.2.4.5 For such other uses as allowed by law.

42.3 Electronic Communication

Electronic communication includes email, instant messages, electronic data exchange, and any other electronic method of exchanging information created, stored, contracted, or managed by DHHS.

42.3.1 Transmitting or emailing CONFIDENTIAL or RESTRICTED DHHS information for use in an unauthorized remote location is prohibited.

42.3.2 Transmitting or emailing FTI is prohibited.

42.3.3 Emailing CONFIDENTIAL or RESTRICTED DHHS information to external partners must be encrypted using DHHS-approved tools and methods

42.3.4 Deliberate spreading of software viruses, unsolicited email or electronic messages (i.e., SPAM) is prohibited.

42.3.5 Electronic communication technology that is not provided or approved by IS&T is prohibited.

42.3.6 Use of personal email accounts (e.g., Hotmail, Yahoo, Gmail, etc.,) or other external resources to conduct official State of Nebraska business is prohibited.

42.3.7 Remote access to the DHHS network, LAN, WAN, or any software application is permitted after review and approval by IS&T.

42.3.8 Email messages containing State or DHHS information may not be forwarded from a state email account to a personal email account.

42.3.8.1 E-mail messages on the mail servers are the property of DHHS and the State of Nebraska

42.3.8.2 Such e-mail may contain sensitive client information, cannot be protected outside of the State network, and may result in data compromise.

42.3.8.3 Staff may not create a rule in their e-mail account to auto-forward e-mail traffic.

42.3.8.3.1 The auto-forward rule does not allow messages containing sensitive information to be encrypted.

42.3.9 Multifunction devices may not be used to scan and send documents via e-mail to non-DHHS e-mail accounts. Such transmissions are not secure and may result in data compromise.

42.4 DHHS Electronic Information (Data)

Electronic information is any digital information (data), pictures or graphics owned, created, stored, retrieved, processed, contracted, maintained, or managed by DHHS.

42.4.1 Use of electronic information is subject to all policies, procedures, privacy rules and regulations, and acceptable use guidelines implemented by the DHHS agency, division, or program area that owns or holds the license of the electronic information.

42.4.2 Accessing or attempting unauthorized access to DHHS CONFIDENTIAL and RESTRICTED information for other than a required business “need to know” is prohibited.

42.4.3 Users must store CONFIDENTIAL and RESTRICTED information on Agency-managed and secured file servers or web portals. Due to storage constraints, Agency desktop, laptop and tablet computer hard drives ARE NOT BACKED UP by DHHS. Any information stored on local computer storage drives will be lost when computers are re-imaged.

42.4.4 CONFIDENTIAL and RESTRICTED electronic information SHALL NOT be copied, processed, or stored on personally owned IT devices.

42.4.5 Electronic information may not be copied or distributed in a manner that violates copyrights, policies, procedures, privacy rules and regulations, and acceptable use guidelines implemented by the Federal Agencies, DHHS, or the program area that owns or holds the license of the electronic information.

42.4.6 CONFIDENTIAL and RESTRICTED electronic information may not be copied or stored on a mobile or portable IT device unless the device is fully encrypted using procedures provided by or approved by IS&T.

42.5 Electronic (digital) signatures

Nebraska Administrative Code (NAC) Title 437 Digital Signatures Act sets the standard for the creation of and use of electronic signatures as enacted by Nebraska Revised Statute §86-611.

42.5.1 Use of electronic signatures must comply with all standards established by NAC Title 437 and meet the electronic signature configuration requirements defined in NAC Title 437 Chapter 7.

42.6 Social media

Social Media is any form of electronic communication, usually web-based, through which people create online persona or communities to share information, ideas, or other content (such as videos, photographs or sound files).

42.6.1 Use of DHHS IT assets to access or interact with social media is limited to the actions and activity defined in the DHHS Social Media Policy managed by the DHHS Communications and Legislative Services unit.

42.6.2 Publishing (posting) protected information including, but not limited to: client, patient or employee data, video, pictures, email, or text messages on any social media, is prohibited.

42.7 Acceptable Use of DHHS Software and Data applications.

Data applications are created, owned, licensed, or managed by DHHS and used to create, store, retrieve, process, transmit and maintain information owned, supported, contracted, or managed by DHHS.

42.7.1 Use of Agency-owned software applications is subject to all policies, procedures, security/privacy rules, regulations, and acceptable use guidelines implemented by the DHHS division or program area that owns or holds the license of the software application.

42.8 Open source software

Open source software has source code available with a license where the copyright holder provides the rights to study, change or distribute the software.

42.8.1 Serve a valid business purpose and provide functionality not available through existing or proprietary software owned, operated, and maintained by the Agency.

42.8.2 be approved for use by the agency;

42.8.3 be thoroughly tested prior to implementation

42.8.4 be configured and maintained in accordance with all applicable state and federal guidance

THIS PAGE INTENTIONALLY LEFT BLANK

Section 11 - IT Contingency Planning

43.0 INTRODUCTION

DHHS is charged with the protection of federal, state, and client data in accordance with applicable regulatory guidance, as well as business agreements and local policies. Part of applying appropriate security controls to protect that information includes ensuring contingency planning is developed and tested regularly. The Agency must be able to ensure IT resources can be efficiently and effectively restored, and data can be recovered with little to no loss.

In accordance with Nebraska Revised Statute §84-712.05, paragraph 8, any contingency planning information or documentation containing network configuration information may NOT be released to the public.

44.0 SCOPE AND APPLICABILITY

44.1 Contingency planning is a necessary component prioritize and restore DHHS IT resources used, and identify and prioritize based on the dependencies with other State of Nebraska Agencies or third-party vendors. Contingency planning must be considered in all phases of system development life cycles for the design, development, implementation, operation and maintenance of IT resources, placing a higher priority on mission critical systems and functions.

44.2 This standard applies to all DHHS staff responsible for contingency, business resumption and disaster recovery planning and coordination.

45.0 ROLES AND RESPONSIBILITIES

45.1 Agency CEO/COO/CIO

45.1.1 Provide oversight and guidance to division directors and business units for continuing operations.

45.1.2 Provide input and coordinate reasonable and appropriate prioritization to support affected locations.

45.1.3 Ensures open communication with affected business units and State of Nebraska agencies to ensure seamless restoration of Agency IT infrastructure and data

45.2 Agency CIO

45.2.1 Receives clear IT resource priority requirement guidance from Agency division senior leadership and communicates those IT resource priorities.

45.2.2 Relays agency IT staffing requirements to Human Resources to ensure mission critical staff are identified and that appropriate staffing levels are available at affected locations to manage workload.

45.3 IS&T

45.3.1 Maintains the Agency Technical Services Business Resumption Plan.

45.3.2 Maintains agency-owned networked resources (servers, workstations, other infrastructure, applications, security, etc.).

45.3.3 Coordinates restoration of Agency IT resources for affected organizations based on priorities coordinated with division directors/department heads

45.3.4 Coordinates with OCIO to ensure the State of Nebraska network infrastructure and Agency-specific applications and data stored on servers maintained by OCIO are available, accessible and secure.

45.3.5 Coordinates with business units to ensure IT resources are accessible and usable.

46.0 IT BC/DR PLAN

46.1 A Business Continuity/Disaster Recovery (BC/DR) plan must be developed and maintained to support the restoration of the IT infrastructure to its baseline configuration and recovery of lost/missing data to the latest known good state.

46.1.1 This is an integral part of and directly supports the Agency's master Continuity of Operations (COOP) plan to support the agency's business units.

46.1.2 The plan must also address interagency dependencies, which may rely on support from other State of Nebraska agencies (such as OCIO).

46.2 Given the unpredictable nature of events, the BC/DR plan must be scalable and flexible to meet the Agency's needs.

46.3 Ensuring the BC/DR plan can be effectively implemented is dependent on the Agency as a whole, and requires several key components:

46.3.1 Identifying the mission-essential functions required to provide services.

46.3.2 Test, Train, Exercise – How frequently does is the plan or portions of the plan tested? For divisions that routinely do real-world restoration of services (such as IS&T), the processes, as well as lessons learned should be well documented.

46.3.3 Ensuring sufficient and position-appropriate personnel are available to conduct restoration/recovery of resources or continuation of services.

46.3.4 Orders of Succession creates a chain of command to identify the individual(s) authorized and capable of acting on behalf of their respective division should key leaders be unavailable.

46.3.5 Open communication channels ensure recall procedures can be readily executed to bring in necessary staff at the required time; and provides a conduit from workers to management for status reporting.

46.3.6 Identification of secondary/tertiary alternate facilities and required resources should the primary locations be unavailable.

46.3.7 Identify the location of essential records to begin restoration/recovery processes.

46.3.8 Devolution of control identifies an entity, either internal or external to the agency who will be able to work on behalf of the primary staff should primary staff be unavailable to perform functions associated with their division. External staff must be knowledgeable of Agency functions.

46.3.9 The ability to restore full information system functionality.

46.4 Dependencies are functions within any division of the agency that require an action or service by either: another division within the agency; another state agency (such as DAS or OCIO); or an external service provider (e.g., power, telephone, internet connectivity, etc.). The following examples of dependencies are not all-inclusive, but paint a rudimentary picture of what is required to ensure resources are functional and available.

46.4.1 Operations must work with the Department of Administrative Services (DAS) to coordinate and obtain the use of facilities and basic services (physical security, power, telephone, cable and internet services).

46.4.2 IS&T coordination with OCIO is required to ensure systems and network infrastructure are functional and accessible, proper security controls are in place to protect resources, Agency-specific data is segregated from other State of Nebraska agencies, and there is minimal risk of cross-contamination or inadvertent disclosure of data.

46.4.3 The DHHS divisions need reasonable assurance from IS&T and OCIO that applications and electronic data used on a daily basis are available, accessible, usable and secure.

46.4.4 Business units must coordinate with third-party entities to assess operational impact of the third party entities' ability to access or process data on behalf of DHHS

46.5 Identification of priorities – DHHS Senior Leadership and the DHHS divisions must communicate service restoration priorities with IS&T to help ensure access to critical applications is achieved and maintained. Service restoration and business resumption priorities are ultimately determined by senior leadership; but how DHHS prioritizes restoration of key resources depends on:

46.5.1 The location and severity of the disaster (which facilities or geographic area of the state are affected?).

46.5.2 The resources required to meet the short or long-term demands to ensure continuation of services such as:

46.5.2.1 Network infrastructure and connectivity;

46.5.2.2 Voice Communications;

46.5.2.3 Computer software and applications; and,

46.5.2.4 File and print services

46.5.3 Clients impacted by the disaster (whose information is needed, when is the information needed, and how is the information accessed?).

46.5.4 Staffing

46.5.4.1 Ensure mission critical personnel are immediately available or can be recalled as required by the situation

46.5.4.2 Ensure support staff can be recalled to resume business functions when resources become available

46.5.5 Any other resources required to continue operations, to include temporary workarounds

47.0 TEST AND EXERCISE.

47.1 Business continuity and disaster recovery plans must be tested at least annually to ensure the existing plan is viable, flexible, and sustainable.

47.1.1 Use NIST 800-84 Guide to Test, Training and Exercise Programs for IT Plans and Capabilities as a guide to develop IT-related exercises.

47.2 Exercising the plan is a coordinated effort: the area of the plan to be tested must be coordinated with the involved agencies/divisions/ business units to ensure the correct individuals (decision makers) are available to collaborate reasonable and appropriate responses in accordance with Federal, State and Agency guidance.

47.3 After Action (lessons learned) reporting is necessary to identify strengths and weaknesses with the Agency's plans. Use lessons learned to adjust the plan, closing any gaps that may exist and ensure the lessons learned are addressed in future exercises.

THIS PAGE INTENTIONALLY LEFT BLANK

HISTORY OF CHANGES

Document	Version	Description	Author(s)	Author Date	Signature Date
DHHS IS&T Security Policy	1.0	New	Cindy Bloom	01/18/2024	

48.0 ACRONYMS AND DEFINITIONS

DHHS Information Technology (IT) Acronyms and Definitions

Attachment 1: List of Abbreviations and Definitions

Abbreviations	Description
DHHS	Nebraska Department of Health and Human Services
DCS	Document Control System
POL	Policy
ACA	Affordable Care Act
AD	Active Directory
BA	Business Associate
BAA	Business Associate Agreement
BH	(NE DHHS Division of) Behavioral Health
CAP	Corrective Action Plan
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
CFS	(NE DHHS Division of) Children and Family Services
CHARTS	Children Have a Right To Support (Application)
CIO	NE DHHS Chief Information Officer
CMS	Center for Medicaid Service
COO	(NE DHHS) Chief Operations Officer
COTS	Commercial Off-the Shelf
DDD	(NE DHHS Division of) Developmental Disabilities
DHHS	(Nebraska) Department of Health and Human Services
DHS	Department of Homeland Security (Federal Agency)
DIFSLA	Disclosure of Information to Federal, State, and Local Agencies
DMZ	Demilitarized Zone
DOTComm	Douglas Omaha Technology Commission
ePHI	Electronic Protected Health Information
FAQ	Frequently Asked Questions
FISMA	Federal Information Security Management Act of 2002
FTI	Federal Tax Information
GLBA	Gramm-Leach-Bliley Act
HHS	Health and Human Services (Federal Agency)
HIPAA	Health Insurance Portability and Availability Act of 1996
IP	Internet Protocol
IRC	Internal Revenue Code
IRS	Internal Revenue Service
IS&T	(NE DHHS) Information Systems and Technology
(A) (S) ISO	(Agency) or (State) Information Security Office(r)
ISRA	Information System Risk Assessment
IT	Information Technology
LAN	Local Area Network
MAN	Metropolitan Area Network
MARS-E	Minimum Acceptable Risk Safeguards for Exchanges
MFD	Multi-function Device
MLTC	(NE DHHS Division of) Medicaid and Long-Term Care
MMIS	Medicare and Medicaid Information System
MOA (U)	Memorandum of Agreement (Understanding)
NE-EES	Nebraska Eligibility and Enrollment Solution
N-FOCUS	Nebraska Family Online Collaborative User System
NIST	National Institute of Standards and Technology
NTRAC	Nebraska Timely, Responsive, Accurate, Customer Service
OCIO	Nebraska Office of the Chief Information Officer

PH	(NE DHHS Division of) Public Health
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POAM (or POA&M)	Plans of Action and Milestones
RACF	Resource Access Control Facility
SCSEM	(Internal Revenue Service) Safeguard Computer Security Evaluation Matrix
SLA	Service Level Agreement
SLDC	System Development Lifecycle
SSA	Social Security Administration
SSP	System Security Plan
SSR	Security Safeguard Review
TIGTA	Treasury Inspector General for Tax Administration
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
Terms	**Definitions**
Authentication	The process to establish and prove the validity of a claimed identity.
Authorization	The granting of access based on an authenticated identity.
Availability	A fundamental security objective that information and information systems are accessible, functional, and usable by authorized individuals when required, and not conversely, not usable for unauthorized individuals.
Biometrics	The use of electro-mechanical devices that measure physical (e.g., fingerprint), electrical, or audio (e.g., voice recognition) characteristics of an individual to verify identity.
Breach	Any illegal penetration, unauthorized access to a computer system or data, or unauthorized disclosure of information that causes damage or has the potential to cause damage.
Chain of Custody	Tracking method to ensure protection by responsible parties to ensure against loss, breakage, alteration, or unauthorized handling of evidence. Protection also includes properly securing, identifying, and dating evidence.
Change Management	A business process required by the agency to ensure no changes occur on a computing resource without prior coordination, approval and testing to ensure any modification to a system will perform as expected.
Classification	The security designation given to information from a defined category based on its sensitivity and criticality.
Confidentiality	The fundamental security objective to endure information is adequately protected and may only be disclosed only to those systems or persons that are intended to received that information.

Controls	Security countermeasures or safeguards implemented to ensure systems comply with appropriate Federal, State and Local guidance. DHHS uses NIST SP800-53 as guidance to implement controls.
Data	Any information created, stored (in temporary or permanent form), filed, produced or reproduced, including all records as defined by the Records Management Act. Data may include, but is not limited to personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, or communications. Data may be presented in either electronic (digital) or hard copy (paper) format.
Data Security	The protection of information and assets from unauthorized disclosure, modification, or destruction.
Decryption	The transformation of data to a readable format using an approved cryptographic key (see Encryption).
Demilitarized Zone	Also called a perimeter network. A physical or logical subnetwork that contains and exposes an organization's external facing services to a larger untrusted network. It is a "buffer zone" between the internal network firewalls and the internet.
Denial of Service	An attack designed to consume or overload resources, resulting in performance degradation or loss of access to business services or resources.
Disaster	A natural or manmade occurrence of sufficient duration that causes significant disruption in the accomplishment of the DHHS business objectives.
Encryption	The transformation of data to render it unintelligible through an algorithmic process using an approved cryptographic key.
External Network	The expanded use and logical connection of various local and wide area networks beyond their traditional Internet configuration that uses the standard Internet protocol, TCP/IP, to communicate and conduct E-commerce functions.
Federal Tax Information	Any information received from the Internal Revenue Service pertaining to an individual's Federal Income Tax return. The IRS requires DHHS to implement safeguards to protect FTI.
Firewall	A security mechanism that creates a logical barrier between internal and external networks.
Gramm-Leach-Bliley Act	Federal regulation requiring privacy standards and controls on personal information for financial institutions. For additional information visit `https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-acth`
Health Insurance Portability and Accountability Act	The 1996 Congressional act that addresses the security and privacy of health data. For additional information visit `https://www.hhs.gov/hipaa/index.html/h`
Incident	Any adverse event that threatens the confidentiality, integrity or availability of information resources.
Incident Response	An organized approach to addressing and managing a security breach or attack.

Incident Response Team	A group of formally assigned personnel within an agency trained, chartered, and equipped to respond to identified information technology incidents.
Information	The representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.
Information Assets	All categories of automated information, including, but not limited to records, files, databases, information technology facilities, equipment, and software owned or leased by Nebraska DHHS.
Information Security	The concepts, techniques and measures used to ensure the confidentiality, integrity, availability, and auditability of Nebraska DHHS information assets.
Information System	A system or application that consists of computer hardware, software, networking equipment, and any data. Such systems include but are not limited to desktop computers, servers, printers, telephones, network infrastructure, email, applications and web based services.
Information Technology	Computing and telecommunications systems and their supporting infrastructure and interconnectivity used to acquire, transport, process, analyze, store, and disseminate information electronically.
Insider Threat	A threat to an organization coming from the people within that organization (such as current or former employees, contractors or business associates) who have information concerning an organization's security practices (see Trusted Insider).
Integrity	The fundamental security objective that assures information is reliable and accurate. The foundation of integrity is ensuring that information can only be accessed or modified by authorized individuals.
Internal Network	A non-public network that uses the same technology and protocols as the Internet.
Internet	The global system of interconnected computer networks that use the internet protocol suite (TCP/IP) to link devices worldwide. It consists of private, public academic, business and government networks from local to global in scope.
Internet Protocol	A packet-based protocol for delivering data across networks.
IT Resources	Hardware, software, content, and communications equipment, including, but not limited to: computers, mainframes, wide and local area networks, servers, peripheral equipment, telephones, wireless communications, video conferences, facsimile machines, technology facilities including but not limited to, data centers, dedicated training facilities, and switching facilities, and other relevant hardware and software items as well as personnel tasked with the planning, implementation, and support.

Local Area Network	A data communications system that (a) lies within a limited spatial area; (b) has a specific user group; (c) has a specific topology; and (d) is not a public switched telecommunications network, but may be connected to one. (See MAN, VLAN, WAN and WLAN).
Malicious Code (Malware)	Software code written to intentionally carry out harmful actions or use up computer resources. Malware may be disguised as useful software or embedded into emails so that users are enticed into activating them. Types of malicious code include Trojan horses, computer viruses, and ransomware.
Metropolitan Area Network	An interconnection of LANs over a citywide geographical area.
Personally Identifiable Information	Any piece of information that can be used individually or with other sources to identify, contact, or locate a single person. PII may include, but is not limited to: addresses, telephone numbers, birth or anniversary dates, mother's maiden name, etc.
Physical Security	The protection of information processing equipment and facilities from damage, destruction, theft or unauthorized access. Physical security includes protecting personnel from potentially harmful situations.
Policy	Approved and ratified DHHS document or series of documents that establish a set of consistent rules and controls necessary to achieve the business objectives for an organization in a secured and compliant manner.
Principle of Least Privilege	The framework that requires users be given no more access privileges to information systems than necessary to perform their normal job functions, and those privileges are granted for no longer than the time required to perform authorized tasks.
Privacy	The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.
Privileged Account	An account assigned to specific individuals whose job responsibilities require additional permissions to perform high-level functions, such as a network administrator, security administrator, database administrator, etc.
Protected Health Information	Any information about a person's health status, provision of healthcare, or payment for healthcare services that can be linked to a specific individual. Electronic PHI (ePHI) is that data stored in digital format.
Ransomware	Malware installed on a computer system, that when activated, encrypts files on the system and requires the end user to pay a fee (ransom) to obtain the key to unlock the files.
Recovery	Defined processes within an incident response plan with the goal of returning affected systems to normal operations.
Risk	The probability of suffering harm or loss based on existing threats and vulnerabilities.

Risk Assessment	The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.
Risk Management	The process of taking actions to assess and reduce risks to acceptable levels, and the ongoing oversight to ensure appropriate attention is given to the highest priority risks.
Security Incident	Any electronic, physical, natural, or social activity that threatens the confidentiality, integrity, or availability of State of Nebraska DHHS information systems, or any action in violation of the DHHS Information Security Policy. For Example: • Any potential violation of Federal or State law, or DHHS policies involving State of Nebraska information systems. • A breach, attempted breach, or other unauthorized access to any State of Nebraska DHHS information system originating from inside the State network or an outside entity. • Malware of any kind, malicious use of system resources, or similar destructive files or services. • Actions or attempts to use, alter, or degrade an information system owned or operated by the State of Nebraska in a manner inconsistent with DHHS policies.
Staff	Any State of Nebraska DHHS full time, part time, and temporary employees; third party contractors and consultants who operate as employees, volunteers and other agency workers.
Standard	A Set of rules for implementing policy. Standards define specific technologies, methodologies, implementation procedures and other detailed factors. Certain exceptions and conditions may appear in the published standard, all other deviations require prior approval.
System Development Life Cycle	A “cradle to grave” development process that includes defining system requirements, design specifications, hardware or software development, installation and training, maintenance, decommissioning and disposal.
Third Party	Any non-agency contractor, vendor, consultant, or external entity.
Threat	A force, organization, or person seeking to gain access to or compromise information or information systems. Threats can be assessed in terms of the probability of an attack. By examining the nature of the threat, its capability and resources, the level of threat can be assessed and the likelihood of occurrence can be determined.
Transmission Control Protocol / Internet Protocol	A protocol for communications between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols.
Trojan Horse	Illegal code hidden in a legitimate program that when executed performs some unauthorized activity or function.

Trusted Insider	An individual within an organization who uses authorized access to knowingly and willfully circumvent existing security safeguards to exploit a network, resources, or clients.
Virtual Local Area Network	A group of hosts with a common set of requirements that communicate as if they were attached to the same wire, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows end stations to be logically grouped together even if they are not physically located on the same LAN segment. Network reconfiguration can be done through software instead of physically relocating devices.
Virtual Private Network	A communications network tunneled through another network, and dedicated for a specific network. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features. A VPN may have best-effort performance, or may have a defined Service Level Agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point. The distinguishing characteristic of VPNs are not security or performance, but that they overlay other network(s) to provide a certain functionality that is meaningful to a user community.
Virus	A program that replicates itself on computer systems by incorporating itself into other programs shared among computer systems. Once in the new host, a virus may damage data in the host's memory, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs.
Vulnerability	A weakness of a system or facility that can be exploited to gain access or violate system integrity and availability. Vulnerabilities can be assessed in terms of the means by which an attack would be successful.
Vulnerability Scanning	The portion of security testing in which evaluators attempt to identify weaknesses to discover if persons may exploit the weaknesses to gain unauthorized or elevated privilege access to otherwise protected resources.
Web Application	An application accessible by using a web browser over a network such as the Internet or intranet.
Wide Area Network	A physical or logical network that provides data communications to a larger number of independent users than are usually served by a local area network (LAN) and is usually spread over a larger geographic area than that of a LAN.
Wireless Local Area Network	The linking of two or more computers by using radio waves to enable communication between devices in a limited area.
Worm	A program similar to a virus that can consume large quantities of network bandwidth and spread from one network to another.