DHHS Information Technology (IT) Access Control Standard

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

Number: DHHS-2013-001-B

1.0 Purpose and Objectives

With the diversity of services, geographic spread of the various business departments, and variety of contractual relationships required to fulfill the mission of the Nebraska Department of Health and Human Services (DHHS), safeguards must be implemented to not only meet State and Federal security and privacy regulations but to also ensure a secure computing environment that meets these unique business requirements for DHHS.

It is DHHS policy to provide the minimum necessary access for Staff to perform their assigned duties, and nothing more. Securing and protecting DHHS IT resources is a critical responsibility of every individual with access to DHHS IT resources.

This standard establishes guidelines for creation of Unique User Identification (also referred to as Log-on ID), Strong Password access controls, access assignments limited to minimum necessary based upon assigned job duties, the protection of these access controls, and requirements for remote access to the DHHS network environment.

2.0 Scope and Applicability

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

The standard applies to all access into the DHHS network or any system owned, leased, or supported by DHHS that stores protected DHHS information.

2.1 Enforcement

Log-on ID and Password audits may be used by Information Systems & Technology (IS&T) periodically to monitor appropriate use of IT resources and ensure they meet the guidelines set in this standard.

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

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

3.0 Unique User Identification Standard

The Unique User Identification Standard provides guidelines for compliance to DHHS-2013-001 *DHHS IT Security Policy*. Security safeguards covered under this standard apply to Unique User Identification and Password Management. It is the responsibility of Staff authorized to access DHHS IT resources to follow all access control standards to secure Log-on ID's, passwords, remote connectivity, and other access control safeguards as defined below. Creation, use, and maintenance of DHHS-assigned Unique User Identification and passwords must meet the requirements detailed in 3.1 Unique User Identification Standards.

The following requirements are minimum standards for DHHS IT resources. If a DHHS business area requires stricter standards, those requirements must be reviewed and approved by IS&T. It is the responsibility of the business areas to inform and train their staff regarding rules exceeding those defined in this standard.

3.1 Unique User Identification Standards

Unique User Identification (Log-on ID) is used to identify an individual, provide services, and levels of access to DHHS networks and applications. Some of the more common uses include LAN access, web accounts, email accounts, and role-based access levels to application functionality and information. Unique identifiers are used as safeguards to monitor and audit appropriate access and to protect an individual's access from unauthorized intrusion.

3.1.1 Log-on ID Standards

Every individual Staff member accessing a DHHS production IT Resource must have a unique Log-on ID assigned to them by IS&T. No generic or sharing of Log-on ID's is allowed on any system capable of making changes or updates to DHHS information resources or that can access confidential or highly restricted information. Using or sharing a Log-on ID not specifically assigned to the individual is a violation of this standard - unless there are additional levels of authentication or a mechanism to ensure individual accountability for information access.

1. The DHHS Customer Service Help Desk is responsible for implementing all access and security request to the DHHS information system.
2. A DHHS Security Administrator will be designated for each Division, Service Area, and local office location with authorization to request Staff security changes to DHHS Help Desk. Security requests include access for new Staff, Staff transfers, name changes, changes to existing security and Staff terminations.
3. The DHHS Supervisor is responsible for requesting access to DHHS IT resources on behalf of their assigned Staff. Access requests must be based upon minimum necessary criteria for the performance of assigned job activities and submitted to the DHHS Help Desk through a designated DHHS Security Administrator. Each request must include system, applications, and level of access being requested.
4. The DHHS Supervisor is responsible for ensuring that all Staff have been sufficiently trained in the appropriate use and management of all Log-on ID's assigned to them. All changes or terminations associated with the Staff assigned to the Log-on ID, must be reported through their Security Administrator immediately.
5. The DHHS Supervisor is responsible for reviewing access roles for each Staff member on an annual basis to determine if access roles are still commensurate with currently assigned job duties. All changes, transfers, or terminations associated with a Log-on ID must be reported through their Security Administrator immediately.
6. Special Log-on ID's requested to meet unique requirements, (e.g., mainframe batch job processing, system maintenance requirements, training ID's) must be approved by the DHHS Information Security Officer (ISO).
7. When special Log-on ID's are created, they must be assigned to a DHHS employee as the assigned owner who is directly responsible for and will be held accountable for any and all activity performed using the Log-on ID.
8. All special Log-on ID's must be terminated immediately when no longer needed.
9. Special Log-on ID's must be terminated or reassigned when the responsible DHHS employee terminates or transfers.
10. Any Log-on ID not used or inactive for:
    - 90 days - will be disabled and the owner will be required to reset the password before access is reset
    - a 13 month period - will be automatically deleted

3.1.2 Log-on ID Protection Standards

Your DHHS Logon and password are your keys to performing secure activity with the State of Nebraska. They should be considered as important as your signature. Do not share your Logon or password with anyone not authorized to know these credentials. It is the responsibility of the Log-on ID owner to protect the integrity of the Log-on ID assigned to them. Only authorized Security Administrators or DHHS Customer Service

Help Desk Security Administrators may assign or make changes to Log-on ID's. New accounts are required to be established by DHHS Customer Service Help Desk Security Administrators only. If you suspect an account or Log-on credentials have been compromised, report the incident to the DHHS Help Desk as soon as possible.

3.2 General Password Guidelines

Passwords are an important aspect of computer security and are the front line of protection for Log-on ID accounts. Passwords are used for various purposes at DHHS (e.g., LAN access, web accounts, email accounts, and user-level application access). Poorly chosen passwords may result in compromising the DHHS network. All Staff with access to DHHS systems are responsible for taking the appropriate steps, as outlined in this standard, to select and secure passwords. Password owners are responsible for any action or activity performed using their password. This standard establishes guidelines for creation of strong passwords, the protection of those passwords, and the frequency for changing passwords.

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 that run on the state mainframe computer utilizing mainframe security safeguards. The state mainframe safeguards are defined and managed by the Office of the Chief Information Officer (OCIO). The mainframe applications will employ the mainframe password standard listed in this document. All other DHHS IT resources and applications must meet the Network/Application password guidelines defined in this document.

3.2.1 Mainframe Passwords Guidelines:

1. Mainframe strong passwords are to consist of a minimum of six (6) and maximum of eight (8) characters in a combination of alpha, numeric, and special characters. The combination must consist of:
   - At least one alpha character (a-z)
   - At least one numeric value (0-9)
   - May include special characters (#$@)
2. Password must be changed at least every 90 days. Users may change passwords more frequently to further strengthen their security. The recommended Resource Access Control Facility (RACF) password change interval is every 31 days.
3. Passwords cannot be reused for 12 months.
4. Log-on ID accounts are automatically locked after three (3) consecutive unsuccessful password attempts.

3.2.2 Network/Application Password Standards:

1. Strong passwords are to consist of a minimum of eight (8) 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 (~!@#$%^&*()_+-=<>?;':\)
2. All system-level passwords (e.g., root, enable, application administration accounts, etc.) must be changed every 180 days.
3. All user-level passwords (e.g., email, LAN access, application access, web, desktop computer, etc.) must be changed at least every 90 days. Users may change passwords more frequently to further strengthen their security.
4. Passwords cannot be reused for 12 months.
5. Log-on ID accounts will be automatically locked after three (3) consecutive unsuccessful password attempts.

3.2.3 Password Protection Standards:

It is the responsibility of the password owner to protect the integrity of the password assigned to them. Password owners must comply with the following protection standards:

1. Do not use the same password for DHHS accounts you use for other non-DHHS accounts (e.g., personal ISP account, email, and benefits).
2. Where possible, don't use the same password for various DHHS access needs. For example, select one password for the LAN Access and a separate password for application access.
3. Do not share DHHS passwords with anyone **INCLUDING SUPERVISORS, administrative assistants, co-workers, or staff assistants**. All passwords are to be treated as **SENSITIVE, CONFIDENTIAL** DHHS information. Should supervisors or managers require access to a staff member account they must contact the DHHS Help Desk for assistance.
4. Do not reveal a password over the phone. The only exception would be to Help Desk staff or DHHS Support Staff working on a support issue initiated by you. Immediately after resolution of the incident, you must change the password shared with support staff.
5. Do not reveal a password in an unsecured email message.
6. Do not talk about a password in front of others.
7. Do not hint at the format of a password (e.g., "my family name").
8. Do not reveal a password on questionnaires or security forms.

9. Do not share a password with family members.
10. Do not reveal a password to co-workers while on vacation.
11. If anyone demands a password, refer him or her to this document or have them call the DHHS Help Desk.
12. Do not use the "Remember Password" feature of applications.
13. Do not write passwords down and store them anywhere in your office 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.
14. Change passwords as required by individual applications.
15. If you suspect an account or password has been compromised, immediately change the password and report the incident to the DHHS Help Desk as soon as possible.

3.2.4 Application Development Standards

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

1. Aligns with all DHHS standards and procedures, and does not degrade the security posture of the underlying infrastructure in which the application runs.
2. Aligns with the minimum password guidelines detailed in this document.
3. Supports authentication of individual users, not groups.
4. Does not store passwords in clear text or in any easily reversible form.
5. RACF passwords – Applications using RACF must meet the strongest password guidelines in force and supported by the OCIO.

4.0 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).

The Remote Access Standard defines requirements and procedures for connecting to the DHHS network from any host connected using the Internet. These standards do not apply to any DHHS web applications or systems designed for public access.

Remote access to the DHHS network containing Confidential or Highly Restricted information will only be permitted from DHHS-controlled, managed, or approved methods or arrangements that have been approved through the policy exception process.

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 are specifically approved by the DHHS CEO may sync to the state email system.

All remote access servers are required to be kept fully patched and managed by authorized DHHS IS&T administrators. Remote access servers are required to 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.

The DHHS ISO is responsible for:

1. Developing and disseminating information concerning recommended safeguards, and the potential security threats and concerns of remote access of DHHS automated information and systems;
2. Ensuring that all personnel are aware of this policy and incorporating it into remote access briefings and training programs;
3. Promptly notifying the CIO and IS&T Management of computer security incidents (or suspected incidents) resulting from remote access.
4. Assuring that information security notices and advisories are distributed to appropriate personnel and that vendor-issued security patches are installed on DHHS software expeditiously.

Supervisors and managers must ensure that:

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

4.1 Remote Access Standards and Requirements

1. The information system must automatically terminate any remote session after fifteen minutes of inactivity, where these systems contain PHI, PII or FTI.
2. DHHS IS&T will authorize, document, and monitor all remote access capabilities used on the system.

3. Multi-factor authentication is required for any remote access to Confidential or Highly Restricted data. Authentication will be controlled by centralized Key Management Centers/Security Management Centers with a backup at another location.
4. The ISO will provide training to assure that users are aware that the unauthorized or improper use of DHHS assets could result in loss of use or limitations on use of assets, disciplinary or adverse actions, criminal penalties, and/or employees being held financially liable for the cost of damages resulting from any unauthorized use.
5. Any security incident (identified as a known or suspected incident) must be reported within one hour of discovery as defined in DHHS-2013-001-E - *DHHS IT Incident Management Standard.*

4.2 Remote Access for DHHS Staff and Offices

The following standards apply to all DHHS Staff that connect to DHHS IT assets 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.

External access from a personally owned computer or a computer not owned or supported by DHHS may only access DHHS network resources via an IS&T authorized and configured remote access connection. Remote access for DHHS Staff must have prior authorization by and be requested by their Supervisor or Division Management. No DHHS classified information other than Public information may be stored on a personal device. These requirements do not apply to remote access to web applications or systems intended for public access.

1. Staff approved for remote connectivity using non-DHHS equipment are required to comply with all DHHS policies and standards, and are required to have approval from DHHS CEO or CIO. It is the responsibility of DHHS Staff with remote access privileges to the DHHS network to ensure that their remote access work environment is given the same security consideration as the user's on-site connection to Nebraska DHHS. All personal devices connecting to the network must have up to date anti-virus protection, active firewalls, and appropriate security patch levels equivalent to those provided for DHHS equipment. All users shall be subject to random inspection by IS&T or the ISO 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.
2. Staff shall use DHHS provided equipment and software for authorized activities only. Employees are prohibited from using such equipment for private or inappropriate purposes as defined in DHHS-2013-002 *DHHS IT Acceptable Use Policy.*

3. DHHS IS&T shall maintain a log of all remote access sessions. IS&T shall perform periodic monitoring of the remote access session and random inspection of the user security settings and protocols to ensure compliance with policy and standards.

4. All information systems that are remotely accessible and contain Confidential or Highly Restricted data must employ mechanisms to ensure Personally Identifiable Information (PII), Protected Health Information (PHI), or other sensitive information cannot be downloaded or remotely stored.

5. All DHHS owned or managed portable devices that have the ability to store Confidential or Highly Restricted information must be password protected and encrypted using approved technology. Encryption technology will be provided or approved by IS&T and must be FIPS 140-2 compliant.

6. Remote users may only connect to the DHHS network using an IS&T authorized remote access connection.

7. Remote users must use access control credentials that are managed and controlled by DHHS IS&T when accessing Highly Restricted or Confidential information.

8. Remote sessions that access Confidential or Highly Restricted information or systems, must use an approved form of multi-factor authentication before connecting to the DHHS network.

9. Remote sessions must employ IS&T approved cryptography during the entire session when connected to the DHHS network.

10. Staff with remote access privileges to the DHHS network must only use their assigned State @nebraska.gov email account to conduct Nebraska DHHS business. Use of personal email accounts such as Hotmail, Yahoo, Gmail or other external resources to conduct official business will be considered an unauthorized disclosure and may result in a disciplinary action.

11. Remote access logon failures shall be logged. Credentials shall be disabled after three (3) failures.

12. Remote sessions shall be locked after 15 minutes of inactivity and remain terminated until the user re-establishes access with the appropriate credentials and authentication procedures.

13. At no time should any Nebraska DHHS employee provide their login or email password to anyone, not even family members.

14. Nebraska DHHS Staff with remote access privileges must ensure that their DHHS-owned or personal computer or workstation, which is 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.

15. Never leave a laptop visible in a vehicle.

16. Immediately report any lost or stolen hardware used to access DHHS resources to the DHHS Help Desk.

4.3 Remote Access Standards for External Partners

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.

1. External Partners are required to have a DHHS Sponsor who will verify the needs of the External Partner and serve as the contact point with the External Access Committee and IS&T. External Partner access levels must be reviewed on an annual basis. Approved External Partner applications are valid for three years or until their contract with DHHS expires (whichever comes first).
2. It is the responsibility of DHHS External Partners with remote access privileges to the DHHS network to ensure that their remote access connection complies with DHHS Security Policy, with particular attention to the protection of PHI and PII.
3. External Partners who require connectivity must 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 to be employed to maintain the security of the DHHS information system and receive the approval before the connection will be allowed.
4. External Partners who access the DHHS network are required to have security contract language included in their contract that provides for the appropriate protection of confidentiality, integrity, and availability of DHHS information commensurate with DHHS policies and standards.
5. DHHS ISO shall perform a periodic review of the External Partners security settings and protocols to ensure compliance with the contract arrangement or DHHS policy and standards.
6. Encryption technology must be FIPS 140-2 compliant.
7. External Partners must use access control credentials that are managed and controlled by DHHS IS&T.
8. Remote sessions that access Highly Restricted or Confidential information or systems must use an approved form of multi-factor authentication before connecting to the DHHS network.
9. External Partners must use their organizations authorized email system when conducting business on behalf of DHSS. All email communication containing DHHS protected information must be through the State Of Nebraska's secure mail tool or a secure email system approved by IS&T. Use of personal email accounts such as

Hotmail, Yahoo, Gmail, or other external resources to conduct Nebraska DHHS business is prohibited, thereby ensuring that official business is never confused with personal business.

10. External Partners with remote access privileges must ensure that when remotely connected to the DHHS network; they may not be connected to any other network at the same time. Split-tunneling is not permitted at any time while remotely connected to the DHHS network.
11. The DHHS ISO may require a risk assessment be performed for any vendors or contractors who require remote access to Confidential or Highly Restricted information. If a risk assessment is required, it must be completed before the vendor or contractor is allowed connectivity to DHHS systems.

5.0 Privileged Account Management Standards

Privileged accounts include administrator accounts, embedded accounts used by one system to connect to another, 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 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 would be locked out of every system.

Due to the elevated access levels these accounts typically have, DHHS requires the following standards and procedures to be followed in order to minimize the risk of incidents caused by these accounts.

1. All privileged access accounts are required to be assigned to an individual or system. Accounts may not be shared, and the assigned individual or system owner shall be held accountable for the actions conducted by the privileged account. As such, privileged account owners should exercise extra diligence in securing these credentials.
2. Privileged access accounts are required to be in compliance with all standards for password strength and expiration – ANY exceptions must be explicitly approved by the DHHS ISO and documented.
3. IT staff are authenticated prior to requesting, approving or gaining access to a privileged account. This ensures accountability for changes they may make using that account.
4. Login sessions to connect to privileged accounts are recorded and certain data is logged as defined in the DHHS IT Audit Standard *DHHS-2013-001-F.*

5. The password change process should support recovery of managed systems from backup media. Very old passwords should remain accessible in a history table in the event that they are needed to activate a backup copy of a system.
6. Logging of privileged access activity is required. Privileged access logging shall take 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 *DHHS-2013-001-F.*
7. Privileged access requests shall follow the normal access request process but shall have an additional approval authority level - from either the DHHS CIO, IS&T Management, or the DHHS ISO.
8. Privileged access accounts shall be assigned in a manner that maintains a separation of duty from audit and compliance functions (e.g., audit reviews cannot be performed by the same personnel who administer access credentials).
9. All activity performed by privileged accounts must be performed using access that requires identification and authorization. No anonymous activity by privileged accounts is permitted.
10. Remote access for privileged functions shall be permitted only for compelling operational needs, shall be strictly controlled, and must be explicitly authorized in writing by the DHHS CIO or his/her designated representative.
11. The DHHS CIO is required to approve any changes or exceptions to the privileged account management infrastructure, operations, or procedures.

6.0 Revision History

Legal Review – 09-16-2013
Policy Approved – 09-30-2013

Signature:

Eric Henrichsen Date: 9/30/2013

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