ADH INFORMATION SYSTEMS PASSWORD REQUIREMENTS POLICY

Purpose/Scope

This policy establishes the requirements for creating strong passwords and protecting user credentials (username and password) in ways that help safeguard ADH information systems against cyber-attacks. These requirements comply with federal and state laws and industry regulations.

This policy applies to all ADH users and non-ADH users who have been granted access to any ADH information system.

Definitions

Access: Upon the presentation of authenticated credentials, permission to use ADH information systems.

ADH User: A person, ADH employee, who has been granted access to any ADH information system and is accountable for the security of such access.

ADH Information Systems: ADH network services (Internet, Intranet, e-mail, etc.); ADH applications (client-server, web-based, mainframe, etc.); or any third-party software legally acquired and installed on the ADH devices for which it was intended. It also includes any computer file, on any device in use by ADH or its agents, that is shared across the ADH network or requires ADH support, or that contains ADH-related information, the privacy of which must be safeguarded.

Authentication: The automated comparison of presented user credentials with credentials on record for access to ADH information systems.

Credentials: Consists of the combination of a user's username and password.

Non-ADH User: A person, not an ADH employee, who has been granted access to any ADH information system and is accountable for the security of such access.

Person: One whose identity has been validated and whose association with ADH has been certified by the Center/work unit requesting access credentials.

System Administrator: Person designated by ADH's Chief Information Officer to provide technical support and access management for ADH information systems.

See the Information Systems Security Access Policy for related security requirements and a complete list of definition of terms.

Policy

Safeguarding of Credentials

Private or mission-critical information stored and processed on computer systems must be protected against unauthorized modification, disclosure, or destruction. Before access is granted to ADH information systems, users must enter their assigned, unique personal identifier (username) and a valid password to authenticate the user. The following requirements are designed to safeguard credentials and prevent unauthorized access to ADH information systems.

Requirements

ADH information systems password construction must conform to the following standards:

A. Network Passwords

1. Must be at least fourteen (14) characters in length.
2. Must contain one (1) character from each of the following four (4) categories:
   a. upper case characters (example: A, C, J, Z)
   b. lowercase characters (example: a, b, x, z)
   c. numeric characters (example: 0,1, 3, 9)
   d. non-alphabetic characters (example: !, $, #, *). Spaces are also considered non-alphabetic characters.
3. May not be the same as any previous twenty-four (24) passwords.

B. Password Selection: Users must select strong passwords composed of a collection of random characters, following construction rules outlined above, rather than passwords that may easily be guessed. Logical names and words, even in combination with a leading or trailing number, are weak passwords. Names spelled backwards, names of celebrities, well-known landmarks, popular culture icons, family names, etc., should be avoided in passwords.

C. Password Life Cycle: Passwords will expire in 60 days or may be changed sooner by the user. Users will receive system prompts in advance of

expiration advising users to select a new password. Users may not reuse any of their last twenty-four (24) passwords. A password should be changed if a user suspects its security has been compromised.

D. Physical Security: Sharing credentials is strictly forbidden. Writing down credentials (username and password) is discouraged but, if written, the following rules should be observed:

1. Never openly post user credentials, particularly near the user's PC.
2. Store written recording of credentials in a secure location.
3. Do not identify the recording as a password.
4. Store the username in a different place than the password.
5. Mix in false characters or scramble the password recording in a manner the user will remember, so the written version is different from the real password.
6. Never record a password online or include a password in an e-mail message.

E. Security of System Infrastructure

1. Non-Technical Requirements**:** To maintain the security of ADH information systems, user access may be granted only after authentication of credentials. Credentials are uniquely assigned to a person and may not be generically ascribed to groups or agents unless explicitly approved by ADH's Chief Information Officer.
2. Technical Requirements: Technical requirements follow the Microsoft regimen.

Disciplinary Action for Violation of Policy

Supervisors should refer to the Employee Disciplinary Policy – Minimum Conduct and Performance in the ADH Human Resources Policy Manual to determine the appropriate disciplinary action for violations of this policy.

Procedures

A. To Obtain User ID and Password for E-mail

Responsibility	Action
Employee's supervisor	Contacts Center personnel coordinator to make request
Employee's supervisor/ personnel coordinator	Prepares ADH Systems Security Access Request (ADH-359) and submits online to ITS Help Desk
ITS Help Desk	Informs personnel coordinator of new ID and password within five working days of receipt of request
Personnel coordinator	Informs employee of new ID and password
Employee	Changes password at least every 60 days

Note: Role-based access to specific data files or work unit application programs is assigned on an individual basis. (See Data and Systems Security Classification and Access policy to determine level.)

B. To Alter or Delete User ID and Password

Responsibility	Action
Employee's supervisor	Immediately informs personnel coordinator of employee's change of status (moving or termination)
Employee's supervisor/ personnel coordinator	Prepares ADH Systems Security Request (ADH-359) and submits online to ITS Help Desk
ITS Help Desk	Denies access to specified user ID on effective date

Please contact the ITS Help Desk for questions about creating or deleting user access, creating strong passwords, safeguarding credentials, or provisions of this policy. ADH.HELPDESK@arkansas.gov; 501-280-4357 or 800-441-9232