5002.0.0 DHS INFORMATION SYSTEMS PASSWORD REQUIREMENTS

5002.0.1 This policy states the requirements for creating, securely storing and retrieving access credentials (User Names and Passwords) for all DHS Information Systems. In order to access DHS Information Systems or application, users must authenticate identity by presenting acceptable credentials. Access privileges protected by user credentials can be compromised if the credentials are improperly stored or inadequately safeguarded.

5002.0.2 See DHS Policy 5001, Information Systems Security Access, for related security requirements and a complete definition of terms.

5002.0.3 This policy applies to DHS Users, non-DHS Users, and Systems Administrators in all DHS divisions.

5002.1.0 Definitions

5002.1.1 DHS User: A person, DHS employee, who has been granted access to any DHS information system and is accountable for the security of such access.

5002.1.2 Non-DHS User: A person, not a DHS employee, who has been granted access to any DHS information system and is accountable for the security of such access.

5002.1.3 Access: Upon the presentation of authenticated credentials, permission to use DHS Information Systems.

5002.1.4 Authentication: The automated comparison of presented user credentials with credentials on record for access to DHS Information Systems.

5002.1.5 Credentials: Consists of the combination of a user's User Name (or similar user identifier) and Password.

5002.1.6 DHS Information Systems: DHS Network services (Network access, Email, Internet, etc.), DHS applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the DHS devices for which it was intended. Also includes any computer file, on any device in use by DHS or its agents, that is shared across the DHS network or requires DHS support, or that contains DHS-related information, the privacy of which must be safeguarded.

5002.1.7 System Administrator: Persons designated by DHS's Chief Information Officer to provide technical support and access management for DHS Information Systems.

5002.1.8 Person: A uniquely identifiable and distinguishable human being. A Person is one whose identity has been validated and whose association with DHS has been certified by the division requesting access credentials.

5002.2.0 Safeguarding of Credentials

Private or mission-critical information stored and processed on computer systems must be protected against unauthorized modification, disclosure, or destruction. Users are assigned a unique personal identifier which must be authenticated in conjunction with a valid password before access is granted to DHS Information Systems. Measures must be employed by Users to safeguard credentials with respect to both physical security and access to DHS Information Systems. The structuring of passwords will meet or exceed prevailing state government standards for strong passwords.

5002.3.0 Requirements

DHS Information Systems password construction will conform to the following standards. Password construction standards are also posted on DHS Gold at:
http://dhsgold/Passwords.htm

A. Network Passwords:

1. Must be at least eight (8) characters in length.
2. Must contain at least one (1) of each of the following: (1) Upper case alpha characters; (2) Lower case alpha characters; and (3) Numeric characters (1 through 9).
3. Should contain one or more "special" characters (e.g., @,#,$,%,&,*,=).
4. May not be the same as any previous 5 passwords.

B. Mainframe Passwords:

1. Must be at least eight (8) characters in length.
2. Must contain at least one (1) of each of the following: (1) Upper case alpha characters; (2) Lower case alpha characters.
3. Must contain at least one "special" character (e.g., @,#,$,%,&,*,=).
4. May not be the same as any previous 4 passwords.

C. Password Selection: Users must make a good faith effort to select strong passwords composed of a collection of random characters, following construction rules outlined above, rather than weak 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.

D. Password Life Cycle: All NT or Active Directory based passwords will expire in 60 day, or earlier if changed by user. All Mainframe based passwords will expire in 90 days, or earlier if changed by user. Users will receive system prompts, in advance of expiration, warning users to select a new password. Users may not reuse any of their last five passwords for DHS Network access, and may not reuse any of their last four

passwords for Mainframe access. A password should be changed if a user suspects its security has been compromised.

E. Physical Security: Sharing of credentials is strictly forbidden. Written recording of credentials is discouraged but if recorded, the following rules should be observed:

1. Never openly post User Credentials, particularly in proximity to the user's PC;
2. Store recording of credentials in a secure location;
3. Do not identify the recording as a password;
4. Do not include User Name with password;
5. Mix in false characters or scramble the password recording in a manner you will remember so the written version is different from the real password.
6. Never record a password on-line or include a password in an email message.

F. Security of System Infrastructure

1. Non-Technical Requirements**:** In order to maintain the security of DHS Information Systems, user access may be granted only after authentication through the presentation of acceptable credentials. Credentials are uniquely assigned to a Person and may not be generically ascribed to groups or agents unless explicitly approved by DHS's Chief Information Officer.
2. Technical Requirements: Technical requirements are contained in separate documents not associated with this policy.

5002.4.0 Disciplinary Action for Violation of Policy

Supervisors should refer to DHS Policy 1084, Employee Discipline, to determine the appropriate disciplinary action for violations of this policy.

5002.5.0 Originating Section/Department Contact

Office of Systems and Technology
1st Floor Donaghey Plaza North
P.O. Box 1437, Slot N101
Little Rock, AR 72203-1437
Telephone: 682-0032