



District of Columbia Department of Health		<b>PROCEDURE 720.50</b> <b>Implementing Office:</b> Chief Information Technology Officer <b>Training Required:</b> No <b>Originally Issued:</b> 12/18/13 <b>Revised/Reviewed:</b> <b>Effective Date:</b> 1/13/14 <b>Valid Through Date:</b>
<h1>Password Management Policy</h1>		
Approved by:  _____ Agency Director	Review by Legal Counsel:  _____	

I. Authority	Reorganization Plan No. 4 of 1996; Mayor's Order 1997-42; DC Official Code §1-1401
II. Reason for the Policy	To provide guidance to DOH, employees and contractors concerning the proper use and management of password-based user authentication for DOH computer networks and systems. This policy defines the roles and responsibilities for the proper use and protection of passwords and password-based authentication systems.
III. Applicability	This policy applies to all DOH employees, contracted staff, volunteers, interns, summer youth employees, and all users of District government Information Technology (IT) resources.
IV. Policy Statement	This policy defines the roles and responsibilities for the proper use and protection of passwords and password-based authentication systems. DOH reserves the right to review Internet use by DOH employees at any time to determine compliance with this and related policies. Any authorized user who violates this policy may be subject to suspension of service and shall be subject to disciplinary action, up to and including termination.
V. Definitions	<p>Expired Password- A password that must be changed by the user before login can be completed. Each password will be set to expire within 180 days, unless administered within a system that processes sensitive information.</p> <p>General Support System- An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).</p>

	<p>Null Password- Password space comprised of blanks.</p> <p>Password- A character string used to authenticate an identity. Knowledge of the password in association with a unique User ID will be minimum proof of authorization to access systems, resources, and capabilities associated with that User ID.</p> <p>Password System- A subsystem of the operating system manages user accounts, confirms user authentication, and enables system access according to policy. Assurance of unequivocal identification is based on the user's ability to enter a private password that no one else knows.</p> <p>User ID- A unique character string assigned to a user and used by an IT system to uniquely identify each user. The security provided by a password system will not rely on secrecy of the user's ID.</p>
<p><b>VI. Contents</b></p>	<ol style="list-style-type: none"> <li>1. Introduction</li> <li>2. Principles</li> <li>3. Potential for Password Compromise</li> <li>4. Password Management Requirements</li> <li>5. Minimum Password Standards for General Support Systems</li> <li>6. Minimum Password Standards for Systems that Process Sensitive Information</li> <li>7. Expired Passwords</li> <li>8. Change Authorization</li> <li>9. Change Procedures</li> <li>10. Remembering Passwords</li> <li>11. Privileged Accounts</li> <li>12. Transmission</li> <li>13. One Time Passwords</li> <li>14. Audit Trails</li> <li>15. Notice to the User</li> <li>16. Disciplinary Action for Violations</li> <li>17. Roles and Responsibilities</li> <li>18. Agency System/Network Administrator Responsibility</li> <li>19. End User Responsibility</li> </ol>
<p><b>VII. Procedures</b></p>	<p>Introduction:</p> <p>A major requirement of IT systems security is accountability. Individual accountability is the key to securing and controlling systems that process information on behalf of individuals or groups. The use of individual user identification, user accounts, or User IDs with passwords is</p>

mandatory for DOH computers. The use of shared user logins or accounts that can be accessed by more than one person is prohibited on DOH.

Principles:

A. User responsibility:

This policy defines the roles and responsibilities for the proper use and protection of passwords and password-based authentication systems. The major standards established in this document are the following:

1. Passwords shall be treated as highly sensitive data.
2. Users shall not share user-ids or passwords under any circumstances.
3. First time passwords shall be generated by security personnel, rather than created by the user.
4. External password records must not be maintained by the user, system administration, or security personnel.
5. Users can change their own passwords without system administration or security personnel intervention.
6. Password construction, management practices, and procedures will comply with these standards and requirements.
7. Audit information will be captured by the system to reflect password usage and management.
8. For the purposes of this policy, sensitive information is defined as data containing financial, personal, or protected health information for which unauthorized access or disclosure may either result in violation of District of Columbia or Federal regulation or otherwise be detrimental to DC Government operations. Sensitive information is to be designated by the information owner in accordance with applicable District of Columbia government or federal information classification standards.
9. Password management on systems that process sensitive information, and passwords on all highly-privileged accounts such as Windows Administrator, UNIX Root and others is required to be much more stringent than general user passwords.

B. Potential for Password Compromise

A password is susceptible to compromise when it is first

generated (in conjunction with the initial User ID to form the user account) or while being used, changed, entered into the system, transmitted over the network or stored. Further, the repeated use of passwords as they age increases the likelihood that they may be cracked. Any credible password security system depends on passwords being kept secret. Password-based authentication mechanisms (password subsystems) are also vulnerable to compromise due to the following types of malicious activity:

1. Password guessing using a dictionary attack or attributes known about the user
2. Social engineering, e.g., manipulating a user to obtain a password
3. Interception during password transmission

All DC Department of Health password management systems will be implemented so as to minimize exposure to these threats of password compromise.

#### C. Password Management Requirements

Each computer network or application hosted on DOH equipment or containing information owned by the DOH is required to implement a password authentication and management system. The sole class of exceptions to this requirement is systems that are designed to be accessed by the public; and within this class of systems, those that do not store, process, or transmit any form of sensitive information.

All password systems will be configured by the appropriate system owner or administrator to implement the following security controls:

1. Password Management. Each password system shall be configured to automatically enforce minimum password standards such as password length, composition, and required password change interval.
2. Accountability. Each password system shall identify each instance of authorized access because systems that process sensitive information must guarantee user accountability.
3. Personal Identification. Each password system shall assure identification of each individual user.
4. Authentication. Each password system shall confirm

	<p>the user's claimed identity.</p> <ol style="list-style-type: none"> <li>5. Password Integrity and Confidentiality. Each password system shall protect the password database at a level equal to the protection given sensitive information throughout the District.</li> <li>6. Auditing. Each password shall be configured to record basic information about user accesses.</li> <li>7. Use of Passwords to Protect Data. Where it is practical, DOH IT resources and applications must implement access control in operating systems, security subsystems and applications, such as database management systems to control access to data. All stored passwords will be encrypted using an approved encryption method.</li> </ol> <p>D. Minimum Password Standards for General Support Systems (GSS)</p> <p>General Support Systems include DOH computing assets that do not process, store, or transmit sensitive information as previously defined in this policy:</p> <ol style="list-style-type: none"> <li>1. Length. All passwords shall be a minimum of 8 characters in length.</li> <li>2. Composition. All passwords shall include at least one numeric character (not the first or last character of the password) so as to defeat dictionary-based password cracking tools. GSS passwords will not be case-sensitive.</li> <li>3. Password Life. All GSS will require users to change their passwords every 180 days.</li> <li>4. Password History. All systems will utilize password history automation so that users cannot re-enter previously used passwords when required to change passwords.</li> </ol> <p>E. Minimum Password Standards for Systems that Process Sensitive Information and for all system accounts (including GSS computers) that have Administrator or Root-level privileges</p> <ol style="list-style-type: none"> <li>1. Length. All passwords will be a minimum of 8 characters in length.</li> <li>2. Composition. All passwords will include at least one numeric character (not the first or last character of the password), as least one UPPERCASE character, and at least one special character: ~ ! @ # \$ % ^ * ( )</li> </ol>
--	--

	<p>_ - + = { } [ ]   : ; " , ? . Do not use &lt; &gt; &amp; or '.</p> <ol style="list-style-type: none"> <li>3. Password Life. All non-GSS systems and highly privileged accounts will require users to change their passwords a minimum of every 90 days. System administration account passwords on critical public safety-related servers or workstations must be changed every 30 days.</li> <li>4. Password History. All systems will utilize password history automation so that users cannot re-enter previously used passwords when required to change passwords.</li> </ol> <p>F. Expired Passwords</p> <p>A password will be invalidated at the end of its maximum lifetime (such as ninety days, or less). The user will be notified by the system a minimum of seven days prior to password expiration. A user who logs in with an ID whose password is set to expire within seven days will be prompted to change their password. If a password is not changed before the end of its maximum lifetime, the system must "lock" the account. No login will be permitted to a locked user ID; however, the security administrator will be able to unlock the user ID by changing the password and invoking the procedure for account creation and requiring the user to change the password on the next login. After a password has been changed, the lifetime period for the password will be reset to the standard; which is one hundred eighty days, or less on specially designated sensitive systems.</p> <p>G. Change Authorization</p> <p>Users are authorized to change their personal passwords without Help Desk assistance.</p> <p>H. Change Procedure</p> <p>Password changes will be done at the user's discretion prior to expiration or when a user logs in with an expired password. If the change is necessary due to an expired password, the user will be so informed. The on-screen prompts will lead the user through the change process. Except when the change procedure is part of the login procedure (e.g., logging in with an expired password), the user's current password will be entered to re-authenticate identity. The change procedure will disallow password reuse. The user will then enter the</p>
--	--

	<p>new password twice to verify correct entry and selection. The new password shall not be echoed in clear text to the display.</p> <p>I. Remembering Passwords Users will memorize their passwords and will not write them on any medium. It will be considered a violation of this policy if a password is recorded externally.</p> <p>J. Privileged Accounts  Privileged user accounts (Windows Administrator, UNIX Root and others) must utilize passwords that are unique for each system accessed. Technical and privileged users will not use the same passwords on all systems under their management. The potential adverse impact is great if the common password is compromised.</p> <p>K. Transmission During transmission, passwords will be protected (encrypted).</p> <p>L. One-Time Passwords Systems that enforce one-time use of a password will be installed where practical. Passwords changed after each use are helpful when the password is not adequately protected from compromise, e.g., during login for dial-in access.</p> <p>M. Audit Trails Login events shall be appropriately logged and audited.</p> <p>N. Notification to the User In order for the user to determine if someone else is using or attempting use their user ID and password, the system will capture and provide the following information at the time of successful login:</p> <ol style="list-style-type: none"><li>1. The date and time of user's last login</li><li>2. Source of last login</li><li>3. Other relevant and appropriate messages about the user account</li></ol> <p>O. Disciplinary Action for Violations</p>
--	---

	<p>A violation of any standards or procedures established in support of the Password Management Policy shall be brought to the attention of agency director for appropriate action and could result in the termination of computer, network, or system access assigned to the user. Users who illegally access District of Columbia or Federal computer systems or data may be subject to criminal prosecution under computer crime laws.</p> <p>P. Roles and Responsibilities</p> <p>Agency Heads are responsible for the Internet activities of their users and for the implementation and enforcement of the policy. Each agency must ensure that District government-provided Internet services are used for legitimate DOH functions and purposes. DOH may add restrictions and guidelines regarding the use of the Internet by their users, based on specific business requirements and mission.</p> <p>DOH reserves the right to review Internet use by DOH employees at any time to determine compliance with this and related policies. Use of DOH IT resources constitutes express consent to monitor those resources. DOH will normally block an offending user account for a period of time to be determined by DOH and will refer violations of policy to the affected agency Director for further corrective action. DOH also reserves the right to block access to specific external Internet sites whose content is deemed inappropriate (e.g., obscene content, communications that encourage hate or violence, access to gambling) and inconsistent with DOH government functions and may reflect unfavorably on the District government image.</p> <p>Q. Agency System/Network Administrator Responsibilities</p> <ol style="list-style-type: none"> <li>1. Delete initial vendor system passwords</li> <li>2. Assign initial user passwords (at least 6 alphanumeric characters)</li> <li>3. Safeguard against password exposure</li> <li>4. Limit the number of login attempts (3 attempts)</li> <li>5. Counter password compromise or exposure threats</li> <li>6. Classify password databases</li> <li>7. Force password change (upon initial logon and at least every one hundred eighty days thereafter, if not more frequently)</li> <li>8. Revalidate users and privileges (at least every one</li> </ol>
--	--



	<p>hundred eighty days)</p> <ol style="list-style-type: none"> <li>9. Expired account validation</li> <li>10. Provide agency-related computer security training</li> <li>11. Ensure users are kept up to date with changes to this policy</li> </ol> <p>R. End User Responsibility</p> <ol style="list-style-type: none"> <li>1. Change his or her password immediately if compromise is suspected</li> <li>2. Report the suspected compromise to his or her supervisor</li> <li>3. Comply with this policy</li> </ol>
<b>VIII. Contacts</b>	Chief Information Technology Officer- (202) 442-4805
<b>IX. Related Documents, Forms and Tools</b>	N/A