CITY OF HOUSTON

Administrative Procedure

Subject: **Password Policy**	A.P. No: **8-4**
	Effective Date: **March 9, 2012**

1. AUTHORITY

1.1 Article VI, Section 7a, City Charter of the City of Houston.

2. PURPOSE

2.1 To strengthen security protocols that govern information systems by ensuring due diligence is satisfied with regards to safeguarding access to City information caches.

3. OBJECTIVE

3.1 To establish a policy and standards for creation of strong passwords, the protection of those passwords and the frequency of change. This policy identifies the minimum security requirements for all City information systems including networks, applications, data stores, and any other electronic resource to which access is granted by use of a password.

4. SCOPE

4.1 This policy applies to all users who have or are responsible for an account (or any form of access) that supports or requires a password on any application or system managed by or on behalf of the City.

5. DEFINITIONS

Legacy Technology – A legacy system is old technology, computer system, or application program that continues to be used, typically because it still functions for the users' needs, even though newer technology or more efficient methods of performing a task are now available.

6. POLICY

6.1 System Configuration Requirements - Information systems, such as applications and operating systems, must be configured to meet the equivalent of these guidelines:

6.1.1 Password history enforcement – Passwords cannot be reused for a minimum of six password change periods.

6.1.2 Maximum password age – Users must change their passwords at least every ninety days.

6.1.3 Minimum password length – Passwords must be a minimum length of eight characters.

6.1.4 Password complexity – Passwords must be strong, and easy to remember. They must contain a combination of at least three of the following:

6.1.4.1 Uppercase letters (A-Z);

6.1.4.2 Lowercase letters (a-z);

6.1.4.3 Numbers (0-9); and

6.1.4.4 Special characters (!, $, &, @, etc.).

6.1.5 Using passphrases are recommended for strong passwords. For example: Th3We@ther1sh0tinM@y (The weather is hot in May).

6.1.6 Password restrictions – Passwords must never contain:

6.1.6.1 Username;

6.1.6.2 Personal information. For example: Family names, pet names, social security number, or date of birth;

6.1.6.3 Repetitive letter or number patterns. For example: aabbcc, 123456; or

6.1.6.4 Common words or slang.

6.1.7 Maximum failed log-in attempts – Systems should allow five failed password logon attempts before system lockout. Users must contact the Information Technology Department (ITD) Customer Support Center (CSC) or, if applicable, your departmental Information Technology (IT) support group to reset your password.

6.2 Password Protection – All passwords:

6.2.1 Must be treated as sensitive and confidential and not shared with anyone including managers, co-workers, outside contractors, or family members;

6.2.2 Must not be used by anyone other than the account owner; and

6.2.3 Must never be written down, stored online, in documents, or anywhere in an office or on any computer system that is unprotected and/or unencrypted.

6.3 Suspected Password Compromise – Users who suspect their account or password has been compromised shall:

6.3.1 Report the incident to the ITD CSC or, if applicable, the departmental IT support group.

6.3.2 The ITD CSC or, if applicable, departmental IT support group must reset the compromised password immediately.

6.4 New and Reset Passwords - All new or reset passwords must be:

6.4.1 Provided by an IT support group or ITD CSC password administrator to the City employee verbally after verifying the individual's identity. An IT support group or ITD CSC password administrator must never write passwords down or send them over unencrypted e-mail;

6.4.2 Unique for each user;

6.4.3 Changed by the City employee after using the new or reset password to login; and

6.4.4 Forced by the system to prompt the user to change their password after initial login if the system possesses that capability.

6.5 The City IT Compliance team may conduct periodic audits to evaluate compliance with the requirements set forth in this policy. The City reserves the right to monitor systems, electronic communications, and usage to ensure compliance.

7. EXCEPTIONS

7.1 Departments that are unable to follow any portion of this policy due to Legacy Technology use or valid business reasons must request an exception to policy and receive approval through the process established in Administrative Procedure 8-3, Managing Exceptions Process.

8. COMPLIANCE

8.1 Failure to adhere to all requirements stipulated in this policy and all related documents may result in disciplinary action, up to and including:

8.1.1 Immediate removal of any applicable hardware/software/access to the City's Network or systems;

8.1.2 Formally reporting the incident to the Human Resources Department and the Chief Information Officer (CIO);

8.1.3 Indefinite suspension or termination of employment; and/or

8.1.4 Any other action deemed necessary by senior management.