Information
Technology &
Telecommunications

The City of New York

CITYWIDE INFORMATION SECURITY POLICY

Password Policy

The Policy

All passwords and personal identification numbers (PINs) used to protect City of New York systems shall be appropriately configured, periodically changed, and issued for individual use.

Scope

This policy applies to all internal City of New York systems. Internal systems are those which reside directly on Citynet or on a City agency's internal network and are not Internet facing. DoITT approved VPN (virtual private network) and remote access are also considered internal. The password policy governing public accounts which are accessed via the internet is covered separately by the External Account Password Policy (TBD).

General Requirements

1) Passwords and PINs:
   - Must never be shared or displayed on screen.
   - Must be classified and handled as City of New York PRIVATE data.
   - Must be changed when there is any indication of system or password compromise.

2) A password-protected screen lock must be activated within fifteen minutes of user inactivity.

3) Passwords used by a person on City of New York systems should be different from any passwords used by the same person on non-City of New York systems (for example, on accounts used on social networking, ecommerce and other personal online sites). In the event that a personal (non-City) account password is compromised, this reduces the risk to City systems.

Encryption and Hashing

4) Passwords and PINs:
   - Must be encrypted when transmitted electronically with a protocol which is compliant with the Citywide Encryption Standard.
   - Must be encrypted or hashed when held in storage. When embedded in configuration files, source code or scripts, they must be either encrypted or secured with compensating controls which provide a comparable level of protection.

Password/PIN Changes

5) A user wishing to change his/her password/PIN must be positively identified by demonstrating knowledge of the current password/PIN or by other comparable methods.

Password/PIN Delivery

6) Passwords must be delivered securely to the recipient (authorized user) with an approved transmission method. Although passwords and PINS must never be shared, initial passwords may be delivered to the recipient's manager. In all cases, the recipient or manager must be positively identified before the password is delivered.

Account Lockout

7) All accounts which provide access to SENSITIVE, PRIVATE or CONFIDENTIAL information must be automatically disabled after a maximum of five (5) sequential invalid login attempts within a fifteen (15) minute period. After being disabled, the account must remain locked out for a minimum of fifteen (15) minutes.

Password/PIN Format, Length and Complexity

8) PINs may only be used where a numeric method for authentication is required, such as a telephone keypad. In all other cases, passwords or pass-phrases must be used for authentication.

9) Passwords and PINs must have a minimum length of eight (8) characters with the exception of voice mail systems, and Blackberry and PDA devices issued by the City which must use a password or PIN of at least 4 alphanumeric characters.

10) Passwords must be constructed using at least one alphabetic character and at least one character which is either numeric or a special character:

Passwords must contain:		Examples
At least one	Alphabetic character	Aa Bb Cc … Zz *(can be lower or upper case)*
and		
At least one	Numeric character	0 1 2 3 4 5 6 7 8 9
	or	
	Special character	{ } [ ] , . < > ; : ‘ “ ? / | \ ` ~ ! @ # $ % ^ & * ( ) _ - + =

11) Passwords must not be derived from easily guessed, common words or phrases such as those found in dictionaries (English and non-English), nor should they be constructed from user IDs, proper names or other names, words, numbers or dates readily associated with the individual user (e.g., telephone extension, Social Security number, or zip code).

Login Account Types

12) Three types of login accounts are defined in Citywide Information Security Policy:

User Accounts	Administrative Accounts	Service Accounts
Are for use by *Individuals,* often referred to as end-users.	Are also for use by *Individuals* but carry an elevated degree of privileges (e.g., root). They are intended for use solely by authorized IT personnel for performing such tasks as managing systems and User Accounts, and for performing password resets.	Are intended for use solely by automated processes for logging into systems to access resources or perform tasks.

Password/PIN Expiration and Re-use

13) Temporary or initial User Account passwords and PINs must be set to expire after initial use. Default passwords and PINs must be changed immediately upon the completion of the installation process and/or first login. If a user is *not* prompted to change a temporary or initial password or PIN, the account may have been inappropriately accessed and he/she should contact the Citywide Service Desk immediately.

14) Additional password/PIN expiration requirements and related guidelines and restrictions are provided in the following table for the three account types defined in point number 11.

User Accounts	Administrative Accounts	Service Accounts
User Account passwords and/or PINS must expire at least every **90** days.	Administrative Account passwords must expire at least every **90** days.	Service Account passwords must expire at least every **90** days.
		Must be known only by a limited number of staff on a need-to-know basis. The names of staff who know the password for any Service Account must be documented and the list of names/service accounts must be kept current.
	Administrative Accounts should be restricted to logging in from specified IP addresses.	Service Accounts must be restricted to logging in from specified IP addresses.
	When a staff member who knows an Administrative or Service Account password leaves the City or changes his/her job function, that password must be changed.	
Exceptions		
No exceptions	Administrative and Service accounts need not expire provided they meet the following requirements:	
	Administrative accounts must a) Use two-factor authentication AND b) Be either randomly generated or highly complex.	Service accounts must: a) Have a minimum length of 15 characters AND b) Be either randomly generated or highly complex.
	Where feasible, the use of password management software and/or certificate-based authentication is recommended as additional control for non-expiring Administrative and Service Accounts.	

15) Passwords and PINs must not be reused for four (4) iterations.

16) Agency security administrators shall have the ability to reset all passwords where proper authorization and audit trails are in place.

Policy Enforcement

17) Where possible, the system must automate the enforcement of these requirements. Where this is not possible, equivalent controls must be established through alternative methods or procedures. For example, as an alternative to enforcing password complexity, the administrator could periodically use tools to detect weak passwords and require users with weak passwords to change them.

18) Agencies may implement controls more stringent than those specified in this policy.

Document Revision History

Date	Description
May 5, 2010	Page 1, paragraph 2: Passwords and pins were incorrectly classified as CONFIDENTIAL. Changed to PRIVATE
June 16, 2011	**Version 1.4** Updated header with new NYC logo and added this revision history table to the document.
Aug 3, 2011	**Version 1.5** Major changes in document organization and formatting. New content added (bullets 11, 13 and 15).
November 29, 2012	**Version 1.6** Added the following text: *Passwords used by a person on City of New York systems should be different from any passwords used by the same person on non-City of New York systems (for example, on accounts used on social networking, ecommerce and other personal online sites). In the event that a personal (non-City) account password is compromised, this reduces the risk to City systems.*
Sept. 9, 2014	**Version 1.7** Policy review and minor formatting updates.