



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

Password Policy

The Policy

All passwords and Personal Identification Numbers (PINs) used to protect City of New York systems must be appropriately configured, periodically changed, and issued for individual use.

Password/PIN Usage and Confidentiality

- 1) Individual users must properly protect passwords and/or PINs for all accounts.
- 2) All passwords and/or PINs must be classified and handled as City of New York Confidential data.
- 3) Passwords and/or PINs unique to an individual must not be shared with other individual or user.
- 4) Passwords/PINs must not be displayed on the screen at any time.
- 5) Passwords and/or PINs must be changed whenever there is any indication of system or password compromise.
- 6) Any password or PIN management system either must avoid caching the password or PIN or must provide adequate protections and controls if such caching is essential.
- 7) Passwords and/or PINs must always be encrypted when held in storage or when transmitted across any network. Exception: One-time passwords or PINs, or hard-coded passwords or PINs
- 8) Use of a City of New York approved hashing algorithm is considered encryption for the purposes of password or PIN protection. Unencrypted passwords and/or PINs must never be embedded in sign-on utilities. For example, an unauthorized user must never be able to authenticate at sign-on merely by using a function key or by running an available program.
- 9) Unencrypted passwords and/or PINs must not be hard-coded in source code, command files, initialization files, scripts or installation kits.
- 10) PINs shall only be used where a numeric method for authentication is required (e.g., for entry on a telephone keypad); in all other instances, passwords should be used for authentication.
- 11) Administrative passwords must be adequately protected and restricted only to required individuals for system support.
- 12) Screen lock must be activated within fifteen (15) minutes of unattended inactivity.

Password/PIN Length

- 13) Passwords and/or PINs must have a minimum length of eight (8) characters. Exception: Voice mail systems, as well as Blackberry and PDA devices issued by the City must use a password or PIN of at least 4 alphanumeric characters.

Password Complexity

Issued: July 28, 2008 Final Version 1.1

Password Policy



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- 14) Passwords must be constructed using at least one alphabetic and at least one character which is numeric or a special character.

Class Description	Examples
1. Upper Case Letters	A B C ... Z
2. Lower Case	a b c ... z
3. Numerals	0 1 2 ... 9
4. Non-alphanumeric ("special characters", punctuation, symbols)	{ } [] , . < > ; : ' " ? / \ ` ~ ! @ # \$ % ^ & * () _ - + =

- 15) Passwords must not be derived from commonly used words or phrases.
- 16) Users should not select passwords consisting of easily guessed words, such as words found in dictionaries (English and non-English), User IDs, proper names or other names or words readily associated with the individual user, such as dates, nicknames and family names.
- 17) Users should not select passwords, or PINs, that contain personally identifiable numbers, such as the user's telephone extension, Social Security Number, or zip code.

Password/PIN Expiration

- 18) Passwords and/or PINs must be changed at least every ninety (90) days.
- 19) Temporary or initial passwords and/or PINs must be set to expire after initial use. The user must be required to change the password or PIN at the first use.
- 20) Administrative passwords must be changed every sixty (60) days, or when an individual who has knowledge of the password leaves their job function.

Disabling of Accounts

- 21) All accounts that provide access to sensitive, private or confidential Information must be automatically disabled after 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.

Default Passwords/PINs

- 22) Any default password or PIN must be changed during or immediately upon the completion of the installation process. The new password or PIN must conform to the requirements defined in this policy.
- 23) Default accounts must be renamed, if possible, to non-obvious names.

Password/PIN Reuse

- 24) User-chosen passwords and/or PINs must not be reused for four (4) iterations.

Password/PIN Changes



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- 25) Proper proof of identification must be provided before changing a password or PIN.
- 26) Users changing a password or PIN via a system command or screen must prove knowledge of the current password or PIN or be cryptographically authenticated before being allowed to change it.
- 27) The minimum time between user initiated password and/or PIN changes must be at least one (1) day. If a user has recently changed a password and is concerned that the new password may have been compromised, but is unable to immediately change it again in accordance with this provision, the user should contact an administrator of the system in which the password is used to request a password reset.
- 28) Users requesting a new password or PIN or requesting a password or PIN change/reset via a help desk or administrator must prove their identity before the change is initiated.

Password/PIN Delivery

- 29) Delivery of passwords and PINs to a user, either when an account is created or when an administrator resets a password/PIN, requires attention to ensure that delivery is done efficiently and with a regard to security. Passwords must not be transmitted over any City of New York voice, video or data network without appropriate identification and authentication.
- 30) A password must be delivered in a manner that requires the recipient to prove his/her identity before the password is received.

Policy Enforcement

- 31) Administrators are accountable for configuring systems to enforce this policy.
- 32) Where possible, the system must enforce these requirements. Where this is not possible, equivalent controls must be established through alternative methods or procedures. For example, to enforce password complexity, the administrator should run tools periodically to detect weak passwords, and require users with weak passwords to change their passwords.