External Identity Management and Password Policy

The Policy

All user accounts and passwords used to protect public facing City of New York systems which permit individuals or companies to manage their own data shall be appropriately configured and issued for individual use.

Scope

This policy applies to all public (Internet) facing City of New York systems which permit individuals or companies to manage their own data.

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 considered internal. The password policy for internal systems is covered separately by the Citywide Password Policy.

General Requirements

1) All internet (public) facing applications requiring authentication must leverage DoITT provided, centralized identity management services from NYC.ID and NYC.gov for user registration and authentication.
2) Public users must be able to utilize DoITT provided self-service mechanisms for password/credentials management.
3) Public facing accounts must be validated with a valid email address and each email address may only be associated with one account.
4) Passwords for public users need not expire.
5) Passwords:
   - Must never be shared or displayed on screen.
   - Must be classified and handled as City of New York PRIVATE data.

Encryption and Hashing

6) Passwords must be encrypted when transmitted electronically with a protocol which is compliant with the Citywide Encryption Standard.

Password Changes

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

Account Lockout and Monitoring

8) Consecutive failed login attempts within a *fifteen minute* period must be handled as follows:

   a) After five consecutive failed attempts, CAPTCHA or equivalent functionality must be invoked to verify that a person (and not an automated program) is attempting login.

   b) After eight consecutive failed attempts, the account must be permanently locked until the user successfully resets his/her password by either of the following self service methods:

      - Email based password reset via link provided or
      - User provides correct answers to pre-determined questions.

9) All Login attempts must be logged and monitored.

Password Format, Length and Complexity

10) Passwords must have a minimum length of eight (8) characters and 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) DoITT provided Password strength meter must be used during account provisioning dialogues.

Policy Enforcement

12) 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.

13) Agencies requiring higher levels of authentication may implement those processes within their applications.

Document Revision History

Date	Description
Nov 28, 2012	**Version 1.0** Initial publication
Sept. 9, 2014	**Version 1.1** Policy review and minor formatting updates.