


Policy Title:	Password Standards Policy		
	INFORMATION TECHNOLOGY SERVICES (ITS)	Category	Password Standards
		Administrative Policy #	
		Revision #	
		Review Frequency	As Needed – no less frequently than triennially
Administrative Division	Information Technology Services	Reviewed By	
BOWC Approval		Last Reviewed/Update Date	
Implementation Date			

1. OBJECTIVE

- 1.1. The objective of this document is to define the processes and standards to be used whenever a user or service requires a user ID and password on Active Directory (AD) or other systems and applications.

2. PURPOSE

- 2.1. The Detroit Water and Sewerage Department (“DWSD”) Password Standards Policy establishes the position that poor password management or construction imposes risks to the security of DWSD’s information systems and resources. Standards for construction and management of passwords greatly reduce these risks. The purpose of this document is to ensure that all AD IDs and passwords, along with general user IDs/passwords, meet DWSD’s security requirements to ensure a stable and secure network environment.

3. SCOPE

- 3.1. This policy applies to:
 - 3.1.1. All DWSD Information Technology Services (ITS) equipment, systems and applications which are capable of being password protected;
 - 3.1.2. All system developers and users (including DWSD staff, interns, contractors, sub-contractors and authorized third party commercial service providers) of the DWSD’s IT resources;
 - 3.1.3. All connections to (locally or remotely) the DWSD network Domains (LAN/WAN/WiFi);
 - 3.1.4. All connections made to external networks through the DWSD network.

4. RESPONSIBILITIES

4.1. Information Technology Services

- 4.1.1. The Chief Information Officer (CIO) is responsible for publishing this policy; communicating this policy to all employees; for review, approval and publishing of divisional standards; and for updating this policy as necessary.

4.2. Management

- 4.2.1. Management is responsible for monitoring work areas for compliance and addressing any incident(s) of noncompliance and alerting Human Resources when a violation has occurred.

4.3. Employees

- 4.3.1. The employee is responsible for being familiar with and fully complying with this policy, including taking the necessary actions to update passwords in a timely manner.

5. POLICY

5.1. Active Directory Domain ID/Password Requirements

- 5.1.1. The AD domain ID is developed according to the City of Detroit standards.
 - 5.1.1.1. AD password requirements:
 - 5.1.1.1.1. Passwords must be at least eight characters long.
 - 5.1.1.1.2. Require strong (complex) passwords (required to use combination of uppercase, lowercase, numbers and special characters)
 - 5.1.1.1.3. Passwords should be changed every 60 days
 - 5.1.1.1.4. Password history should be remembered so users cannot reuse recent (6) previous passwords.
 - 5.1.1.1.5. User accounts should lock after 3-5 failed login attempts.

5.2. Generic Application and Access ID/Password Requirements

- 5.2.1. This section pertains to vendor applications, applications hosted in the cloud, and other applications and/or systems that are not directly administered by DWSD staff.
 - 5.2.1.1. Generic application and access ID/password requirements:
 - 5.2.1.1.1. Each user must have a unique user ID; shared IDs are not permitted.
 - 5.2.1.1.2. Passwords must be at least eight characters long.
 - 5.2.1.1.3. Require strong (complex) passwords (required to use combination of uppercase, lowercase, numbers and special characters)
 - 5.2.1.1.4. Passwords should be changed every 90 days
 - 5.2.1.1.5. Lockout Policy: The application/system must have the capability of locking out the user after a specified number of failed logon attempts. The number of attempts to trigger a lockout will depend upon the application/system.

5.3. Password Storage, Transmission, and Documentation

- 5.3.1. Users must not share user accounts or passwords, and passwords must not be written down or stored/transmitted in electronic files or communications, unless originating from authorized ITS personnel and delivered through an encrypted email.