LUCAS COUNTY Information Services	Policy #:	Section: **Governance Policies and Standards**
	Date Issued: 5/6/2021	Name: **Password Management Policy**
	Date Revised:	Contact: **LCIS Director**

Password Management Policy

1.0 PURPOSE

- To establish password management practices which ensure the appropriate protection of Lucas County information assets and maintain accountability.

2.0 APPLICABILITY

- This policy is applicable to all Lucas County information assets, including applications and systems, organizations, agencies, departments, and Workforce Members.

3.0 DEFINITIONS

- 3.1: Active Directory
  A directory service from Microsoft Corporation that serves as the central authority for network security, providing Workforce Member Authentication and access control to network resources.

- 3.2: Administrative Resources
  Such as routers, switches, WAN links, firewalls, servers, internet connections, administrative-level network operating System Accounts, Active Directory and Directory Enterprise Administrative level accounts and any other information technology resources.

- 3.3: Authentication
  A security procedure designed to verify that the authorization credentials entered by a named Workforce Member to gain access to a network or System are valid.

- 3.4: Automated Logon Process
  Storing Authentication Credentials in a registry entry, macro, or function to automatically authenticate a User to a system without User intervention.

- 3.5: Information Asset
  A definable piece of information, information processing equipment, or an information system, that is recognized as “valuable” to the Organization that has one or more of the following characteristics:

1. Not easily replaced without cost, skill, time, resources, or a combination thereof,
2. Part of the Organization's identity, without which, the Organization may be threatened.

- 3.6: Organization
  Every Lucas County office, every officer, every institution, and every department, division, board, and commission.

- 3.7: Passphrase
  An exceptionally long password generally derived from a phrase or short sentence that typically eliminates spaces and replaces some letters with special characters; for example, "TheDark3stHourI$JustBeforeDawn"

- 3.8: System
  Software, hardware, and interface components that work together to perform a set of business functions.

- 3.9: System Account
  A specialized Workforce Member account, generally used by a server operating system to start a process for an application.

- 3.10: Multi-Factor Authentication
  A security process that confirms User identity using two or more distinctive factors – factors being something the user has (like a mobile phone) and something the user knows (like the name of their first pet or a six digit code texted to the Workforce Member). Risk of fraud and penetration into Lucas County assets is reduced by requiring multiple factor based electronic identification.

- 3.11: Workforce Members
  Employees, volunteers, interns, and other persons whose conduct, in the performance of work for Lucas County, is under the direct control of Lucas County, whether or not they are paid by Lucas County. This includes full and part-time elected or appointed officials, members of boards and commissions, employees, affiliates, associates, students, legal interns, volunteers, and staff from third party vendors, third party consultancies, and other entities who provide service to Lucas County.

4.0 POLICIES

- 4.1: Mandatory Use
  Workforce Members must use appropriate authentication credentials consisting of a login-ID and password to validate their identity when connected to Lucas County Information Assets. Each Workforce Member must be issued unique authentication credentials. Generic user accounts are prohibited; for example, "Intern1".

- 4.2: Storing Passwords
  Organizations shall require that any Authentication System that stores passwords must store them in an encrypted format. When developing and/or acquiring Systems or Application Software, Organizations shall not consider any solution that requires the storage of passwords within the System in an unencrypted format. All cloud based applications must offer multi-factor authentication.

- 4.3: Accountability
  Workforce Members are accountable for all activities performed under their authentication credentials unless an investigation proves that the Workforce Member did not violate this policy at the time of the incident requiring the investigation.

  - 4.3.1: Vendor Default Authentication Credentials:
    To ensure accountability and security, all newly installed systems will have vendor default authentication credentials removed, changed, or replaced.

- 4.4: Password Management

  - 4.4.1: Password Issuance

    - 4.4.1.1: Identity Authentication
      Organizations shall implement a procedure to authenticate the identity of the Workforce Members receiving a new or changed password.

    - 4.4.1.2: Forced Change
      Organizations shall implement a System procedure that forces the Workforce Members to choose a new password before the logon process is complete when the original temporary password is issued by a System Administrator at Lucas County Information Services.

  - 4.4.2: Sharing Passwords
    Workforce Members shall keep their passwords secret and shall not make their passwords known to anyone else, including elected officials, management, supervisors, personal assistants, proxies, human resources, and system administrators. Workforce Member passwords must not be shared under any circumstances.

- 4.4.3: Displaying Passwords
  Organizations shall implement policies that prevent passwords from being displayed openly.

- 4.4.4: Changing Passwords
  Whenever possible: Organizations shall implement System password Policies that automatically force the Workforce Members to change their password at least once every six months. Workforce Members must also change their password immediately after their password or Information Asset has been (or is suspected of being) compromised.

- 4.4.5: Password History
  Whenever possible, Organizations shall implement a system which prohibits the re-use of at least the last four passwords.

- 4.4.6: Failed Login Attempts
  When the technology allows, Organizations shall implement a process that after five (5) unsuccessful attempts to enter a password, the user account is disabled for at least thirty (30) minutes unless unlocked by a System Administrator at Lucas County Information Services.

- 4.4.7: Automated Logon
  Workforce Members shall not use passwords in any Automated Logon Process.

- 4.4.8: Password Composition
  Workforce Members shall use strong passwords and Organizations shall implement password Policies that require Workforce Members to choose strong passwords that are

  - 4.4.8.1: Password Length
    At least eight (8) characters in length

  - 4.4.8.2: Password Elements
    Contain at least three (3) of the following four (4) elements:
    1. English upper case letters: A,B,C…Z
    2. English lower case letters: a, b, c….z
    3. Westernized Arabic numbers: 1, 2, 3…9
    4. Special Characters: { } ! $ % & …

  - 4.4.8.3: Non-Compliant Passwords
    Organizations shall not allow or assign passwords that contain personal information, including but not limited to name (or part of a name), birth date, social security number, or employee number.

- 4.5: Administrative and/or System Account Password Management

- 4.5.1: Limit Password Access

    - 4.5.1.1: Need to Know
      Organizations shall limit access to administrative and System passwords to System Administrators who have a need to know.

    - 4.5.1.2: Storing System Passwords
      System Administrators who share an administrative or System password shall keep the password stored securely.

- 4.5.2: Changing System Administration Passwords
  System Administrators shall immediately change the password of their administrative or System accounts after the password or the administrative asset has been, or is suspected of being, compromised or when a System Administrator separates from employment or changes jobs within Lucas County. If the account is a System Account and a password change is not possible, the Organization shall perform a risk assessment and develop alternative security measures and provide a copy to the director of Lucas County Information Services.

- 4.6: Enterprise Level Training and Awareness
  Organizations shall provide Workforce Members annual training on this policy and their responsibilities for password management.

- 4.7: Compliance
  Organizations shall include this policy in the annual compliance review as specified by the State of Ohio.

5.0 RESPONSIBILITIES

- 5.1 Workforce Members comply with this policy, follow its guidelines, and understand the ramifications of all activities involving his/her Authentication Credentials.
- 5.2 System Administrators maintain the integrity of Workforce Members passwords and passwords for administrative resources, comply with this policy, and follow its guidelines.

- 5.3 Organizational Management advises System Administrators when a Workforce Member no longer needs access to a System (such as, upon termination or a job change), provide training to Workforce Members reinforcing good password management practices, and require compliance with this policy.