LUCAS COUNTY Information Services	Policy #:	Section: **Security**
	Date Issued: 1/10/2022	Name: **Password Management**
	Date Revised:	Contact: **Director, Lucas County Information Services**

Title: Password Management Policy

Policy Affected Agencies: Countywide

Keywords: Vulnerability, Password Management Policy, Vulnerabilities

Sponsoring Agency: Lucas County Information Services (LCIS)

Approved by the Data Processing Board 1/10/2022

I. Purpose:

The Data Processing Board recognizes the unique role and independence of the Judiciary under Ohio Law.

The purpose of this policy is to establish management practices which ensure the appropriate protection of Lucas County information assets and maintain accountability.

II. Applicability and Audience

A. Users

This policy applies to all persons working for, or on behalf of Lucas County, including workforce members, third parties, volunteers, and contractors accessing technology assets governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84). This policy applies to Guests of Lucas County, Tenants of Lucas County, and Non-County Agencies that attach to the Lucas County Network (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)). These requirements apply whether the workforce member is working within a Lucas County facility or connecting remotely.

B. Technology Assets

1. This policy applies to the use of all Lucas County technology assets including web or "cloud" based platforms, applications, and services that are owned and operated by a service provider on behalf of Lucas County (e.g Oracle Corporation).
2. This policy also applies to the use of third party or personal devices, if used to access Lucas County's technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) in the process of working for or on behalf of Lucas County.

III. Policies

A. Identity and Access Management Platforms (Governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84).

Lucas County Information Services (LCIS) is responsible for identity and access management platforms, directories, and tools utilized by Lucas County government (e.g. Active Directory, Azure AD, Active Directory Federation Services, Application Proxies, Microsoft Identity Management, Azure AD Privileged Identity Management, etc.) and for ensuring these systems comply with the Access Management Policy and Audit Logging and Monitoring Policy.

Lucas County Information Services will utilize and administer centralized identity platforms and will provide a single set of credentials to workforce members. Workforce members responsible for technology asset administration and support may receive a second set of credentials dedicated to those purposes

Lucas County Information Services will ensure that technology asset and support owners are provided appropriate rights to manage identities and/ or groups of identities in the centralized identity platform for which they are authorized to manage in accordance with the Access Management Policy.

County, employing Lucas County Information Services, is responsible for ensuring that identity, authentication, authorization, and access platforms and associated processes are indisputable and provide high confidence (i.e., validity cannot be challenged or denied) to the degree reasonably possible.

B. 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 (Governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84). Each Workforce Member must be issued unique authentication credentials. Generic user accounts are prohibited; for example, “Intern1”. (See also Kiosk and Shared Device Identification and Authentication)

C. Storing Passwords

Organizations shall require that any Authentication System that stores passwords must store them in a secured 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 unsecured format. All cloud based applications must offer multi-factor authentication.

D. 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.

E. Vendor Default Authentication Credentials

To ensure accountability and security, all newly installed systems will have vendor default authentication credentials removed, changed, or replaced.

F. Password Management / Password Issuance / Identity Authentication

Organizations shall implement a procedure to authenticate the identity of the Workforce Members receiving a new or changed password.

G. 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.

H. 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 unless required by authorized support personnel who, upon completion of support work, immediately advise the user on steps to establish a new password unknown to that support agentl.

I. Displaying Passwords

Organizations shall implement policies that prevent passwords from being displayed openly.

J. 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.

K. Password History

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

L. 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.

M. Automated Logon

Workforce Members shall not use passwords in any Automated Logon Process with exception of Kiosk and shared devise identification and authentication portion of this policy.

N. Kiosk and Shared Device Identification and Authentication

Accounts may be created to enable automated logins for kiosks or shared devices.
These accounts:

1. Must not have administrative rights.
2. Are not required to utilized multi-factor authentication
3. May utilize maximum password ages (e.g. a week, a month, a year)
4. Must utilize strict configuration and hardening tools to limit users of the device to authorized and intended interactions with the device configuration, software, and other functions.

O. Password Composition

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

1. Password Length at least eight (8) characters in length.
2. Password elements Contain at least three (3) of the following four (4) elements

   English upper case letters: A,B,C…Z
   English lower case letters: a, b, c….z
   Westernized Arabic numbers: 1, 2, 3…9
   Special Characters: { } ! $ % & …

P. 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.

Q. Administrative and/or System Account Password Management

Limit Password access / Need to know: Organizations shall limit access to administrative and System passwords to System Administrators who have a need to know.

R. Storing System Passwords

System Administrators who share an administrative or System password shall keep the password stored securely.

S. Changing System Administration Passwords

System Administrators shall immediately change the password of their administrative or System accounts after the password or the administrative asset (Governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) 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 Lucas County Data Processing Board.

T. Enterprise Level Training and Awareness

Organizations shall provide Workforce Members annual training on this policy and their responsibilities for password management.

IV. Implementation Plan

This policy becomes effective for countywide use on the date that it is approved by the Lucas County Data Processing Board.

A. Maintenance

This policy will be maintained by and approved by the Lucas County Data Processing Board. This includes, but may not be limited to:

1. Ensuring this policy content is kept current
2. Recommending updates to this policy and related resources
3. Developing an escalation and mitigation process if an Organization is not in compliance
4. Assisting Organizations to understand how to comply with this policy
5. Monitoring annual compliance by Organizations

This policy will be reviewed annually. A new, revised, or renewed policy will be initiated by the Director of Lucas County Information Services and approved by the Lucas County Data Processing Board, prior to the expiration date.

Agency or department Directors, elected officials, administrative judges, tenants and guests of Lucas County, non-county agencies that attach to the Lucas County network (Governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84), and the State of Ohio will be notified prior to the expiration date of the policy and will be notified by Lucas County Information Services of any proposed changes or new policies drafts allowing time for review and feedback.

B. Consequences for Noncompliance

1. Violations of this policy may be grounds for and result in a recommendation by the Lucas County Data Processing Board to the appropriate Appointing Authority for disciplinary action, up to and including termination and enforcement action which may include civil or criminal charges
2. If Lucas County Information Services determines that an employee should have network access halted due to noncompliance (password change, mandated training, etc.) Lucas County Information Services and the Elected Official/ Appointing Authority of that employee must sign off prior to any access shut off, to prevent any interruption to the entity's operation for any services or support.
3. At no time will Lucas County Information Services shut down an agency or department of Lucas County or any court