LUCAS COUNTY Information Services	Policy #:	Section: **Security**
	Date Issued:	Name: **Access Management Policy**
	Date Revised:	Contact: **Director, Lucas County Information Services**

Title: **Lucas County Access Management Policy**

Affected Agencies: **Countywide**

Keywords: **Access Management**

Approved by the Data Processing Board 4/7/2022

I. Purpose:

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

The purpose of this policy is to ensure Lucas County Data Processing Board provides secure and appropriate access to technology assets (e.g., hardware, software, data, and authentication information) (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)).

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 owned and operated by Lucas County (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)).

This policy applies to Guests of the County, Tenants of Lucas County, and non-County agencies/ offices that attach to the Lucas County Network (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)).

B. Technology Assets

This policy applies to all Lucas County technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)). This policy also applies to the use of third party or personal devices, if used to access Lucas County's technology assets in the process of working for or on behalf of Lucas County.

III. Definitions

All definitions are contained within the Lucas County Policies and Standards Glossary.

IV. Policy

Lucas County Data Processing Board shall provide each user (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) the minimum access to technology assets necessary to fulfill assigned duties or tasks. This is referred to as the principle of least privilege. Technology asset owners or their designees are responsible for ensuring that users of their assets have the appropriate levels of access.

A. Deny All by Default

All technology assets shall be configured to deny access by default. Access must be explicitly granted to users, liaisons, groups, roles, or technology systems, devices or services through a validation and approval process. This includes scenarios where the public is intended to have some level of access. The access should be configured with the minimum necessary privileges (e.g., Read Only, other privileges validated and explicitly granted)

B. Access Approval Requirements

1. The Lucas County Data Processing Board is responsible for providing an enterprise access request and approval process.

   This includes retention of access approval documentation for auditing by the State of Ohio Auditor, Lucas County Auditor, federal or state regulatory bodies, third party auditors.

2. Technology asset owners must approve access requests to their assets. Technology asset owners may delegate approval authority to an individual, role, or group.

3. Technology asset owners must ensure access levels are approved consistent with the principle of least privilege necessary for a workforce member to complete their work.

4. Technology assets must be configured to require multi-factor authentication prior to managing or modifying access privileges where possible.*

5. Access can be requested by and granted to individual users, groups, or roles in accordance with the least privilege principle. Technology asset owners are highly encouraged to utilize groups and roles to reduce the administrative overhead of access management.

6. Prior to granting access to technology assets, technology asset owners or their designee must:

   a. Determine whether a criminal background check is required to comply with local, state, or federal law. The technology asset owner is responsible for ensuring a criminal background check is conducted both initially and ongoing as required by applicable regulations.

   b. Determine whether specific security awareness training is required for the technology assets being accessed. The Lucas County Information Services is responsible for

providing a security awareness training platform capable of enabling technology asset owners and workforce members to meet these requirements however alternate training platforms may be used where necessary.

c. Determine whether any contractual or other legal requirements have been established for the technology asset which may require acknowledging those set of requirements by those being provided access (e.g., data sharing agreements, acknowledgement of security or privacy requirements, etc.)

C. Access Audit Requirements

1. Access to Lucas County technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) must be logged as required by the Audit Logging and Monitoring Policy.

D. Removal/Modification Requirements

1. In the event of workforce member termination (e.g., retirement, voluntary separation, involuntary separation) or job transfer within Lucas County, the workforce member's current supervisor or manager must open a ticket with the Lucas County Information Services helpdesk so that access may be modified accordingly.

2. All instances of a terminated workforce member's access, especially remote access, must be disabled as soon as possible. If a terminated workforce member will subsequently volunteer or perform a new role with Lucas County this should be considered a job transfer and access should be updated in accordance with the new role that will be performed.

3. Strictly limited access to payroll and benefits information may be granted to a terminated workforce member so long as that access cannot be used for any other Lucas County technology assets.

4. Processes that create, modify, or remove identities or account credentials must comply with the Lucas County Password Policy.

E. Multi-Factor Authentication

Multi-factor authentication must be used when available when accessing Lucas County's technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) in compliance with the Lucas County Password Policy.

F. Session Control and Lockout

1. Technology assets used for kiosk or display purposes may be configured to allow sessions of inactivity longer than 30 minutes if:

   a. Configured as a display only system for purposes of visualizing information within a secured area controlled by Lucas County such as a utility or emergency operations environment

b. Configured as a kiosk (i.e., completely limits interactions with the technology asset to a specific set of interactions and prevents administration or changes to configuration of any kind to non- administrators)

c. Required by use cases covered by the Americans with Disabilities Act

2. Identities and accounts used to access Lucas County technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) must be immediately, and if possible, automatically prevented from any further access (e.g., account lockout or disable, application specific account lockout mechanisms, token revocation):

   a. After five unsuccessful attempts to authenticate within a 30 minute time period

   b. If a potential security incident is suspected to be in progress due to security incident detection and response systems and tools, conditional access policies or security incidents reported by users.

   c. 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.

      At no time will Lucas County Information Services shut down an agency or department of Lucas County or any court.

G. Account Expiration and Inactive Accounts

1. Identities and accounts created as part of working for or on behalf of Lucas County must be automatically disabled through the use of an expiration date if an expiration date is known and technically possible (e.g. Lucas County Board of Election seasonal staff, volunteers, other time limited employment or vendor contracts).

2. Identities and accounts created as part of working for or on behalf of Lucas County with access to Lucas County technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) must be reviewed and automatically or manually disabled (i.e., prevented from being used but may still be retained) if not used for more than 90 days.

   a. Identities and accounts created and used for emergency operations only when an emergency or incident is declared or for associated emergency training exercises may be configured to remain enabled even if not used within 90 days so long as these accounts can only access technology assets used for the same emergency operations. (e.g. Lucas County Cyber Security Incident Response Team)

   b. Additional exceptions may be granted with the approval of the Lucas County Data Processing Board (ORC 307.84).

H. Vendor, Third Party, and Contractors

1. Identities and accounts assigned to vendors for maintenance purposes must only be activated as needed and have an automatic expiration period not to exceed 24 hours.

2. Accounts assigned to vendors or contractors for ongoing project based work must be unique and assigned to specific individuals and have automatic expiration not to exceed 180 days. Project teams are required to review and request a re-enablement of the expired accounts to ensure they are still necessary. These credentials may not be shared by more than one individual (i.e., a single account given to a vendor and used by all of the vendor's staff).

3. Technology asset owners that have requested identities and accounts assigned to vendors must notify the Lucas County Information Services or the technology support owner by opening a ticket at the helpdesk immediately upon contract termination so that the accounts can be disabled.

4. When contracting with outside vendors, agencies must include language in the contract stating that vendors must notify the data asset owner or their designee when individuals who have been provided accounts have been terminated.

5. All contractors, vendors, and third parties who will be provided access to Lucas County technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) must acknowledge receipt of and agree to comply with Lucas County's Acceptable Use Policy.

I. Administrator Accounts

1. Lucas County Information Services is responsible for defining and managing a process for administrator accounts that:

    a. Ensures these accounts are inventoried

    b. Confidentially validates the workforce member has met any background check requirements

    c. Receives approval from the technology asset owner for creation, modification, removal

    d. Generates an audit log and alert when created, modified, or deleted

2. Accounts used to administer information security platforms and tools (e.g., firewalls, endpoint detection and response, anti-virus, content filters, vulnerability scanners, forensics and penetration testing tools, dynamic and static code analysis, etc.) must be approved by the Lucas County Data Processing Board (ORC 307.84).

3. All non-console administrative access must be encrypted end to end using approved technologies such as Secure Socket Shell (SSH) or Transport Layer Security (TLS).

J. Emergency Access, Investigations, Public Records

1. The Lucas County Data Processing Board, in conjunction with the Elected Official/Appointing Authority/Data Asset Owner or upon order of the Court, may approve access to any

technology asset for emergency or investigative purposes in accordance with the Lucas County Incident Response Policy.

2. Lucas County legal representatives for the technology asset owner may be provided access as part of a legal process (e.g., discovery).

3. Department or agency records officers working for or on behalf of the technology asset owner may be provided access.

V. Implementation Plan

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

All new technology implementations and new material changes to existing technology implementations must ensure compliance with this policy as of the effective date. All other technology implementations must be brought into compliance within twelve months after the effective date.

VI. Maintenance

A. This policy will be maintained 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

B. This 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.

C. 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.

VII. Consequences for Noncompliance

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.

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.

At no time will Lucas County Information Services shut down an agency or department of Lucas County or any court.

VIII. Appendix A: References

This section provides references to key regulations and standards that apply to Lucas County. This section does not replace the authoritative source and is just a reference to assist with further research. Please use the Compliance Standard and Section No. to further research the entirety of the regulation, framework or standard from the authoritative source.

Compliance Standard	Section No.	Description
HIPAA	45 CFR 164 Subpart C	Security Standards for the Protection of Electronic Protected Health Information
	164.308(a)(3)(i)	Workforce Security
	164.308(a)(4)(i)	Information Access Management
	164.312(a)(1)	Access Control
CJIS Security Policy v5.9	5.5	Access Control