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

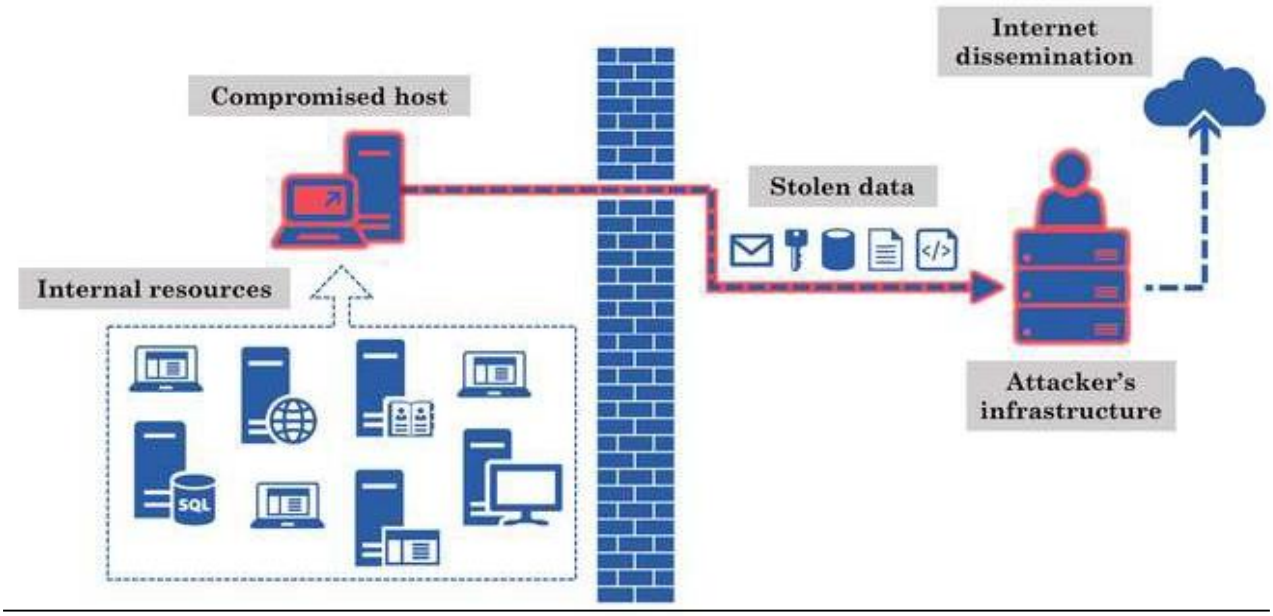
Title: **Lucas County Data Security Policy**

Affected Agencies: **Countywide**

Keywords: **Data, Open Data, Data Security, Data Governance**

Sponsoring Agency: **Lucas County Information Services**

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 security controls are in place to prevent data exfiltration, mitigate the effects of a data breach, and protect the confidentiality, integrity and availability of Lucas County's data assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)).

Control of Data

LCIS is a centralized and secure site for the storage and retention of electronic data. The data consists of various types of electronic information generated and owned by various offices. While this data is stored and secured by LCIS, neither LCIS nor the County Automatic Data Processing Board has the authority to access, control, and release or use this data.

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 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. Data Assets

This policy applies to all Lucas County data assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)). A data asset is any data that is created, stored, processed, transmitted, used, or observed by a Lucas County system or by an individual working for or on behalf of Lucas County (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) Data assets also include a service that may be provided to access data from an application.

III. Definitions

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

IV. Policy

A. Data Governance: Data Owner and Data Custodian

1. All Lucas County technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) must have a designated Data Asset Owner.

   Data Asset Owners are the Board, department or agency director, elected official, Court, or non-county office that receives the services of the Lucas County Data Processing Board pursuant to ORC 307.84 or by agreement.

   Data Asset Owners are responsible for data content, context, and associated business rules. Data Asset

Owners manage as functional experts the data asset (e.g. payroll record, parcel number, court case number) throughout its lifecycle and are most familiar with the purpose and use of the data asset.

2. Data assets must have a data custodian.

   Data custodians are responsible for the safe custody, transport, and storage of the data.

   The Lucas County Data Processing Board is the custodian of all data assets governed by ORC section 307.84, either by law or by agreement.

3. Data asset ownership may be delegated or transferred but this must be recorded in the data asset management system of record. *(ORC or State Audit citation required)*

4. Data Asset Owners or their designee must complete identity verification as defined in the Lucas County Password Policy.

5. Data Asset Owners or their designees are responsible for:

   a. Participating in data governance activities within their departments (and those activities coordinated by Lucas County Information Services; for instance, updating federal, state, and local tax codes).

   b. Understanding the regulatory requirements associated with their data assets.

   c. Authorizing and auditing access to data assets in accordance with the Access Management Policy (policy draft is forthcoming).

   d. Ensuring that a rigorous justification process exists to ensure that the minimum amount of Personally Identifiable Information (PII) is collected, stored, processed, and transmitted in order to provide services in accordance with federal and state law, and Lucas County privacy policies.

A. Authorization to Access Data Assets

1. Access must be approved in compliance with the Access Management Policy.

2. Data Asset Owners must require a non-disclosure agreement (NDA) or confidentiality agreement be signed by Lucas County workforce members or third party agents acting on behalf of Lucas County prior to receiving access to Lucas County data assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) or third party data assets Lucas County has been authorized to use:

   a. If required by federal, state, or local law

   b. If required by the Data Asset Owner

B. Data Asset Documentation and Controls

Data Asset Owners are responsible for working with Data Custodians to ensure proper documentation and controls are in place.

1. Data Asset Owners, or their designees, and Data Custodians must:

   a. Complete a review of business continuity and disaster recovery requirements

   b. Complete a review of records retention requirements

c. Implement controls at the appropriate level (assets governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)).

   This typically is not at the individual file or record level but for a collection of data records such as those in a database or a series of files and folders that together have similar relevance to a workflow, public service, regulations, or other commonalities that have the same business requirements. For example:

   - Structured Data Assets controlled by Management Systems (e.g. Oracle databases, OnBase data warehouse, PeopleSoft) and associated metadata
   - Unstructured or Semi-Structured Data Assets (e.g. PDF or Text Documents and files, Spreadsheets, Image Files, Video/Audio Files, XML Files, JSON Files) containing regulated data (e.g., criminal history, protected health information)
   - Network File Share Folder Hierarchy (group or dedicated to single user)
   - Source Code Repositories managed by Lucas County Information Services
   - Virtual Infrastructure Files (e.g. virtual hard disk files for virtual machines)
   - System Files critical to enterprise infrastructure (e.g. Active Directory Domain Services and Domain Controllers, DNS Zone Files, DHCP addressing databases) or critical individual system files (e.g. Windows and Linux operating system files).

d. Implement controls that include but are not limited to:

   i. Access and Authorization Controls
   ii. Encryption/Decryption for Data at Rest, In Use, and In Transit
   iii. Cryptographic Integrity Validation
   iv. Environment Separation Requirements (e.g., production, non-production) Production data (real data that isn't fake or generated for testing purposes) must not be used or accessible to development, test, or other non-production environments unless all the required controls for a production environment are in place first
   v. Backups for Business Continuity and Disaster Recovery
   vi. Audit Logging
   vii. Security Incident Monitoring and Alerting
   viii. Retention and Secure Destruction

e. Develop a process for Data Asset Owners to audit access to their data assets and ensuring access to the data asset is appropriate and in compliance with the Access Management Policy.

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 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 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.

C. Agency or department Directors, elected officials, administrative judges, tenants and guests of Lucas County, non-County offices 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 policy 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

- Security and Awareness Training Policy

IX. Appendix B: Relevant Compliance Requirements

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
	164.306(a)	General Requirements
	164.308(a)(1)(ii)(A)	Risk Analysis
	164.310(d)(2)(i)	Disposal
	164.312(a)(2)(ii)	Emergency Access Procedure
	164.312(a)(2)(ii)	Encryption and Decryption
	164.312(c)(1)	Integrity
	164.312(e)(1)	Transmission Security
	164.314(a)(1)	Business Associate Contracts or Other Arrangements
CJIS Security Policy v5.9	4	Criminal Justice Information and Personally Identifiable Information
	5.1	Information Exchange Agreements
	5.10	System and Communications Protection and Information Integrity
PCI DSS v3.2.1	3	Protect Stored Cardholder Data
	4	Encrypt Transmission of Cardholder Data Across Open, Public Networks
NIST CSF	PR.DS	Data Security
NIST 800-53r5	AC	Access Control
	PT	PII Processing and Transparency
	SC	System and Communications Protection
	SI	System and Information Integrity

CIS Controls v7.1	13	Data Protection