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

Title: Lucas County Incident Response Policy

Affected Agencies: Countywide

Keywords: Security Incident Response

Sponsoring Agency: Lucas County Information Services

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 requirements for response to security incidents by workforce members through the establishment of an information security incident response plan.

II. Applicability and Audience

This policy applies to all information security incidents that may impact the confidentiality, availability, and integrity of technology assets (governed by and/or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) , including but not limited to attempted network intrusion, denial of service attack, detection of malicious software, unauthorized access to data, and violation of Lucas County Data Processing Board approved policies.

A. Incident Definition

Incident defined: A violation or *imminent threat of violation* of security policies, acceptable use policies, or standard security practices that jeopardizes the confidentiality, integrity, or availability of information resources or operations. Security incidents may have one or more characteristics; including but not limited to:

1. Violation of security policies previously approved by the Lucas County Data Processing Board
2. Attempts to gain unauthorized access to a Lucas County Information Resource
3. Denial of Service to a Lucas County Information Resource

4. Unauthorized use of a Lucas County Information Resource
5. Unauthorized modification of Lucas County information
6. Loss of Lucas County confidential or protected information

B. Users

This policy applies to all persons working for, or on behalf of Lucas County, including workforce members, third parties, volunteers, and contractors who access Lucas County 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 at a Lucas County facility or connecting remotely.

C. 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 (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. Policy

A. Reporting of Potential Information Security Events or Issues

1. All workforce members, guests, tenants, third party vendors, and employees of 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)) are required to immediately report information security incidents or information security vulnerabilities to an appropriate Appointing Authority and to Lucas County Information Services by opening a ticket with the helpdesk.
2. Information Security Awareness Training can come from a variety of sources including Lucas County Information Services or the specific Lucas County agency or department. In some instances, training is also provided, in part, by the State of Ohio. But, in all instances, Lucas County Information Services shall make available training on **reporting** potential information security events.
3. Lucas County Information Services will provide additional and required training to workforce members, guests, tenants, third party vendors, and employees of 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)) at least annually in accordance with the Security and Awareness Training Policy.

4. The Lucas County Cyber Security Incident Handling Team in conjunction with the Director of Lucas County Information Services will ensure that regulatory notification requirements regarding information security incidents are followed (e.g. notification to the Lucas County Sheriff for incidents covered by the CJIS Security Policy).

B. Information Security Incident Response Plan

Lucas County Data Processing Board working through Lucas County Information Services and in conjunction with the Lucas County Office of Management & Budget - Risk Management Department is responsible for establishing an information security incident response plan (for approval by the Lucas County Data Processing Board) that includes:

1. Procedures for responding to suspected or known information security incidents including escalation to Lucas County Office of Emergency Management where necessary.
2. Reporting procedures to regulatory or third parties where required
3. Documentation procedures for incidents
4. Roles and responsibilities during an information security incident
5. Communication and notification requirements and procedures when an information security incident is confirmed and how to conduct communications during an information security incident including when normal communication channels are unavailable
6. A list of Authorities to make decisions during response activities
7. Consistency with the Lucas County Comprehensive Emergency Management Plan and Emergency Support Function 2 as defined by the Federal Emergency Management Agency's National Response Framework.
8. The definition of a data breach and the requirements and procedures to manage a data breach
9. Incident closeout procedures that include a review for improvement opportunities

C. Incident Information Sharing

1. The Lucas County Data Processing Board working with Elected Officials and the appropriate Appointing Authority, will be notified prior to any public release of information concerning an information security incident.
2. With the exception of a direct report to a Director, an elected official, or an appointing authority, information about security incidents must not be shared by those select workforce members who have been chosen to participate in an incident response plan.

D. Information Security Incident Metrics

Procedures and Agency specific security metrics shall be established by the Director of Lucas County Information Services working in conjunction with the Lucas County Office of Risk Management and approved by the Lucas County Data Processing Board. The objective being: to report on information security incidents including types, frequency of occurrence, and costs of information security incidents. This information must be reviewed at least annually by the Lucas County Data Processing Board.

E. Documentation

Users responsible for responding to information security events and incidents are required to document confirmed information security incidents.

Information security incidents managed by automated security tools or processes (Cloud based or in the care of Lucas County Information Services) must generate the same documentation which must be reviewed on at least an annual basis for opportunities to reduce or prevent recurrence. Documentation must include at a minimum the following information:

1. Name of person(s) and organization(s) or system(s) conducting or participating in the response
2. Description of the technology assets affected by the incident
3. Time and date of the incident discovery
4. Time and date of earliest known event causing the incident
5. Impact to the technology assets
6. The suspected cause of the incident
7. The actions taken to mitigate the incident and restore the technology asset to a trusted and healthy operating status

8. Recommendations for further actions to prevent the recurrence of a similar incident

IV. 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 one year after the effective date.

V. Maintenance

A. This policy will be maintained 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

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 agencies that attach to the Lucas County network (governed by or under the jurisdiction of the Lucas County Data Processing Board in accordance with 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

VI. 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.

VII. Appendix A: References

- Incident Response Plan
- Security and Awareness Training Policy
- Federal Emergency Management Agency's National Response Framework

VIII. 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
	164.308(a)(6)	Security Incident Procedures
CJIS Policy v5.9	5.3	Incident Response

Lucas County Office of Risk Management		Documentation provided by the Lucas County insurance vendor FRSecure Security Incident Management Plan
NIST CSF	RS.RP	Response Planning
	RS.CO	Communications
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements
NIST 800-61r2	IR	Incident Response
CIS Controls v7.1	19	Incident Response and Management