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

Title: Lucas County Security Awareness Training Policy

Affected Agencies: Countywide

Keywords: Security Awareness Training

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 ensure workforce members are informed about information security policies and standards, regulatory requirements, and modern cyber threats to Lucas County technology assets and services.

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, 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.

III. Policy

All workforce members with access to Lucas County technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84) are required to complete Security Awareness Training in compliance with this policy. Agencies may present current non-Lucas County training of similar import to the Lucas

County Data Processing Board for approval in meeting or superseding the Lucas County mandated training.

Security Awareness Training must be completed within 60 days of hire, and at least annually thereafter.

A. Security Awareness Training System

1. The Director of Lucas County Information Services (LCIS) or designee, working in conjunction with department and agency Directors, Elected Officials, and Administrative Judges, is required to provide an enterprise countywide training system that:

   a. Enables Lucas County workforce members to meet the requirements of this policy

   b. Enables progress reporting for purposes of compliance with this policy

   c. Provides a form at the end of each training module for workforce members to provide feedback

2. The Director of Lucas County Information Services or designee working in conjunction with the Lucas County Office of Risk Management must review and report on the Security Awareness Training System at least once per year to department and agency Directors, Elected Officials, and Administrative Judges to determine:

   a. Where improvements can be made

   b. If regulatory or business requirements have changed

   c. If roles and responsibilities or organizational requirements have changed

B. Information Security Awareness Training

Department and agency Directors, Elected Officials, and Administrative Judges are required to ensure that workforce members complete security awareness training on information security topics as determined by the Lucas County Data Processing Board and as required by regulatory requirements (e.g., CJIS Security Policy, HIPAA, PCI DSS).

Topics may include, but are not limited to:

- Information Security and Privacy Policies and Regulations
- Password usage and management
- Implications of non-compliance
- Malicious email attachments
- Phishing and spoofed emails
- Web usage - allowed/prohibited
- Security of devices issued to or used by workforce members

- Visitor control and physical access to spaces
- Reporting unusual activity and potential security and privacy incidents

C. Role-Based Security Training

Workforce members in specific jobs and roles in Lucas County may require additional security awareness training.

Lucas County Information Services will work with departments and agencies to identify these roles to ensure required training is completed. These specific jobs and roles include but are not limited to:

1. Workforce members with duties covered by regulations and security standards such as HIPAA, the PCI DSS, or the FBI CJIS Security Policy

   (eg. The Lucas County Sheriff Department, Guardianship Services Board, The Toledo Board of Health, etc.)
2. Workforce members who have Incident Response responsibilities
3. Workforce members participating in software development or other technology engineering and support
4. Workforce members who have Business Continuity responsibilities

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 four years 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, Agency, or Department 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 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 the Director of 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 the 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: 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)(5)	Security Awareness and Training
CJIS Policy v5.9	5.2	Security Awareness Training
	5.3.3	Incident Response Training

PCI DSS v3.2.1	6.5	Address common coding vulnerabilities in software-development processes as follows: - Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. - Develop applications based on secure coding guidelines.
	9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. - Do not install, replace, or return devices without verification. - Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). - Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).
	12.6	Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.
	12.10.4	Provide appropriate training to staff with security breach response responsibilities.
NIST CSF	PR.AT	Awareness and Training
NIST 800-53r5	AT	Awareness and Training
	CP-3	Contingency Training
	IR-2	Incident Response Training
CIS Controls v7.1	17	Implement a Security Awareness and Training Program