Logan-Union-Champaign
regional planning commission

Director: Bradley J. Bodenmiller

Cybersecurity Policy

Purpose

To establish a framework for safeguarding information technology resources, ensuring confidentiality, integrity, and availability of data, and comply with Ohio HB 96 / ORC 9.64, as well as other applicable laws, regulations, and best practices.

Scope

This policy applies to all employees who access or manage LUC's technology resources.

Definitions

- Cybersecurity Incident: An impermissible use, disclosure, modification, or destruction of information, or interference with system operations.
- Ransomware: Malware that encrypts data or locks systems and demands payment for restoration.
- Personally Identifiable Information (PII): Any information that can identify an individual
- Information Technology (IT) Resources: All computing devices, network components, software, data, or communication channels.

Governance & Roles & Responsibilities

- Executive Committee - Provide oversight, approve cybersecurity program.
- Director - Overall responsibility for cybersecurity program, risk assessment, program implementation, and incident response. Ensure staff follow this program, enforce access controls, and report incidents.
- Employees
    - Adhere to security policies.
    - Report suspicious activity.
    - Participate in training.
    - Do not install unapproved software.
    - Do not connect unapproved devices to the network.
    - Do not reuse passwords across home and work accounts; instead, use strong, unique passwords for each account.
    - Remain vigilant for phishing attempts or suspicious activity. Report anything unusual to the Director and Operations Manager immediately.
- Prosecutor's Office – Provide advice on legal/regulatory obligations, review contracts, and data sharing agreements.

Cybersecurity Controls

- Requires unique user ID's and strong passwords
- Enforced by multifactor authentication for remote and administrative access.

10820 St. Rt. 347, PO Box 219
East Liberty, Ohio 43319
• Phone: 937-666-3431 •
• Email: luc-rpc@lucplanning.com • Web: www.lucplanning.com

- Limit access to sensitive data on a role-based basis.
- Access to personal email, social media, etc. shall not be made on LUC devices.
- Power down computers nightly and on the weekends.

Network and System Security

- Maintains up-to-date firewalls, antivirus, and cybersecurity software.
- Network drives are backed up daily to a cloud system.
- Network drives are backed up monthly on a separate hard drive.
- Sensitive data backed up as needed on a separate hard drive.
- All laptops have a camera cover

Acceptable Use & Access Control

- Access to systems and data shall follow the principle of least privilege
- Multi-factor authentication (MFA) required where feasible
- Passwords/credentials must meet complexity standards
- Use of resources for lawful, authorized purposes only

Incident Reporting & Notification

- Employees must report suspected or confirmed incidents immediately to the director.
- Reporting requirements:
  - Director – immediately
  - Law Enforcement Automated Data System (if applicable) – within 4 hours
    - (800) 589-2077
  - Ohio Homeland Security – within 7 days
    - Ohio Cyber Integration Center
      - (614) 387-1089
      - OCIC@dps.ohio.gov
  - Auditor of State – within 30 days
    - Fill out the Cybersecurity Reporting Form and email it to Cyber@ohioauditor.gov

Ransomware / Extortion Payments

- No ransom or extortion payments shall be made.

Confidentiality & Record Retention

- Incident and security program records are not public records under section 149.43 of the Ohio Revised Code
- Logs and evidence retained securely
- Retention period – minimum of two years

Privacy

- No expectation of privacy.
  - When an employee uses a LUC computer, technology, or network, there is no expectation of privacy in their activity or stored files.

Audits & Compliance

- Regular internal or external audits
- Program reviewed/updated as needed
- Compliance with Ohio Law (HB 96 / ORC 9.64)

Enforcement

- Violations may result in disciplinary action up to termination.

Policy adopted: _____

I acknowledge that I have read and understand the above policy and will adhere to said policy.

_____ _____

Employee signature Date