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

Title:	Acceptable Use Policy
Affected Agencies:	Countywide
Keywords:	Acceptable Use Policy, AUP
Sponsoring Agency:	Lucas County Information Services (LCIS)

Approved by Data Processing Board March 3, 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 define what "acceptable use" means as it pertains to the use of Lucas County's 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)), and confirm that authorized users are aware of the rules by their acknowledgement of this policy.

Information technology resources are provided to authorized "users" to conduct and/or facilitate official County business. It is the responsibility of each user to make certain that such resources are not misused. This policy summarizes user responsibilities and governs the acceptable use of IT infrastructure, services, and equipment.

Lucas County Data Processing Board, employing Lucas County Information Services, may propose additional, supplemental, or new polices subsequent to this agreement to better define specific categories relating to IT resources. Changes to policies must be approved by the Lucas County Data Processing Board.

All "users" (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) must sign this agreement indicating that they understand and will comply with all IT policies and procedures. In addition: The acceptance and use of Lucas County provided system "logins" (username + password) (for assets governed by or under the jurisdiction of the

Lucas County Data Processing Board (ORC 307.84)), is further acknowledgement of all IT policies.

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. Technology Assets

This policy applies to the use of all Lucas County technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) including web or "cloud" based platforms, applications, and services that are owned and operated by a service provider on behalf of Lucas County (e.g Oracle Corporation) and department or agency specific cloud based platforms managed by functional business processes owners.

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. Acceptable Use Behavior

Lucas County, employing Lucas County Information Services (LCIS) and agency specific functional business process owners, must protect the confidentiality (authorized access to systems and information), integrity (authorized modification of systems and information), and availability (making sure systems and information are available when needed) of all technology assets governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84).

When engaged in the performance of your role with Lucas County:

1. Attempts to disable or circumvent any Lucas County security controls, policies, or procedures (e.g., disabling virus protection or installing unauthorized software) (assets governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) is prohibited. This includes, but is not limited to:

    a. Use of tools that compromise security (e.g., password crackers, network sniffers, attack frameworks and software distributions , proxies, unauthorized VPN clients, or other tunneling technology)

    b. Attempts to disable, defeat, or circumvent any Lucas County information security components

    c. Intentional interference with the normal operation of Lucas County technology assets

2. Use that violates Lucas County policy or local, state, and/or federal laws is strictly prohibited. This includes, but is not limited to:

    a. Theft of Lucas County technology assets, including sensitive data

    b. Use of Lucas County systems for any type of harassment, which includes using any words or phrases that are derogatory based on race, color, sex, age, creed, disability, marital status, national origin, religion, pregnancy, gender, gender identity or expression, genetic information, sexual orientation, veteran or military status, use of a service animal, or any other status protected by federal, state and local law

3. Unauthorized use, destruction, modification, or distribution of Lucas County external and internal systems, applications, and data, governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84) is prohibited. This includes, but is not limited to:

    a. Release or disclosure of Lucas County data to unauthorized parties inconsistent with federal, state, and local law (e.g., HIPAA), Lucas County policies, or inconsistent with your assigned job role and responsibilities.

b. Attempts to modify administrative settings or configurations or repair hardware and software. Such modifications, configurations and repairs shall only be performed by authorized functional support personnel for your department or agency.

   This excludes basic troubleshooting such as closing and restarting an application or a restart/reboot of a single workstation.

   Modification, configuration, and repairs of enterprise level information technology equipment and networking infrastructure shall only be performed by authorized support personnel or third parties supervised by authorized support personnel.

c. Removal of technology assets from Lucas County premises without prior approval by Lucas County Information Services (LCIS), agency or department Directors, or administrative judges is prohibited.

   This excludes technology issued directly to you for employment purposes approved for taking home by your supervisor, human resources personnel, or Lucas County Information Services (LCIS).

4. Use of personal devices including computers, network devices, or any other personal equipment to make a direct network connection to Lucas County internal private networks (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) is prohibited.

   Examples of direct connections to internal private networks include but are not limited to: workforce members plugging in personal computers to network ports in the walls, workforce members bringing personal wifi extenders to work, workforce members bringing Sony or Nintendo gaming systems to work, workforce members bringing programmable internet enabled thermostats to work, etc..

5. Personal devices such as mobile phones and tablets may be used to access Lucas County technology such as email, calendar, and unified communications (e.g. Microsoft Teams, Cisco WebEx, and Zoom) and for purposes of multi-factor authentication.

   Personal devices must utilize apps (mobile applications and/or software e.g. VPN software) authorized by Lucas County Information Services (LCIS) for the purposes of accessing Lucas County information assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)).

6. Use of information systems (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) to solicit for commercial ventures, religious or political causes, or for personal gain unrelated to the processes of working for or on behalf of Lucas County is prohibited unless explicitly allowed by Lucas County policy or federal, state, or local law.

7. Lucas County's assets must never be left unattended in an unsecured location (e.g., at the airport, or in a coffee shop). A secured location can be a locked vehicle (out of sight if possible), your home (secured from use by family members and guests), or within designated areas in Lucas County facilities such as an assigned cubicle or equipment storage location. Please review Lucas County telecommuting policies and guidance for further information regarding secured location requirements when telecommuting.

   When working remotely or in a Lucas County facility, workforce members must lock, "auto lock", or log out of Lucas County technology assets like laptops when not in use to prevent an unauthorized individual from obtaining data or information.

   When working with regulated data, workforce members should take precautions (e.g., positioning the equipment so the screen cannot easily be viewed or using a screen protector) to prevent others from being able to view the information on the screen while in use. When regulated data is being communicated through phone calls or spoken aloud, workforce members should take precautions (e.g., closing a door, asking people to step out for a few moments, using a headphone, speaking softly, or finding an alternative way to communicate the information) to prevent access by unauthorized parties.

8. Lost or stolen Lucas County technology assets must be reported immediately by opening a ticket with Lucas County Information Services. **Your department or agency may have additional procedures for lost or stolen assets. Please speak with your supervisor to determine what these additional procedures may be**.

9. Upon termination of any Lucas County workforce member, including a third party or contractor, all Lucas County technology assets must be returned the appropriate appointing authority, agency or department Director, or to Lucas County Information Services if the asset needs to be secured or preserved for additional review.

10. Hardware and software must be procured in accordance with Lucas County Data Processing Board procurement policies and properly licensed and registered in the name of Lucas County Board of Commissioners.

B. Personal Use

Lucas County technology assets are purposed for conducting the business of Lucas County.

Occasional personal use of technology equipment issued to workforce members is permitted (e.g., phones and/or unified communication systems, workstations and peripherals like keyboards, monitors, mice, printers, copiers, and fax machines)

Be aware: Information created, processed, sent, received, or stored during personal use of Lucas County technology assets will not be handled differently by Lucas County.

Such information may be subject to Lucas County policies, and federal, state and local laws including Public Records Act. Personal files should not be permanently stored on Lucas County technology assets. Lucas County is not responsible for backing up or recovering personal data.

C. Acceptable Use of the Internet (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)

You represent Lucas County when using Lucas County's technology infrastructure to access the internet, and some types of activities on the internet can pose a security risk to Lucas County's technology assets.

You are responsible for ensuring that your use of the internet is appropriate, ethical, lawful, and within the scope of your employment at Lucas County.

1. Lucas County Information Services (LCIS), reserves the right to block access to internet web sites and addresses, including malicious internet web sites or internet addresses unrelated to Lucas County's business.
    a. Blocked websites may include possibly malicious or hacked websites, websites that contain inappropriate or offensive content, or websites provided from geographic locations known to be hostile to the United States. These websites could lead to disclosure of non-public information.
    b. You may submit a ticket to the LCIS helpdesk to unblock websites for legitimate business usage, as determined by an appointing authority, agency or department Director, or Administrative Judge.

2. Lucas County Information Services may monitor and log the use of the internet by technology assets connected to Lucas County operated networks for the express purpose to comply with various laws, legal proceedings, or internal policy, to troubleshoot and support technology, or to monitor and investigate unauthorized activity.

   This includes, but is not limited to:

   a. Use of monitoring tools installed locally on a workstation;

   b. Analysis of various logs generated by the user or system activity (such as proxy servers, network devices, authentication and directory servers, intrusion prevention/detection devices, firewalls, web/file servers, and other systems as necessary); and,

   c. Traffic analysis on inbound or outbound network traffic, including the interception, decryption, and inspection of encrypted traffic.

3. While using Lucas County technology assets you must not:

   a. Use the internet for any unlawful activity or for personal gain

   b. Reproduce, distribute, or display copyrighted materials without prior permission of the copyright owner. This includes text, images, photographs, music files, sound effects, and other legally protected works.

   c. Represent personal opinions as those of Lucas County, such as in social media, blogs, or forums.

   d. Perform any activities that may harm the reputation of Lucas County operations or staff with controversial issues (e.g., sexually explicit materials).

      This does not refer to appropriate and legal activities (e.g., activities by collective bargaining units, or use of Lucas County public or personnel feedback or complaint processes) regarding the delivery of Lucas County services.

C. Acceptable Use of Electronic Messages

Malicious individuals often use email when trying to acquire Lucas County customer data, non-public information and data, or to compromise Lucas County's technology assets.

You are required to use Lucas County email applications in the following professional manner:

1. Not all workforce members are authorized to access the same information. Accounts are issued solely for use by the individual to whom the account has been assigned. Sharing

individual account information may lead to unintentional disclosure of data and is prohibited. Exceptions to this policy: In some instances, if you must share individual account information with authorized support personnel, who upon completion of support work, you will be immediately advised to establish a new password unknown to that support agent.

Shared mailboxes where an authorized workgroup can monitor emails sent to and from the shared mailbox are allowed.

Administrative proxy delegation of access to an individual email account is acceptable (e.g., an executive or administrative assistant or a peer), as long as this is accomplished through the email system's delegation functionality and not by sharing credentials. (State or Federal laws/ regulations may apply.)

2. If you have doubts or serious concerns about the origin or authenticity of an electronic message, or if you receive a highly abnormal or suspicious message, you should report the message by submitting a ticket to the LCIS helpdesk or by use of the messaging systems integrated reporting mechanism (e.g., a spam/ or phishing button in email clients). Your department or agency may have additional reporting requirements so check with your supervisor.

3. Use caution when opening emails and attachments, particularly those received from an external sender.

    a. Don't open any attached files or click on hyperlinks to download files containing macros, scripts, or executables from an unknown or suspicious source.

    b. Malicious messages often appear to come from a valid source and could attempt to make you disclose personal or sensitive information. Use caution when opening attached files or clicking on hyperlinks, or when unusual requests or information is included in the email even if from a familiar sender.

    c. Training will be provided on detecting malicious emails to all Lucas County workforce members.

        Additional training may be required if there is repeated susceptibility to malicious emails by individuals.

4. Do not forward Lucas County email containing confidential, sensitive, or regulated data to personal email accounts. Exceptions may be granted by Lucas County Information Services (LCIS), agency or department Directors, elected officials, or Administrative Judges.

5. Automatic forwarding of email through the use of rules to any external domain requires approval by Lucas County Information Services (LCIS), agency or department Directors, elected officials, or Administrative Judges and can be requested by opening a ticket with the LCIS helpdesk.
6. Do not send fictitious or forged messages that could be mistaken for official Lucas County statements, marketing, or materials.
7. Do not send junk mail or chain letters.
8. Do not use profanity, inappropriate language, pornography or sexually explicit material, slanderous, discriminatory language, or harassing comments.
9. Do not use Lucas County messaging applications to send threatening or libelous messages.

D. Acceptable Use of Voice Communications Systems

Lucas County's phone and communication systems are information assets and attach to the Lucas County Network which is managed by Lucas County Information Services pursuant to ORC 307.84 through 307.847. Similar to internet browsing and other computing activities, phone call information and metadata (e.g. Caller ID, Date and Time of Call, Call Duration) may be monitored and logged.

1. If the call is to be recorded, you must notify all call participants that the call will be monitored or recorded, including the purpose of recording at the outset of the recording and include the notification in the recording.

   This does not apply to lawful monitoring or recording that does not require consent in accordance with federal, state, or local law. Voicemail or other automated telephony system recordings comply with this section if the recorded greeting clearly indicates that the caller has reached a voicemail system or is about to be recorded.

2. Call recordings containing sensitive or regulated data presents serious security and compliance risk and should be avoided. Departments or agencies that will purposefully and continuously record sensitive or regulated data such as payment card data or protected health information must notify the Director of Lucas County Information Services unless explicitly authorized in federal, state, or local law (e.g., calls to 911).

E. Acceptable Use of Wireless Networks

Not all wireless networks are configured with strong security protections. In addition, unauthorized and malicious wireless devices may pose a risk to Lucas County technology assets. While performing your role at Lucas County:

1. Direct connections (i.e., directly connected to internal wireless access points or physical network infrastructure like a data jack in a wall plate or a network switch port) to Lucas County's protected internal private wired and wireless network is provided only to Lucas County workforce members using Lucas County owned and operated technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)).

   Third parties, vendors, contractors, and other non-Lucas County personnel access to Lucas County's protected internal private wireless or wired network (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) is prohibited without prior approval by Lucas County Information Services (LCIS) who may employ security measures to prevent unauthorized network connectivity. If an exception is required for a legitimate business need please open a ticket with the LCIS helpdesk.
2. Third-party internet access (such as access provided at airports, hotels, and coffee shops) carry potential security risks to Lucas County technology assets. Special care should be taken to ensure you are connecting to the correct network and not bypassing any security alerts and warnings.
3. Lucas County's wireless network infrastructure (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) may only be altered and managed by Lucas County Information Services (LCIS).
4. You must not install, connect, or modify any wireless infrastructure such as Wireless Access Point (WAPs) to Lucas County's network (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) without explicit written authorization from Lucas County Information Services (LCIS).

F. Acceptable Use While Utilizing Remote Access Technology

Remote access to Lucas County's applications is available for workforce members to work outside of the office or for telecommuting.

While using remote access:

1. Ensure you do not type any remote access passwords while someone is watching.

2. Do not leave technology assets unattended and remotely logged on to Lucas County's network. When not in use, store your equipment and media used to remotely access Lucas County systems in a secured location.
3. Do not share passwords, smart cards, tokens, keys, fobs or any other access or authentication devices with any other person unless required by authorized support personnel who upon completion of support work immediately advise the user on steps to establish a new password unknown to that support agent.
4. Vendors must be limited to the minimum amount of privilege and access required to perform the necessary duties while using remote access methods approved by Lucas County Information Services (LCIS).
    a. Remote support sessions must first be authorized by LCIS technology support personnel before the session is established and terminated as soon as the vendor has finished their work.
    b. No vendor may be given remote access that is not strictly controlled and monitored.
    c. Vendors shall not be given permanent remote access to Lucas County's network unless that access is strictly limited to the systems supported by the vendor and controls are in place to monitor their activities to ensure they are not able to gain additional access to other Lucas County technology assets from the systems they are able to remotely access.
5. Remote access to technology assets that contain sensitive or regulated data requires multi-factor authentication and use of a secure connection between the host and the remote device.
    a. You must not use remote access products like TeamViewer, GoToMyPC, or similar products unless approved by Lucas County Information Services (LCIS).
    b. Do not use public facing Wi-Fi or private wireless networks that do not require user authentication with login credentials and passwords. Do not bypass warnings that indicate the wireless network is not secure.

G. Acceptable Use of Social Media

1. You must exercise judgment and use caution when interacting online. It is important to remember that in an online environment, the lines between public and private, and personal and professional, are not always clear. When you identify yourself as a Lucas County workforce member, employee, or affiliate on social media, a perception is created about you as a representative of Lucas County, your expertise, and Lucas County itself.

2. Creation and use of a social media account on behalf of Lucas County must be done in compliance with Lucas County social media policies.

H. No Expectation of Privacy

1. Lucas County, employing Lucas County Information Services, manages and monitors systems designed to store information assets.

   Lucas County, employing Lucas County Information Services must monitor all systems and users of technology assets (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)), in order to maintain a secure environment and meet compliance requirements.

   Except in instances when an expectation of privacy is codified, mandatory, or otherwise part of the law, you should have no expectation of privacy or confidentiality while using Lucas County technology assets, including internet access and emails.

   Usage may be monitored for policy, security, or network management reasons and may be subject to inspection. Unless prohibited by law or other policy, inspection and monitoring of Lucas County technology assets by management does not require the consent of individual workforce members.

2. Except in instances when an expectation of privacy is codified, mandatory, or otherwise part of the law, all electronic messages or data created, stored, transmitted, or received over Lucas County systems or through Lucas County internet connections may be subject to inspection or monitoring.
3. Lucas County, employing Lucas County Information Services reserves the right to store the contents of any messages or data sent over networks (governed by or under the jurisdiction of the Lucas County Data Processing Board (ORC 307.84)) and use that information to enforce policies previously approved by the Data Processing Board or comply with federal, state, or local law.

   If the content violates regulations or laws, Lucas County, working with the Lucas County Data Processing Board and the appropriate agency or department Directors, elected officials, or Administrative Judges, reserves the right to submit the information to law enforcement for potential prosecution.

I. Reporting Known or Suspected Vulnerabilities or Security Incidents

You must report known or suspected security weaknesses, instances of inappropriate access, and suspicious activities to Lucas County Information Services (LCIS) by opening a ticket with the helpdesk. **Your department or agency may also have reporting requirements so please check with your supervisor**.

1. You will be responsible for the confidentiality, integrity, and availability of your files. If concerning circumstances occur with your files such as inappropriate access, loss of the files, or changes are made to files without your consent please speak with your supervisor and report this issue by opening a ticket with the LCIS help desk.
2. You must report suspicious activities happening to or on your workstation such as someone remote controlling the workstation without your consent or new and unfamiliar software performing unusual activities by opening a ticket with the LCIS helpdesk.

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 twelve months after the effective date.

V. 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 (technology assets 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.

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 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
	45 CFR 164.316	Policies and procedures and documentation requirements.
CJIS Security Policy v5.9	5.2.1	Basic Security Awareness Training
PCI DSS v3.2	12.3.5	Acceptable Uses of the Technology

NIST CSF	PR.AT	Awareness and Training
	PR.IP	Information Protection Processes and Procedures
NIST 800-53r5	AC-8	System Use Notification
	AT-1	Policies and Procedures
	PL-4	Rules of Behavior
	PS-6	Access Agreements
CIS Controls v7.1	17	Implement a Security Awareness Training Program