Toledo-Lucas County Health Department Policy

Computer, Network, & Internet Acceptable Use Policy

Original Effective Date:	Review / Revision Date:	Board of Health Resolution:
June 22, 2017	July 16, 2018	2017.06.082

Maintenance Steward: Supervisor of Information Services **History:** ☒ New ☐ Revised ☐ Archived

Organizational Scope:

☒ Full Agency ☐ Administration ☐ Community Services ☐ Environmental Health ☐ Health Services

Frequency of Review:

☒ Annually ☐ Biennially ☐ 5 Years ☐ As Needed ☐ Other:

Location:

G-Drive: G: → Users → Common → Policies & Procedures

Website: www.lucascountyhealth.com/employee-login/

Hardcopy: Information Services Department

Archived Version(s):

Requisite Signatures

☒	Board of Health President	Date 6.22.2017
☒	Health Commissioner	Date 06-26-17
☒	Director of Administrative Services	Date
☒	Director of Environmental Health & Community Services	Date 7/5/2017
☒	Director of Health Promotion & Policy Integration	Date 6-22-2017
☒	Director of Health Services	Date 6-27-17
☒	Director of Human Resources	Date 6-27-17

Computer, Network, & Internet Acceptable Use Policy

I. Policy

It is the policy of the Toledo-Lucas County Health Department (TLCHD) to provide guidance on acceptable use of network services and to protect employees, partners, and TLCHD from illegal, malicious, or otherwise damaging actions that compromise the digital security of the Department's operations.

II. Scope

This policy applies to employees, contractors, consultants, temporaries, volunteers, interns and other workers at TLCHD, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by TLCHD.

III. Purpose

The purpose of this policy is to outline the acceptable use of network services and computer equipment issued by or within TLCHD, and applies to the use of information, electronic and computing devices, and network resources to conduct TLCHD business. These rules are in place to protect the employee and TLCHD. Inappropriate use exposes TLCHD to risks including virus attacks, compromise of network systems and services, and legal issues.

IV. Background

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, tablets, cell phones, software, operating systems, storage media, network accounts providing electronic mail, World-Wide Web (WWW) browsing, and File Transfer Protocol (FTP), are the property of TLCHD. These systems are to be used for business purposes in serving the interests of TLCHD, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every TLCHD employee and affiliate who deals with information and/or information systems. It is the responsibility of every employee to know these guidelines, and to conduct their activities accordingly.

V. General Use & Ownership

A. In accordance with section (V)(A) "Ownership & Equipment Privacy" of the *Department Issued Equipment Policy*:

1. All TLCHD issued equipment remains, at all times, the property of the Board of Health.

2. TLCHD reserves the right to access, search, examine, and/or monitor the contents or usage of network services and department issued equipment (especially computers, email, internet, and cell phones) for the purpose of supervising or investigating the performance of the employee's duties, including compliance with all TLCHD policies and procedures.

    a. Employees shall have no expectations of privacy when using TLCHD issued equipment or network services, when accessing or disseminating information over the same, or when using personal devices in conjunction with TLCHD issued equipment or network services.
    b. Employee use of TLCHD equipment constitutes the employee's consent to search, examine, or otherwise monitor the contents and use of such equipment or network services (including browser and network histories, password protected websites/email, and deleted materials).
    c. Any passwords or locks used in connection with department issued equipment or network services must be made available/provided to the appropriate TLCHD representative.

3. Employees who use personally owned electronic devices (cell phones, tablets, etc.) for TLCHD business purposes to access email, internet, or other TLCHD online services, shall have no expectation of privacy in that access or for those communications. Such use of personally owned devices may be subject to monitoring and the contents may be subject to the provisions of the *Public Records Request & Retention Policy*.

B. TLCHD proprietary information stored on electronic and computing devices- whether owned or leased by TLCHD, the employee, or a third party- remains the sole property of TLCHD. Staff must ensure through legal and/or technical means that proprietary information is protected.

C. All employees, contractors, consultants, temporaries, volunteers, interns, and other workers are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with TLCHD's policies and standards, local laws, and regulations.

D. Staff must promptly report the theft, loss or unauthorized disclosure of TLCHD proprietary information to their immediate supervisor.

E. Staff may access, use or share TLCHD proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties.

F. Employees are responsible for exercising good judgment regarding personal use of department issued equipment or network services.

1. Personal use of internet or other network services during work hours should be limited to employee breaks, lunch, or other non-work time.

    a. At no time shall department issued equipment or network services be used for personal gain or to advance any individual views or position that is contrary to TLCHD policies, procedures, or mandates.

b. Any personal use of department issued equipment must adhere to the *Social Media, Ethics, and Workplace Violence & Harassment* policies.
c. Any personal use of department issued equipment that interferes with employee productivity or the operation of TLCHD technical services may be subject to disciplinary action up to and including termination.

2. Individual departments are responsible for creating and monitoring guidelines concerning personal use of the internet.
3. If there is a business need for special access, staff should consult their supervisor or manager and make a request to the TLCHD helpdesk (healthhelpdesk@co.lucas.oh.us) for approval in accordance with Lucas County *Electronic Mail and Internet Use Policy*.

G. For security and network maintenance purposes, authorized individuals within TLCHD may monitor equipment, systems and network traffic at any time.

H. Staff must get approval from TLCHD Information Services department for use of any new or updated hardware and/or software prior to download, installation or connection to the network or inclusion for use on any TLCHD device.

I. No Electronic Protected Health Information (ePHI) should be stored or transported on any device or media and removed from TLCHD physical facilities without express management approval and proper data protection/encryption.

J. No password or other credentials shall be saved to automatically login a user to any computer or software system. This includes, but is not limited to, Internet access and systems containing ePHI.

K. Employees shall not change the default time-out/log-out settings for any software or workstation.

L. IT Setup Requests

1. To ensure the necessary technology is in place for new employees, an IT Setup Request Form must be completed and submitted to the Information Services Helpdesk by the department director and/or supervisor 1-2 weeks in advance of the new employee's start date.

    a. This form is located at: S:\COMMON\2. Forms, Templates & Resources\Electronic Forms\EmployeeITSetupRequest.docx

2. This form is also required to be used when existing employees transition to a new job position, a new office location, or other special technology requirements arise.

M. Technology Quotes and Purchasing

1. All technology quotes and purchasing of IT equipment and software should be conducted by TLCHD Information Services and approved by the Information Services Manager.

2. Reasonable advance notice shall be provided to ensure an appropriate technical evaluation can be made in order to meet the business needs of the organization, provide for future product support, and ongoing maintenance.

N. Off-Duty Use & Access

1. Employees who use or access TLCHD issued equipment or network services during non-work hours shall have no expectation of privacy regarding such usage. TLCHD reserves the right to monitor use of all equipment or network services at any time.

    a. This includes, but is not limited to, using Virtual Private Networks (VPN), email synced to employee owned or department issued cellular phones, tablets, or laptops, and any other use of TLCHD equipment or network services.

VI. Security and Proprietary Information

A. All mobile and computing devices that connect to the internal network directly or through VPN or other means must comply with the Lucas County *Electronic Mail and Internet Use Policy*.

B. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. If there is any uncertainty of the contents of an email, do not open and contact the TLCHD Help Desk for further evaluation.

C. During environmental or operational changes that could affect the security of ePHI, staff shall routinely monitor and evaluate procedures to adequately protect ePHI in accordance with all federal laws, regulations, and guidance documents.

D. Staff access to ePHI may be audited by external organizations, administration, or the Information Services department, their identity may not be protected, and consequences of inappropriate access can be issued.

E. No ePHI or Personal Identifiable Information (PIN) shall be removed from TLCHD premises on any device, cloud based service, or portable electronic media capable of storing or transmitting data unless authorized by their division director.

F. Password Rules and Criteria

1. **Passwords may not be shared.**
2. All user passwords must comply with requirements set forth by each software application in order to protect ePHI. Providing access to another individual, either deliberately or through failure to secure its access, **is expressly prohibited.**
3. Employees must lock their workstation / computer or log off when the device is unattended.
4. No password should include personal information (i.e., SSN, family member names, etc.)
5. Passwords created or used to conduct TLCHD business must be made known to an appropriate TLCHD representative to allow TLCHD access in accordance with section (V)(A).

VII. Unacceptable use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities.

Under no circumstances is an employee of TLCHD authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing TLCHD-owned resources or on TLCHD's premises.

A. Users shall not enable/disable any configured automatic updates for operating system or software patches (Windows, IOS etc.) and are responsible for ensuring their devices are up to date. If they have any questions regarding a software update or computer configuration they should contact the TLCHD Helpdesk for advice/assistance.

B. Any use that interferes with normal TLCHD business operations; involves solicitations; or promotes personal gain is considered unacceptable.

C. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed or approved for use by TLCHD.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which TLCHD or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Intentional introduction of malicious programs into a computer, network or server is subject to disciplinary action up to termination.
5. Revealing your account password to others or allowing use of your account by anyone at any time.
6. Procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws and policies.
7. Making fraudulent offers of products, items, or services originating from any TLCHD account.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended

recipient or logging into a server or account that the employee is not expressly authorized to access.

9. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
10. Circumventing user authentication or security of any host, network or account.
11. Introducing honeypots, honeynets, or similar technology on the TLCHD network.
12. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's computer via any means.
13. Providing information about, or lists of, TLCHD employees to parties outside TLCHD without prior administrative approval.

D. Email and Communication Activities

When using TLCHD resources to access and use the Internet, users must realize they represent TLCHD. Whenever employees state an affiliation to TLCHD, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the Toledo-Lucas County Health Department".

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or messaging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email information.
4. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
5. Creating separate email accounts or technical software or services to conduct official TLCHD business without proper archiving and approval from TLCHD Information Services.

E. Online Journals (Blogging) and Social Media

1. Please refer to the *Social Media Policy* for more information on acceptable use and practices concerning online journals.

VIII. Compliance

A. TLCHD Administration will verify and ensure compliance to all provisions in this policy.
B. Any exception to the policy must be approved by the TLCHD Administration in advance.
C. An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

IX. Maintenance

A. Review

1. The *Information Services Acceptable Use Policy* is to be reviewed annually to ensure compliance with both agency and accreditation standards.

B. Revision

1. All changes made to this policy are to be noted on the **Record of Change**. Substantial changes will require renewed signatures from all applicable parties. This includes changes to the intent, scope, procedures, or policy statement.
2. Changes in style, format, grammar or minor error correction will not require renewed signatures but must be indicated on the Record of Change.

X. Glossary

A. <u>Department Issued Equipment</u>: includes office space; lockers & file cabinets; laptops; cell phones; tablets; laser levels; lead survey equipment; portable printers; projectors; electronic probe thermometers; vacuum pumps; air compressors; blood pressure monitoring equipment; EKG machines; and other equipment necessary for employees to perform their jobs.

B. <u>Portable Electronic Media</u>: includes, but is not limited to, hard drives, floppy disks, CDs, DVDs, flash drives, smart cards, personal digital assistants (PDAs), tablets, smart phones, or other storage devises.

Record of Change

(Required for all policies)

Date of Change	Changes Made By	Changes Made/Notes	Approved By
7/16/2018	BP	During review by TLCHD staff and the Personnel Committee on 7-16-18, this policy's content was found to be accurate, sufficient, and current.	Personnel Committee