POLICY AND PROCEDURE	
SUBJECT/TITLE:	Information Technology Policy
APPLICABILITY:	All staff
POSITION & DIVISION:	Executive Assistant, Administration
ORIGINAL DATE ADOPTED:	10/04/2017
LATEST EFFECTIVE DATE:	10/04/2017
REVIEW FREQUENCY:	Every 5 years
BOARD APPROVAL DATE:	N/A
REFERENCE NUMBER:	800-005-P

A. PURPOSE

A strong operational infrastructure is necessary in order to administer public health services efficiently and effectively to meet the needs of the population. By maintaining a strong organizational infrastructure, the health department can assess and improve its operations, staffing, and program support systems.

This policy will establish the general operational policy and guidelines that are essential to maintain a strong, secure, and responsive information infrastructure.

B. POLICY

Information technology (IT) resources that include but are not limited to: computer networks, computers, software, websites, data files and systems, phones, printers, and other devices are provided by the department to support the administrative functions of the department. Department technology resources shall be used in a manner that protects the security and integrity of these resources. Use of these systems is governed by federal, state, and local privacy protection regulations.

C. BACKGROUND

This policy, commonly referenced as the IT policy, refers to the acquisition and implementation of the hardware and software used to support the department's needs to capture, store, retrieve, transfer, communicate, and disseminate information. It includes acquiring, leasing and licensing systems. This also includes communication network systems such as videoconferencing, voice mail, and email, as well as internet, intranet, and social media use.

D. GLOSSARY OF TERMS

Hardware refers to all electronic devices used to access all professional networks and data, including, but not limited to personal computers and workstations; laptop computers; mobile devices such as tablets and smart phones; computer components such as disk drives and tape drives; peripheral equipment such as printers, modems, fax machines, flash drives, scanners and copiers.

Software refers to applications and associated files and data, including applications that grants access to services, such as the internet and electronic mail systems.

HIPAA – Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information.

E. STANDARD OPERATING GUIDELINES

1. GENERAL USE

a) CCHD provides the IT tools necessary for staff to complete their assigned duties. These tools include hardware and software necessary to access internal networks (e-mail, intranet, etc.) and external networks like the internet. CCHD requires that these systems be used responsibly, ethically and in compliance with all legislation and other health department policies, including HIPAA. IT resources are not to be used for personal purposes.

b) Authorization

i) CCHD staff are authorized access to only the CCHD hardware and software necessary to fulfill their job duties.

ii) New hires, job changes and terminations

(1) Supervisors will be responsible for initiating requests for access to IT systems for newly hired employees pursuant to department policy. Access to IT systems will only be granted pursuant to Section 3010 of the department's HIPAA policy (minimum necessary clause).

(2) Supervisors must notify the Fiscal Officer of job changes. The Fiscal Officer will process requests for any necessary adjustments pursuant to department policy and in accordance with Section 3010 of the department's HIPAA policy.

(3) Supervisors must notify the Fiscal Officer of terminations. The Fiscal Officers will process requests to remove access pursuant to department policy and in accordance with Section 3010 of the department's HIPAA policy

(4) The employee shall sign upon hiring the Information Technology User Agreement (800-005-03-F)

c) Portable Devices, Mobile Devices and Home Computer Use

i) These devices may be supplied by the department or those personal devices approved by the department. Use of these devices is only permitted when they are used in accordance with Section 3085 of the department's HIPPA policy.

d) Improper Uses

i) Prohibition Against Prohibited Speech and Actions

(1) Harassment, political speech, illegal activities or any other speech or actions prohibited by legislation or policy, such as the Health Code, remains prohibited when using CCHD hardware and software.

ii) Personal Use of CCHD Hardware and Software

(1) CCHD hardware and software must not be used to conduct personal business.

e) Hardware and Software acquisition

i) Hardware and software purchases must be approved by the Fiscal Officer and the City of Canton Information Technology (IT) department, or another applicable entity.

(1) Supervisors should contact the IT department for pricing before creating a purchase request.

(a) If the IT department is unable to provide a price, standard purchasing procedures should be followed and approval of the suitability of the hardware or software from the IT department must be obtained prior to completing purchase request.

(i) IT approval requests can be submitted via a work order at http://itnet.

2. SOFTWARE USE

b) Appropriate use

i) Appropriate use of software including email, internet browsing, social media and instant messaging are defined in Sections 3080 and 3082 of the department's HIPAA policy.

(1) All usage may be logged.

(2) Email should be stored in accordance with the department's Electronic Mail Retention Guidelines (800-018-P).

c) License Restrictions

i) All software in use on CCHDs Technology Resources must be licensed for use by the department.

(1) The licensing terms of free or open source software must be reviewed prior to its use.

d) Software installation

i) Software installation must be performed in accordance with Section 3080 of the department's HIPAA policy.

ii) Software Pre-Approved for Installation (800-005-01-A) contains a list of pre-approved software. Changes to this list must be approved by contacting the department's HIPAA Security Officer and Fiscal Officer, in accordance with the HIPAA policy.

e) Software patching

i) Software updates must be performed in accordance with Section 2090 of the department's HIPAA policy.

3. SOCIAL MEDIA

f) When using department computers, Social Media sites, including Facebook, LinkedIn and others, are to be used only in conformance with, 3082 Use of Social Media in the HIPAA Policy. This policy also addresses requirements for use of social media from outside the department.

4. SECURITY

a) Introduction

i) CCHD staff are likely to encounter protected health information. It is the duty of every staff member to ensure the security of this information. For this reason, the department's electronic security policies are defined in the HIPAA policy

b) Passwords

i) Passwords shall be maintained in accordance with Sections 3010 and 3080 of the department's HIPAA policy.

c) Other Technical Safeguards

i) Other technical safeguards must adhere to Sections 2060, 2090 and 3080 of the department's HIPAA policy.

(1) These safeguards include, but are not limited to, virus and malware protection, firewalls, network configurations, device encryption and workstation configurations.

5. DATA BACKUP

a) Daily backups of the department's server and data files are performed by the city's IT department, in accordance with the IT Department's policy.

b) To restore a lost or damaged file, a work order should be submitted to the city's IT department including the name and location of the file and the last date it was known that the file was still accessible.

c) Only information that is stored on the network/server is backed up by the IT Department. Data saved on personal devices or on computer hard drives (C drive) is not backed up.

6. MALFUNCTIONS

a) Hardware and Software maintenance services at CCHD are provided by the City of Canton's IT department unless specified otherwise by grant requirements.

i) Problems affecting the whole department such as a server outage or voice mail outage should be reported to the Administrative Executive Assistant who will contact the IT department.

ii) For individual problems, each division will have its own problem reporting procedure but these procedures must include at least;

(1) A specific point of contact for Hardware and Software issue reporting

(2) A process for troubleshooting before contacting the IT department

(3) A process for submission of work orders using the system provided by the IT department

i. http://itnet in a web browser;

ii. or contacting the IT department via phone at 330-438-6168

7. EMAIL

a) See 800-018-P for Email Retention and Storage

F. CITATIONS AND REFERENCES

Canton City Health Code

800-016-P HIPAA Policy

800-018-P Electronic Mail Retention Guidelines

G. CONTRIBUTORS

The following staff contributed to the authorship of this document:

1. Technology Committee

H. APPENDICIES AND ATTACHMENTS

800-005-01-A Software Pre-Approved for Installation

800-005-02-A Canton City IT Department Backup Procedure/Policy

800-005-03-F_Information Technology User Agreement

I. REFERENCE FORMS

J. REVISION AND REVIEW HISTORY

Revision Date	Review Date	Author	Notes

K. APPROVAL

This document has been approved in accordance with the "800-001-P Standards for Writing and Approving PPSOGFs" procedure (this procedure) as of the effective date listed above.