Yolo County Housing

Lisa A. Baker, Executive Director
147 W. Main Street
WOODLAND, CA 95695

Woodland: (530) 662-5428
Sacramento: (916) 444-8982
TTY: (800) 545-1833, ext. 626

DATE: January 14, 2010

TO: YCH Board of Commissioners

FROM: Lisa A. Baker, Executive Director

PREPARED BY: Janis R. Holt, Resource Administrator

SUBJECT: **Review, Approve and Adopt Information Technology Policy**

RECOMMENDED ACTION;

That the Board of Commissioners review and approve the proposed YCH Information Technology Policy and authorize the Executive Director to implement the policy.

BACKGROUND / DISCUSSION

Information and the systems, networks and software necessary for processing confidential staff and tenant data must be appropriately protected against all forms of unauthorized access, use, disclosure, or modification. Policies and Procedures for YCH information and associated information technology (IT) assets which are owned, managed, operated, maintained, or in the custody or proprietorship of Yolo County Housing must be implemented to ensure privacy and confidentiality, data integrity, availability, accountability, and appropriate use.

The proposed YCH Information Technology Policy will establish standards for all departments. The policy defines:

a) Information Technology Operations (ITO) as the responsible party for all YCH information technology systems including servers, desktops, laptops, mobile devices, telecommunications equipment, file storage, passwords, remote access, email, software, and network management tools.
b) A formal working protocol on issues related to Information Technology for all YCH staff.
c) Established guidelines for use of Information Technology Systems remotely with reference to telecommuting options and business continuity planning.
d) Prohibited activities related to the use of YCH technology systems, equipment, and communication devices.

e) Established guidelines for use of Information Technology Systems remotely with reference to telecommuting options and business continuity planning.
f) Prohibited activities related to the use of YCH technology systems, equipment, and communication devices.
g) Allowable and prohibited uses of social media in conjunction with YCH business. This section includes authority to post articles or information to the social media site; employee guidelines for social media use, and responsibility to adhere to public laws and regulations.
h) Legal references for applicable federal, state, and local laws and regulations related to the administration of the Information Technology Policy.

Currently, the YCH has no IT or data management policy. With the increasing use of our website, increased deployment of computer and VOIP systems, as well as the rising use of social media, such as Facebook, the YCH should position itself to manage and safeguard its data. The proposed policy has been jointly developed by ITO and the Agency's Risk Manager to meet these evolving needs.

Features of the YCH Information Technology Policy will enhance YCH business practices in the areas of:

a) disaster preparedness and response;
b) business continued operations planning including telecommuting options;
c) using social media to market YCH programs and services, update the public through news articles, trends in affordable housing, and other related information;
d) providing a vehicle for tenants, landlords, and the public to provide feedback; and
e) outlining clear guidelines and expectations of YCH employees when utilizing YCH electronic equipment, internet, and information technology resources.

Staff has met and conferred with union representatives regarding this proposed policy.

FISCAL IMPACT

None at this time. However, damage, data loss or theft could have serious future financial implications for the Agency.

CONCLUSION

Staff recommends approval of the Yolo County Housing Information Technology Policy.

Attachment: Yolo County Housing Information Technology Policy

Yolo County Housing

2010 Information Technology Policy

Adopted on _____ by

Yolo County Housing Board of Commissioners

YOLO COUNTY HOUSING

INFORMATION TECHNOLOGY POLICY

Table of Contents

VIII. Prohibited Activities (cont'd)

- **I.** Degrading bandwidth
- **J.** Making unauthorized changes to databases
- **K.** Unauthorized long distance calls
- **L.** Moving, altering, replacing I.T. or T-Com equipment

VIV. Enforcement

Attachment I - *Employee Certification and Receipt of IT Policies and Procedures*

YOLO COUNTY HOUSING

INFORMATION TECHNOLOGY POLICIES & PROCEDURES

I. PURPOSE

The Information Technology Policy (the "Policy") outlines the expected code of conduct associated with access, acceptable and prohibited use of all technology systems, equipment and communication devices issued by Yolo County Housing (YCH) and/or used to conduct YCH business. Employees should not expect any right to privacy as it relates to the physical equipment, systems, and/or the content of communication created, sent, received, stored and used, while on YCH time and/or conducting YCH business. Further, YCH reserves the right to monitor, audit and/or otherwise scrutinize both content and equipment at any time for any reason including when there is a reasonable suspicion that employee use of any YCH technology systems, equipment and communication devices violates YCH policy.

All YCH issued electronic equipment including, but not limited to: hardware, software, email systems, Intranet, Internet connections, telecommunication systems, laptops, cell phones, or such similar technological communication devices and all content created, stored, sent and/or received are the sole property of YCH and thereon to be solely used for official business purposes.

At all times, YCH technology platforms are to be used in compliance with internal policies and all local, state and federal statutes. Failure to comply with these policies may result in disciplinary action in accordance with the applicable Collective Bargaining Unit Agreements and/or the YCH Personnel Policy and Procedure Manual.

All employees will be required to execute an Employee Certification of IT Policies and Procedures, which will be filed and maintained in the employee's Personnel file.

II. DEFINITIONS OF TECHNOLOGY TERMS

BlackBerry: A cellular phone marketed primarily for its wireless email- handling capability.

Blog: A website with regular entries of commentary, descriptions of events, or other material such as graphics or video.

Communication Devises: Telephones, two-way radio, etc.

Desktop: PC, personal computer, workstation, etc.

Domain Name: A domain name is the way to identify and locate an address on the Internet, for example, johndoe@ycha.org. The domain name is used to send e-mail, make FTP requests, locate a website, etc.

Drive: A location on the YCH network where official YCH business files are saved and stored.

Electronic Mail: Email; a means of sending text messages, pictures and attachments between computers using a computer network (internal) or the Internet (external).

File Transfer Protocol (FTP): Commonly used to upload or download programs and other files to a computer from other servers via a secure FTP connection.

G Drive and S Drive: A department's shared drive where data is saved.

H Drive:: An employee's personal drive where data is saved.

Hacking: Attempting to break into a network and/or server on which the violator has no authorized account.

Home Page: (or *Index* page): This is the first page that appears when a website is accessed. Usually has links to other pages on the same website or to other websites.

Information Technology (I.T.): YCH's array of network, hardware, software, and telephony resources that allows for the conduct of official business and the creation, sharing, and storing of files, emails and data.

Information Technology Operations (ITO): YCH's I.T. unit.

Information Technology Resources Request form (I.T.R.R. form): Found in the I.T. section of the YCH Shared Drive, this is the form to use when requesting information technology or telecommunications resources from ITO.

Internet: The Internet is a series of globally-interconnected digital networks, communicating through a common communications (Internet Protocol) language, by which data and e-mail may be digitally exchanged in near real-time. Also called: *World Wide Web.*

Intranet: YCH's internal website with departmental links for employees' use.

Malware: Harmful executable programs such as *viruses*, *worms*, *trojans* or *spyware* that are installed onto computers without the operator's knowledge.

PDA (Personal Digital Assistant): Any small mobile hand-held device that provides computing capability and information storage.

Peripheral: Electronic device attached to a desktop computer, such as a personal printer, all-in-one, etc.

Personal Identifiable Information (P.I.I.): Any piece of information which can potentially be used to uniquely identify, contact, or locate a single person, such as a client's or employee's social security number, address, driver's license, date of birth, etc. The inadvertent release or loss of such client information may cause harm to the interests of the client, the privacy of which is governed by various local, state and federal statutes, such as *Sarbanes-Oxley*.

Policy and Procedures: Primary computing policies of YCH as contained in this document.

RSA (Named after developers Rivest, **S**hamir and **A**dleman**):** An Internet encryption and authentication system that uses 'two-factor authentication', i.e. password-protected log-on and a security access token to allow secure remote access to YCH servers.

Server: A computer that provides services to other computers (and their users) on a network.

Smartphone: A wireless telephone set with special computer-enabled features.

Social Media: Social media is content created by individuals using accessible and scalable technologies through the Internet. Examples of social media include Facebook, blogs, MySpace, RSS, UTube, Second Life, Twitter, LinkedIn, Flicker, etc.

Streaming: Downloading compressed, bandwidth-intensive real-time audio and/or video from the Internet to a computer.

Superuser: YCH employees who possess and exercise a high level of ability with the YCH enterprise software systems, and assist in the training and supervision of employees who use those systems.

Trojan: A malicious computer program *hidden* in a seemingly harmless computer program or process for later destructive use on a computer. See *Malware*.

Ultra Mobile Personal Computers (UMPC): Very small, portable personal computing devices.

Vendor: Any private person or business enterprise.

Virus: Destructive computer code surreptitiously installed onto a computer via an 'infected' email or web page. See *Malware*.

Web Page: A single page on the Internet (as displayed by a web browser such as Microsoft's *Internet Explorer*).

World Wide Web (WWW): That part of the Internet which allows the publishing of information to a world-wide audience.

Worm: Self-replicating computer virus. See *Malware*.

III. EMPLOYEE RESPONSIBILITY

It is the responsibility of every employee to follow the directives as outlined and described throughout this Policy and maintain compliance as it relates to acceptable and prohibited use of YCH information, systems, equipment, devices, and the contents thereof. All YCH technology systems, equipment and communication devices are intended for YCH business only.

IV. Manager/Supervisor Responsibility

YCH managers and supervisors shall play an active role in educating YCH employees, temporary employees and subcontractors about the proper use of YCH information technology systems, Intranet and Internet connections.

1. Managers/Supervisors are responsible for supervising his or her employees' use of all YCH information technology systems, the intranet, and the Internet connection.

2. Manager/Supervisors are also responsible for the informational content of their departments' communications, Internet and/or intranet web pages.

3. Violations of this policy shall be reported to the next immediate supervisor/manager of the employee who committed the violation.

4. Managers/Supervisors shall not modify or suspend any terms or conditions of this Policy without written consent of the Executive Director.

V. YCH Information Technology Systems

A. Network Access - Employee access to the YCH network requires an approved *Information Technology Resources Request* form (I.T.R.R. form), submitted to ITO (Information Technology Operations).

B Software Systems - Access to email, the TenMast system, etc. requires an approved *I.T.R.R.* form, submitted to the ITO. Temporary employees

and volunteer staff may be limited in their access to YCH software systems depending on their function/capacity.

Superusers (see Definitions of Technology Terms) are those YCH employees (typically, non-ITO staff) who oversee system modules in the YCH's enterprise software systems.

They assist in the training and supervision of employees who use those systems. Superusers must approve the levels of system access granted to employees in their respective modules.

Superusers shall undertake continuous ongoing training provided by YCH in their respective modules to stay current.

C. Servers – YCH servers are to be maintained and administered by qualified YCH ITO staff *only*. No system administrator or database administrator rights shall be assigned to anyone except to ITO staff, authorized 3rd party technical consultants working on behalf of ITO, or to temporary, qualified designees. Designees shall be determined by the Executive Director on a case-by-case basis.

D. Desktop Computers – Only ITO staff will have administrative privileges on YCH desktops & laptops, with certain 'business-justified' exceptions determined by the Executive Director. All desktops deployed in YCH offices shall be a standard model for all, unless a special technical need can be demonstrated for a computer with greater memory, computing power, specialized software, etc.

1. Desktop Computers shall be used for the purpose of carrying out YCH business only.

2. Employees are encouraged to shut down their computers at the end of the day.

E. Mobile Devices - The following stipulations apply: The authorized issuance of laptops, smaller portable computing devices such as cell phones, BlackBerrys, SmartPhones, PDA's, and similar, successive technologies, etc. to employees requires an approved I.T.R.R. form signed by the Executive Director, submitted to ITO. Non-approved devices shall not directly connect to the YCH network. All YCH mobile devices shall be pass-code or password-protected at all times, on or off YCH premises. All device users shall cooperate with I.T. policy and enable their devices to be password protected.

1. Those employees approved and/or required to use communication devices shall be required to go through ITO for requisition and approvals.

2. Mobile devices shall be operated according to the YCH Distracted Driver Policy.

3. Staff who have been approved by the Executive Director to utilize their personal devices (i.e. cell phone, laptop, etc.), in lieu of receiving a YCH issued phone or device, for YCH related business will receive the following stipends:

   a. Cell Phones with access to YCH e-mail databases - $40/month.
   b. Remote access to YCH Server to conduct YCH business - $20/month, **or**;
   c. Access to the Corporate account if it is determined that it is in the best interest of YCH to establish a corporate account.

This determination will be on a case-by-case basis and substantiated by "business necessity". In the event of a disaster, IT protocols outlined in the YCH Business Continuity Plan will take precedence (Reference Business Continuity Plan).

The YCH Executive Director will provide a list of individuals receiving above defined stipends to the Board of Commissioners for review annually.

F. Peripherals – A request for a personal printer or other non-networked peripherals requires an approved I.T.R.R. form.

G. Telecommunications Equipment & Services - All land lines and cellular telephones, long distance service, fax lines, DSL service, etc. require an approved I.T.R.R. form. Only ITO is authorized to order these services and equipment and obtain approval from the Executive Director. Any exceptions for the purchase of equipment on an emergency, shall be reviewed by ITO and/or the Executive Director on a case by case basis. YCH reserves the right to terminate YCH cell phone accounts. Unless otherwise approved in writing by the Executive Director or designee, YCH issued cell phones shall not be enabled for internet, texting, file download, etc.

H. Saving Data & Files –All YCH employees shall save work-related data and files to their departments' respective H and S drives, *not* to the *C* drives of desktop computers or laptops. ITO cannot be responsible for data and files saved to a C drive. Unsaved changes to open files in open applications will be lost.

I. Portable Memory Storage Devices – Only ITO-approved portable memory storage devices (also known as thumb drives, mini drives, memory sticks, etc.) will be allowed for use on YCH own/leased equipment. All ITO-issued portable memory storage devices shall be encryption-enabled to prevent unauthorized users from accessing data.

J. Passwords - Employees are responsible for all activity performed with individual user-IDs and passwords. User-IDs and passwords may not be utilized by anyone but the individual to whom it has been issued. Sharing passwords is prohibited in all YCH internal systems (Tenmast etc.). Passwords for access to external non-YCH systems and Internet websites (including use of login name and passwords) may be utilized with approval from the Department Head or their designee. The below guidelines shall be followed in the selection and maintenance of passwords:

1. Unique user-ID and password are required.

2. Passwords must be a minimum of 6 characters long.

3. Systems shall not be set to remember passwords.

4. Password reminders such as notes shall not be placed anywhere they can be easily found, such as under or on phones, keyboards, PCs, monitors, mouse pads, desktops, etc.

5. Employees should refrain from using the same passwords on multiple systems to avoid compromise of other systems when one system is compromised.

6. After multiple incorrect logon attempts, employees will be locked out for a predetermined period of time.

7. Password change requests shall be processed over the telephone; managerial verifications will have to be provided for password changes to be made.

K. Remote Access - Remote access (from offsite locations) to the YCH network shall be awarded on a case-by-case basis, and requires an approved I.T.R.R. form. Remote access shall require a two-step authentication process, using an RSA (remote access) token and a password, and/or other security techniques.

L. Network Management Tools – These tools are to be used by ITO staff and authorized designees only. Security flaws are not to be tested by anyone other than members of ITO. Security concerns shall be forwarded to ITO and/or the Executive Director for resolution.

M. Email - Employees shall use professional etiquette when composing emails. Email system is not to be used for the creation or distribution of any offensive or disruptive message, including messages containing offensive comments about race, gender, sexual orientation, profanity, pornography,

religious or political beliefs, national origin, disability, or "chain" emails. Unlawful messages, such as emails that infringe on copyright are also prohibited.

The size of email attachments shall be regulated by the ITO to ensure the smooth operation of email systems. ITO will address issues and technology changes as they become evident.

PII (Personal Identifiable Information) shall not be emailed outside the confines of the YCH network(s). This prohibition also applies to the *forwarding* of official YCH files, data, etc. to personal email accounts.

If an employee is receiving unwanted and unsolicited emails, the employee shall report this activity to his/her Supervisor, the Resource Administrator, or the IT Manager. YCH will investigate each incident as necessary.

N. Email Disposition - YCH email systems are not designed to be 'storage systems'. Employees may be notified to purge their email to allow for continued communications.

VI. YCH Intranet & Internet

The YCH Intranet (internal) site, its public website and Internet connection are fundamental communication tools for providing timely and critical YCH information to employees, to increase public awareness of YCH programs, and to facilitate the agency's mission and program goals.

The use of YCH websites and Internet connections are for official business use only. Do not use YCH technology systems, equipment and communication devices for personal use.

All administrative, design, policy and technical questions regarding the YCH Intranet site and Internet website shall be directed to the IT Manager.

Requests for Access - Departmental requests for access to the Internet must be signed by departmental directors on behalf of the requestor and submitted to ITO for approval. Requests shall be made on the I.T.R.R. form. Requests must also describe the desired level of access as well as the intent (business case) for the access.

VII. Social Media

Yolo County Housing may use social media and social network sites to further enhance communications with various stakeholder organizations in support of YCH goals and objectives. Department managers and supervisors have the ability to publish articles, facilitate discussions and communicate information through various media related to conducting YCH business. Social media

facilitates further discussion of YCH issues, operations and services by providing members of the public with the opportunity to participate in many ways using the Internet.

A. All YCH social media sites shall be (1) approved by the Executive Director and the IT Manager; (2) published using approved YCH social networking platform and tools; and (3) administered by the IT manager or their designee.

B. All social network sites and entries shall clearly indicate that any articles and any other content posted or submitted for posting are subject to public disclosure.

C. YCH reserves the right to restrict or remove any content that is deemed in violation of this IT Policy or any applicable law.

D. Each YCH social networking site shall include an introductory statement which clearly specifies the purpose and scope of the social network site and/or blog. When possible, social networking sites should link back to the official YCH website for forms, documents, and other information.

E. YCH social networking content and comments that contain any of the following shall not be allowed for posting:

1. Comments not topically related to the particular site or article being commented upon;
2. Profane language or content;
3. Content that promotes, fosters, or perpetuates discrimination on the basis of race, ethnicity, creed, color, age, religion, gender, marital status, status with regard to public assistance, familial status, physical or mental disability, or sexual orientation;
4. Sexual content or links to sexual content;
5. Solicitations of commerce;
6. Conduct or encouragement of illegal activity;
7. Information that may tend to compromise the safety or security of the public or public systems; or
8. Content that violates a legal ownership interest of any other party.

F. All social networking sites shall clearly indicate they are maintained by YCH policy and shall have YCH contact information prominently displayed.

G. YCH IT security policies shall apply to all social networking sites and articles.

H. YCH employees and Board members representing YCH via social media outlets must conduct themselves at all times as a representative of YCH and in accordance with all human resource and Board policies.

I. YCH understands that social networking and internet services is a common form of communication in the workplace and among stakeholders and citizens. If employees or Board members choose to participate in social networks **as a YCH employee or YCH Board member**; you should adhere to the following guidelines:

1. YCH policies, rules, regulations and standards of conduct apply to employees that engage in social networking activities while conducting YCH business. Use of your YCH e-mail address and communicating in your official capacity will constitute conducting YCH business.
2. The YCH Executive Director or designee has the option of approving or disallowing employees to participate in existing social networking sites as part of their job duties.
3. Protect your privacy, the privacy of citizens, and the information that YCH holds. Follow all privacy protection laws, i.e. HIPPA, and protect sensitive, confidential information.
4. Follow all copyright laws, public records laws, retention laws, fair use and financial disclosure laws and any other laws that might apply to YCH or your functional area.
5. Do not cite vendors, suppliers, clients, citizens, co-workers or other stakeholders without their written approval.
6. Make it clear that you are speaking for yourself and not on behalf of YCH. If you publish content on any website outside of YCH and it has something to do with the work you do or subjects associated with YCH, use a disclaimer such as "The postings on this site are my own and don't necessarily represent YCH position or opinion".
7. Do not use ethnic slurs, profanity, personal insults, or engage in any conduct that would not be acceptable in the YCH workplace. Avoid comments or topics that may be considered objectionable or inflammatory.
8. If you identify yourself as a YCH employee, ensure your profile and related content is consistent with how you wish to present yourself to colleagues, citizens and other stakeholders.
9. Correct your mistakes, and don't alter previous posts without indicating that you have done so.
10. Add value to YCH through your interaction. Provide worthwhile information and perspective.

VIII. PROHIBITED ACTIVITIES

YCH technology systems, equipment and communication devices are for YCH business only. In addition, it is against local, state, and federal laws to interfere with or disrupt the YCH network, servers, desktop computers, other network equipment, software systems or services. It also violates the policies of YCH. Such prohibited interference or disruption includes but is not limited to:

A. Hacking - Using the network to force unauthorized entry (*hacking*)

into other information technology network devices or resources. Unauthorized users shall not attempt to enter any server, workstation or computer with (or without) Internet access. Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. 2510.

B. Introducing Viruses - Introduction of computer viruses, worms or trojans into the YCH network.

C. Unauthorized Use of Personal Identifiable Information (P.I.I.) - Downloading, copying, emailing, transmitting, etc., YCH-owned data, material, information, or software in violation of any local, state or federal law or YCH policies.

D. Spamming - Distribution of unsolicited advertising via email.

E. Chain Emails - Chain emails are widely-distributed, non-business emails sent to dozens or hundreds of users. Creating, sending or forwarding chain emails is prohibited.

F. Sharing Passwords - Sharing network system passwords.

G. Connecting Personal Devices to YCH Network - Plugging in, or attaching personal electronic devices to the YCH network is strictly prohibited unless otherwise authorized in accordance with Section V-I.

H. Unauthorized Downloads - Downloading games, non-authorized programs, music, video; playing games using unauthorized programs on YCH desktops or laptops.

I. Degrading Bandwidth - "Diluting" bandwidth by streaming non-authorized audio, video, or web services that serve to cause network slowdowns for YCH users.

J. Unauthorized Changes to Databases - Making unauthorized changes/updates to any YCH database system. Making unauthorized changes to and/or deletions of any YCH data or files.

K. Unauthorized Long Distance - Making long distance calls, texting, accessing Internet pages (*non-email* portals) from YCH-issued mobile devices or from YCH land lines without approval.

L. Unauthorized I.T. Equipment Removal - Moving, altering, or replacing I.T. or telecommunications equipment without authorization of ITO is prohibited.

M. Prohibited Uses of Removable Storage - Use of *personally*

purchased portable memory storage devices on YCH premises is prohibited; exceptions will be addressed by department head or designee on a case by case basis. Removing YCH-issued portable memory storage devices from YCH premises is prohibited. The loading of P.I.I. (Personal Identifiable Information, please see *Definitions*) such as social security numbers, payroll information, etc. onto portable memory storage devices, as well as onto CDs, floppy discs, external drives, etc. is strictly prohibited.

VIII. Enforcement

A. External.

YCH shall follow all applicable federal, state and local laws and regulations related to the administration of this information technology policy. Some examples of the statutory supports of this policy are as follows:

1. Federal Information Security Management Act of 2002 ("FISMA") - consists of Title III of the E-Government Act of 2002 (U.S. Public Law 104-347) enacted into law at the close of 2002 which became effective on April 17, 2003. As per FISMA, "information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide –

a) integrity, which means guarding against improper information modification or destruction, and includes ensuring information…[authenticity];

b) confidentiality, which means preserving authorized restrictions on access and disclosures, including means for protecting personal privacy and proprietary information; and

c) availability, which means ensuring timely and reliable access to and use of information."

http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

2. Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C - This statute spells out the types of unauthorized electronic activities that are unlawful. Some examples are below.

Communication Interference (Denial of Service Attacks) - 18 U.S.C. §§. 1362 & 1030 (a)5(A)(i)

Privacy & Security - 18 U.S.C. §§ 2510 & 2511

Spamming - 18 U.S.C. § 1037

3. The Computer Fraud and Abuse Act (as amended 1994 and 1996) (18 U.S.C. §1030)- This federal statute governs those who: (5)(A)

(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss;

4. California Penal Code Section 502 - Prescribes penalties for damaging, deleting, destroying data and/or otherwise disrupting computer operations.

5. California Public Records Act ("CPRA"), Government Code Section 6250 - Requires the Housing Authority to make all public records available for inspection and to provide copies upon request.

B. Noncompliance

1. Failure to comply and/or willful violation of this I.T. policy may be investigated and may result in disciplinary action against the employee in accordance with the applicable Collective Bargaining Unit Agreement and/or YCH Personnel Policy and Procedure Manual. When applicable, should the employee also violate federal, state or local laws, YCH may notify the appropriate authorities and thereafter cooperate as requested.

2. Employees shall cooperate with any investigation regarding the use of YCH computer equipment and Internet usage.

Attachment I

YOLO COUNTY HOUSING

EMPLOYEE CERTIFICATION OF RECEIPT OF INFORMATION TECHNOLOGY (IT) POLICIES AND PROCEDURES

I certify that I have been trained, read and reviewed the YCH INFORMATION TECHNOLOGY POLICY. By signing this form, I acknowledge that these policies and procedures apply to me and I agree to comply with them.

Print name: _____

Signature:_____ Date:_____

cc: Employee Personnel File