**HOUSING AUTHORITY
COMPUTER NETWORK, PHONE, AND INTERNET USE POLICY**

Housing Authority information network resources are made available to the Authority's staff to improve communications and information exchanged with employees, tenants and others and to provide communication, information, and research resources. Certain restrictions are necessary to avoid improprieties and ensure that established standards are met. To reduce potential liability, the risk of inappropriate use, and possible adverse public perceptions, personnel shall use the provided phones, network and Internet for ***official Housing Authority business purposes only****.* information network resources, including email, are not to be used for entertainment, or for illegal, harassing, or libelous purposes.

All employees shall use the phones, Internet and E-Mail in a responsible manner. Use of electronic information resource is a **privilege**, not a right.

All phones, computer equipment and software is for business purposes only. The use of phones and computer equipment for regular personal reasons shall be prohibited. Computer equipment may not be used for video games, private chat rooms or similar entertainment endeavors.

**PROCEDURE FOR USE**

1. The Authority provides employees with phones and access to the Internet for the purpose
of fulfilling the Authority's mission of serving the Authority's clients. Uses are to be
related to the operations of the Authority.
2. The Authority phones and E-Mail accounts are owned by the Authority and therefore are not private. The Authority retains the right to review, audit, intercept, access and disclose all messages created, received, or sent over the electronic mail system as necessary.

RULES

(1) Employees shall:

* Use phones and computing equipment, software, and network access in a manner consistent with appropriate Authority policies.
* Be aware of and abide by copyright and licensing laws.
* Be sensitive to the security/safety issues related to publishing names, addresses, and pictures on the Internet.
* Protect tenant and landlord information, insure that it is not used inappropriately and does not fall into the wrong hands.

(2) Employees shall not:

* Interfere with the ability of others to make effective use of Authority phones, computing and network resources.
* Use any form of obscene, harassing, racist, sexist or abusive language or behavior on the phones or online or at any time.
* Send messages using someone else's name without consent.
* Read mail, delete, copy, or modify files created by others without permission from your supervisor, or other person designated as being responsible by the Authority.
* Intentionally access Internet sites containing hate materials.
* Forge or attempt to forge electronic mail messages and/or documents.
* Install any software, screensavers, and/or programs to their computers. Any needed applications must be approved and installed by IT personnel. Installation of third party screensavers is prohibited.
* Install any hardware without consent of IT personnel. This includes flash drives.
* Transfer in any manner any personal files to your computer. This includes, but is not limited to, transfers made by email, CD's, floppies or flash drives.

**E-MAIL USER RESPONSIBILITY**

The content and maintenance of a user's electronic mailbox and data folder is the user's responsibility.

1. Check E-Mail regularly.
2. Keep messages remaining in your E-Mail inbox to a minimum. Emails must be moved to your personal folders for storage.
3. Never assume that your E-Mail is private. It is not private and is not intended to be private. The administration can, and others may be able to, read or access your mail. Never send or keep anything that you would not mind seeing on the evening news.
4. Report any misuse of the E-Mail system to your supervisor immediately upon discovery.
5. Do not send / forward any external email not related to business without consent from your supervisor and IT personnel. This includes chain letters, jokes, hope letters, request for passing letters, etc.
6. Any document or email containing confidential information subject to the Privacy Act shall not be transferred outside of the computer network.

PERSONAL USE OF THE INTERNET

As with telephones, photocopiers, fax machines, and other technology supplied by the Authority, use ***of the Internet is for business purposes only*** and must be conducted in compliance with Authority policies.

USER ACCOUNT PASSWORD POLICY

It is imperative that users practice due diligence in controlling access to their computer system and the computer network, by protecting their user accounts with passwords which are not easily guessed or deduced. This policy is intended to reduce the risk of unauthorized access to confidential information. The following principles apply:

user account passwords must be at least eight (8) non-blank characters in length and must contain characters from three of the following four categories: capital letters, lower case letters, numeric characters 0 thru 9 and non-alphabetic characters for example, !, @, #, $ ,%. Must be changed at least once every 45 days, and cannot be the same as the past four (4) passwords.

Computer systems will lock-out a user's account after six (6) failed attempts within 30 minutes to login with a wrong password. Account lock-out duration is one (1) hour or until reset by an authorized administrator.

If an account is inactive for more than 180 days, the account is automatically locked and must be reactivated by IT personnel.

When users will be away from their systems for more than 30 minutes, the systems must be either locked or logged off.

Saving passwords to the system, and using automatic logins is prohibited. Storing passwords in files on the user's system is also prohibited unless the file is encrypted. Passwords are not to be written down and stored on paper.

Providing your password to someone else to use, or utilizing another user's password is prohibited and could result in disciplinary action up to and including termination. Never give your passwords to anyone for any reason. IT personnel or administrative staff will never ask for your password. If someone asks for your password, refer them to this policy and let IT personnel know.

**HARASSMENT, DEFAMATION AND INVASION OF PRIVACY**

Downloading and displaying or disseminating materials which may be considered by some people to be racist, sexist, defamatory or otherwise offensive, or which may invade another person's privacy, may constitute harassment by creating a hostile work environment. This is no different from telling racial jokes or displaying a "pin-up" calendar in the office. Such actions are expressly forbidden. Moreover, they may subject both you and the Authority to legal action.

Downloading or viewing of materials of a racist, sexist, defamatory or otherwise offensive nature, or which constitute an invasion of another person's privacy, is **STRICTLY PROHIBITED.** All such materials and actions are subject to the Authority's harassment policies.

**VIOLATIONS OF POLICY**

While all Authority employees serve on an **"at will"** basis, employees are expressly advised that violations of these procedures or rules will result in appropriate disciplinary action up to and including written reprimand, suspension without pay, and discharge.

**Please refer to the U. S. Department of Housing and Urban Development Notice PIH-2014-**
**10 issued April 30, 2014 and its successors regarding Privacy Protection Guidance for
Third Parties.**

HOUSING AUTHORITY
ACKNOWLEDGEMENT OF RECEIPT
OF
'S

REVISED COMPUTER NETWORK, PHONE, AND INTERNET
USE POLICY

Signing this form acknowledges that the employee has received a copy of the Housing Authority's Computer Network, Phone and Internet Use Policy and adopted by the Board of Commissioners on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ as Resolution No. \_\_\_\_\_\_\_\_\_\_\_.

By my signature below, I acknowledge that I have received a copy of the revised Computer Network, Phone, and Internet Use Policy. I understand that it is my obligation to read, understand and comply with the revised policy and that violation of this revised policy may result in discipline up to and including termination.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name of Employee Employee Signature

Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_