Technology Policy

Housing Opportunities Commission
Of Montgomery County

HOC

Originated: April 2003
Revised: April 2006

Housing Opportunities Commission (HOC)
Technology Policy

Table of Contents

Housing Opportunities Commission (HOC)
Technology Policy

Table of Contents

I. Introduction

Information technology systems and networks are an integral part of business at the Housing Opportunities Commission of Montgomery County, Maryland. The Agency has made a substantial investment in human and financial resources to provide business processes and infrastructure support.

The **HOC Technology Policy has been established** in order to:

- Protect **HOC's** investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect the **reputation of the Commission**

Application

This policy applies to all HOC employees and other users (temporaries, contractors, volunteers, etc.) of HOC technology related resources .

Administration

The Director or Information Technology is responsible for the administration of this policy.

Contents

The topics covered in this document include:

- Electronic Systems
- Network Security
- Password Security
- Computer Software Guidelines
- E-mail and Internet Usage Guidelines
- Application Security
- Cell Phone Usage and Guidelines

Statement of Responsibility

General responsibilities pertaining to this policy are set forth in this document. The following lists additional specific responsibilities.

Staff Responsibilities

- Comply with all technology policies contained within the Information Technology Policy

Management Responsibilities

Division Directors and Supervisors Must:

- Ensure that all personnel are aware of and comply with this policy.

- Create performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

- Request all technology related services through the Information Technology Division.

Director of Information Technology Responsibilities

The Director of Information Technology shall:

- Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.

- Provide support and guidance to assist users to fulfill their responsibilities under this directive.

- Provide or designate final approval authority for all technology related requests.

Violations

Violation of this policy may result in disciplinary actions up to and including termination. HOC reserves the right to recover costs attributable to the unauthorized or inappropriate use of the Information Technology related systems from the responsible employee. In addition, HOC reserves the right to take legal action if so warranted. Violations of this policy by users should be reported to the violator's supervisor and the Director of Information Technology. Questions regarding appropriate uses should also be directed to supervisors or the Director of Information Technology.

II. Electronic Systems

A. Purpose

The purpose of this section is to establish the policy and procedures relating to electronic communications (defined as: *All electronic communications, including but not limited to, E-mail, Voice mail, Internet, Intranet, World Wide Web Access; telephone and cellular communications; facsimile communications; and data files*) and the use of electronic devices (defined as: *All electronic communications devices, including but not limited to, facsimile (fax) machines; computers, computer peripherals; printers; telephones, cellular phones; and pagers*).

All components of electronic systems and the data stored on them are the property of HOC and all electronic communications composed, sent or received are and remain the property of HOC. All electronic communication systems are provided solely for use in conducting HOC business. HOC reserves the right to access and disclose the contents of all electronic communications and/or data created, sent, received or stored using any of its electronic systems. HOC maintains electronic systems (defined as: *All electronic communications and electronic devices*) to assist in the conduct of HOC business.

B. Policy

1. Privacy and Security

HOC electronic systems are used to conduct HOC business. As such, the communications and data stored on them may be accessed by an individual other than the intended recipient or owner. HOC reserves the right to retrieve and read any electronic communication composed, sent, received or stored on any HOC electronic system. HOC also reserves the right to monitor the usage of all technology -related activities covered under this policy.

2. Usage

All electronic communications are to be handled in the same professional manner as hard copy letters, memoranda or other business communications. Electronic systems shall be used solely for the performance of duties and responsibilities of a user's work program. No copyrighted or HOC proprietary information is to be distributed by HOC e-mail or electronically published without prior written approval from your supervisor.

All electronic communication systems shall be used for HOC's business purposes as follows:

- activities related to HOC or departmental missions;
- activities related to official assignments and job responsibilities;
- job-related communications, such as networking and collaboration;
- research in connection with official duties;
- responding to approved public access mandates or directions.

3. Prohibited Uses or Conduct

Use of the electronic systems for activities unrelated to HOC business is prohibited. This includes but is not limited to:

- activities of a personal, commercial, religious or political nature;
- unauthorized advertising, broadcasting, or message sending;
- use for private enterprise, including marketing of products or services, business transactions, personal financial gain for self or others; and ,
- solicitation for religious and/or political causes.

Electronic communications are to reflect professional business standards and should not be of an offensive content. Offensive content includes but is not limited to:

- abusive, obscene or harassing language or images;
- racial, ethnic, sexual or gender specific comments or images;
- comments or images that are false, inflammatory or disparaging or are negatively based on religious or political beliefs, sexual orientation, national origin, age, disability.

Prohibited conduct related to electronic systems includes, but is not limited to:

- unauthorized access, or attempted access, to computer-based records or services;
- unauthorized changes to the electronic systems including changing the software and hardware settings;
- unauthorized use or disclosure of data protected by federal, state or county laws or HOC regulations;
- violations of federal, state, local or HOC laws or regulations with regard to copyright, software license agreements, and information services contracts, including unauthorized duplication of software, files, operating instructions or reference manuals;
- propagation of computer viruses;
- installation of HOC-owned software, or accessing contracted information services, on personal computing equipment
- removal of HOC-owned electronic communication equipment or devices from assigned locations
- encryption of any sort on HOC equipment or devices
- sharing passwords or allowing a user access to a software or function for which he or she does not have rights;
- installation of hardware or software not approved by the Director of Information Technology.

It is recognized that occasional and incidental personal use may be necessary. However, such activities are subject to the scrutiny consistent with the intent of policy and shall not interfere with performance of users' duties and responsibilities. Such use would include electronic mail and/or voice mail to communicate employee news such as births, serious illnesses, deaths, or HOC-sponsored activities.

4. Electronic Devices

Users are responsible for assuring the physical safety of all electronic communication devices taken off HOC premises. Users are responsible for any lost or broken equipment when the equipment is not on HOC premises. No modification to any HOC electronic communications devices is allowed regardless of the location of the equipment.

III. Network Security

A. Purpose

The purpose of this section is to establish the policy and procedures relating to network security. HOC provides access to electronic resources and communications systems such as the Internet, electronic mail, voicemail, file servers, and the local and wide area networks, to authorized employees to facilitate business-related tasks.

The integrity of HOC's electronic information is critical to HOC accomplishing its mission. Electronic information is subject to attack from many places, including viruses, hackers, and internal sources. All HOC employees share the responsibility of securing HOC's electronic information. The following policy provides the framework by which all HOC employees will help to insure the integrity of HOC's electronic data.

B. Policy

1. System Access Form

A System Access Form must be completed for each new employee or other user requiring access to the HOC network, or for current employees requiring access to additional network resources. The form must be approved by the employee's direct supervisor.

2. Default New User Access

By default, each new user will be given an e-mail account and a home directory on the network. They will also be given access to public areas of the HOC local area network (LAN) (such as the Intranet, and public group folders) and access to their departmental "groups" folder. Any other access (including access to the Internet), must be specifically requested, on the System Access Form.

3. Network Storage

HOC network file storage is organized into shares (folders), according to business function. There are certain "public" areas of the LAN that all employees are allowed access. Other shares are restricted according to business function. Users must not attempt to access network shares to which they have not been authorized. If a user finds that they have access to a share to which they should not have access, they must report their findings to the IT Division immediately.

All HOC business-related data must be stored on a share on the HOC LAN (not on the local desktop computers). Users are responsible for storing confidential information in the appropriate, secured area on the LAN. If you are unsure of where to store a particular file, please contact your direct supervisor.

There is a limited amount of storage space on HOC servers. If you have stored information that has not been accessed in some time, please contact the IT Help Desk about having the data archived.

4. Desktop Security

Before leaving a computer unattended, users must either log ou t of the HOC LAN, or lock their computer. This will prevent an unauthorized individual from accessing the HOC network via your account. Computers that are idle (or left unattended) for ten minutes, will be automatically locked.

Desktop equipment is not t o be moved to another location, either within or outside of HOC, without the written approval of your direct supervisor, and the Director of Information Technology .

You may not install any hardware or software on to your HOC -supplied workstation which has not been approved, in writing, by the Director of Information Technology .

5. Remote Access

It is possible to connect to the HOC network from home via direct dial -up, and via most Internet Service Provider s (using a VPN client) .

Permission to access the HOC network in this fashion is not granted by default. It must be requested and approved via the Remote Access Request Form. Remote Access Request forms must include adequate justification for remote access, and be approved by the users' direct supervis or and division Director. If approved, remote access is granted until the end of that calendar year.

At the end of each calendar year, all remote access users must resubmit a Remote Access Request form, for re -approval. Users who fail to submit a new for m will have their remote access privileges revoked.

For remote access to the HOC network, users may use an HOC -assigned computer (from the HOC computer inventory) or they may wish to supply their own. User-supplied computers must be brought to the HOC IT Division to be examined and approved for connection to the HOC network. Computers must meet the following criteria for approval:

- Computers must be running an approved Operating System. As of the time of the preparation of this document, the approved Op erating Systems are:
  - Windows 2000 Service Pack 4 or later
  - Windows XP Service Pack 2 or later
- Computers must be running a real -time anti-virus scanner, such as E - trust Antivirus or Norton Antivirus. The Antivirus scanner must be configured to automatically update its virus definition files at least weekly.
- Computers must be running a real-time malware protection product, such as the SpyBot Search and Destroy SDHelper.
- Computers must require authentication (i.e. computers may not be set to login in automatically on startup).
- Computers must be protected by either a hardware or software -based firewall, when connected to the Internet.

Computers determined to be unsuitable will not be permitted to connect to the HOC network. Users will have to make other arran gements to connect. Users found attempting to connect an unapproved computer to the HOC network will be subject to loss of remote access rights, and other disciplinary actions up to and including termination of employment.

Computers which are examined, and meet the preceding requirements will be approved for remote access to the HOC network. The user will be provided with written verification.

Approved computers will be examined and the end of each calendar year to determine their continuing eligibility for connection. Computers which are not brought in for re-examination, or fail re-examination, will not be permitted to connect to the HOC network.

When accessing the HOC network from home the following rules must be followed:

- Do not leave a computer unattended, while it is logged into the HOC network.
- Always log off the HOC network when you have completed your task.
- Any computer you use to login to the HOC network (even a user-supplied computer) is subject to the same guidelines (including anti-virus, monitoring, privacy, etc.) as the computers at HOC locations.

Failure to follow these rules me result in the loss of remote access rights, and other disciplinary actions up to and including termination of employment.

6. Portable Equipment

HOC users may be assigned certain portable equipment (such as laptops, PDA's digital cameras, etc.) depending on their business requirements. Use of such equipment is subject to the following guidelines:

- Portable equipment must be physically secured when not in use.
- Portable equipment must not be checked in airline luggage systems.
- Whenever HOC confidential information is stored on portable media, such as a floppy disk, that media must be secured at all times.
- Portable equipment is subject to the same guidelines (including anti-virus, monitoring, privacy, etc.) as the computers at HOC locations.
- Any incident involving the theft, loss, or damage of HOC-owned portable equipment must be reported to your direct supervisor, and the HOC IT division immediately. A police report should be filed when appropriate.

7. Security devices

HOC has installed security and monitoring devices to assure the security and safety of our network (such as firewalls, proxy servers, etc.). Any employee who attempts to disable, defeat, or circumvent these devices will be subject to disciplinary action, up to and including termination.

8. Data Center

To insure the security of HOC's electronic data, all HOC network servers are stored in the HOC data center. No server may be maintained outside of the HOC data center without the written permission of the Director of Information Technology.

Access to the HOC data center is restricted to HOC IT and HOC Facilities division employees as well as the HOC Executive Director and Chief of Staff.

9. Backups

To protect HOC information resources from loss or damage, all HOC file and database servers are backed up regularly, according to the published HOC backup guidelines. Typically, workstations are not backed up.

To assure the safety of HOC business-related information, all HOC business-related information must be stored on the appropriate network share. Data stored on local hard drives ("C" drives) is not protected in case of disaster or computer failure.

HOC backup data is stored in a secure facility offsite, for a period of at least six months. Users may request that lost files be restored via the IT Help Desk.

10. Employee Privacy and Encryption

All messages created; sent or retrieved through HOC's electronic resources and communications systems, as well as any data stored on these systems, are the property of HOC regardless of content. HOC reserves the right to access and monitor its employees' usage of the agency's electronic resources and communications systems, such as the Internet, e-mail, and voicemail, including reviewing a list of sites accessed by an individual without prior notice to the employee. HOC will comply with reasonable requests from law enforcement agencies for information (including log files) on individual's activity. No employee should have any expectation of privacy in terms of their usage of the electronic resources or communications systems. Thus, even though employees must maintain passwords for accessing such resources, employees must not expect that any information transmitted, received, or maintained through these resources is private.

The use of data encryption is forbidden, without written permission from the Director of Information Technology.

11. Antivirus

A computer virus is an unauthorized program that replicates itself, attaches itself to other programs, and spreads onto various data storage media and/or across a network. Viruses may spread via the network, shared diskettes or via e-mail. Symptoms of virus infection may include much slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sized, and total failure of computers.

To assure continued, uninterrupted service for both computers and networks, all HOC workstations are provided with approved virus screening software, and all HOC servers run screening software as well. HOC also filters out suspicious and dangerous incoming e-mail attachments. Anti-virus definition files are updated weekly.

Users may not attempt to disable or bypass the anti-virus screening software.

Contact the IT Help Desk immediately if:

- You believe that your computer has been infected with a virus.
- Your computer exhibits any of the symptoms listed above.
- You receive a suspicious computer file.
- You receive an e-mail attachment from someone you do not know.

- You receive an e-mail attachment you were not expecting.
- You suspect that your anti -virus scanning software is not functioning.

Always play it safe: never open or attempt to run a computer file of which you are unsure. Instead, contact the IT Help Desk, or simply delete the file.

IV. Password Security and Account Lockout Policy

A. Purpose

The purpose of this section is to establish the policy and procedures relating to password security. Passwords are an important aspect of computer security. They are the front line of protection for user accounts and agency data. A poorly chosen password may result in the compromise of HOC's entire corporate network. As such, all HOC employees are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

B. Policy

1. Password Selection Policy

Passwords are used for various purposes at HOC. Some of the most common uses include: user network accounts, and voicemail accounts. Users must use the following guidelines for selecting passwords:

- Passwords must be at least six (6) characters long.
- Passwords will expire every 90 days .
- Users must select different passwords for different HOC systems.
- A password history of five (5) will be kept, meaning that a user may not reuse one of his or her previous five (5) passwords.
- Passwords must meet the following complexity requirements :
    - Passwords must contain at least one character from three of the following four categories:
        - I. English uppercase characters
        - II. English lowercase characters
        - III. Numerals
        - IV. Non alphabetic characters (such as !, $, #, %)
    - Passwords may not contain your username, or any part of your full name.

2. Securing your passwords

After selecting a suitable password, do not minimize its value by failing to protect it. Never share you passwords with anyone. All passwords are to be treated as HOC confidential information. Users must adhere to the following guidelines for securing their passwords:

- Don't reveal a password over the phone to ANYONE.

- Don't reveal a password in an e -mail message, or any other form of electronic communication.
- Don't reveal a password to your supervisor, co-worker, subordinate, or IT Division employee.
- Don't talk about a password in fro nt of others.
- Don't hint at the format of a password.
- Don't share a password with family members.
- Don't use the "remember password" option in applications.
- Do not write any passwords down and store them in your office.

If anyone demands a password, refer them to this document, or have them contact the Director of Information Technology.

If you suspect an ac count or password has been compromised, change the suspected password, and report the incident to IT as soon as possible.

The Information Technology division reserves the authority to reset passwords for business necessity when required.

Password audits ma y be performed periodically by the IT department, where an attempt is made to guess or "crack" passwords. If a password is guessed during one of these audits, the user will be required to change it immediately.

3. Account Lockout Policy

While attempting to l og on to the HOC network, If a user types his or her password three times incorrectly, that user's account will be locked out until they contact the OT Helpdesk to have it unlocked.

V. Computer Software Guidelines

A. Purpose

The purpose of this section is to establish the policy and procedures relating to computer software guidelines. It is the policy of HOC to respect all computer software copyrights and to adhere to the terms of all software licenses to which HOC is a party. HOC will take all steps necessary to prohibit users from duplicating any licensed software or related documentation for use either on HOC premises or elsewhere unless HOC is expressly authorized to do so by agreement with the licensor. Unauthorized duplication of software may subject users and/or HOC to both civil and criminal penalties under the United States Copyright Act.

Misuse of software in any manner inconsistent with the applicable license agreement, including giving or receiving software or fonts to or from clients, contractors, customers and others is prohibited.

B. Policy

1. Acquisition of Software

All software acquired by HOC must be purchased through the IT division. Software acquisition channels are restricted to ensure that HOC has a complete record of all software that has been purchased for HOC computers and can register, support, and upgrade such software accordingly. This includes software that may be downloaded and/or purchased from the Internet.

2. Registration

When HOC receives the software, the IT Division must receive the software first to complete registration and inventory requirements before installation. In the event the software is shrink-wrapped, the IT Division is responsible for completing the registration card and returning it to the software publisher. Software must be registered in the name of HOC and the department in which it will be used. The IT Division maintains a register of all HOC's software and will keep a library of software licenses.

3. Installation of Software

After the registration requirements above have been met, the software will be installed by the IT Division. Once installed, the original media will be kept in a safe storage area maintained by the IT Division. User manuals, if provided, will either reside with the user or reside with the IT Division.

4. Home Computers

HOC's computers are Agency-owned assets and must be kept both software legal and virus free. Only software purchased through the procedures outlined above may be used on HOC's machines. Users are not permitted to bring software from home and load it onto HOC's computers. Generally, Agency-owned software cannot be taken home and loaded on a user's home computer if it also resides on HOC's computer. If a user is to use software at home, HOC will purchase a separate package and record it as an Agency-owned asset in the software register. However, some software companies provide in their license agreements that home use is permitted under certain circumstances. If a user needs to use software at home, he/she should consult with the software man ager to determine if appropriate licenses permit home use.

5. Shareware

Shareware software is copyrighted software that is distributed via the Internet. It is the policy of HOC to pay shareware authors the fee they specify for use of their products. Under th is policy, acquisition and registration of shareware products will be handled the same way as for commercial software products.

6. Biannual Audits

The software manager or designated department will conduct a bi annual audit of all HOC's PCs and servers, inclu ding portables, to ensure that HOC is in compliance with all software licenses. Surprise audits may be conducted as well. Audits will be conducted using an auditing software product. The full cooperation of all users is required during audits.

7. Employee Usage Guidelines

Software will be used only in accordance with its license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup and archival purposes by the IT Division, is a violation of copyright law. In addition to violating copyright law, unauthorized duplication of software is contrary to HOC's standards of conduct. The following points are to be followed to comply with software license agreements:

- All users must use all software in accordance wit h its license agreements and the HOC's software policy. All users acknowledge that they do not own this software or its related documentation, and unless expressly authorized by the software publisher, may not make additional copies except for archival purposes.

- HOC will not tolerate the use of any unauthorized copies of software or fonts in the Agency.

- No user will give software or fonts to any outsiders including clients, customers, and others. Under no circumstances will software be used within HOC that has been brought in from any unauthorized location under HOC's policy, including, but not limited to, the Internet, the home, friends and colleagues.

- Any user who determines that there may be a misuse of software within the Agency will notify the Director of Information Technology , or their direct supervisor.

- All software used by the Agency on Agency-owned computers will be purchased through appropriate procedures.

8. Penalties and Reprimands

According to the US Copyright Act, illegal reproduction of software is subject to civil damages of as much as $100,000 per title infringed, and criminal penalties, including fines of as much as $250,000 per title infringed and imprisonment of up to five years. An HOC user, who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances. Such discipline may include termination of employment. HOC does not condone the illegal duplication of software and will not tolerate it.

VI. E-Mail and Internet Usage Guidelines

A. Purpose

The purpose of this section is to establish the policy and procedures relating to e-mail and internet usage. The following guidelines have been established for using HOC e -mail and Internet access. HOC provides the use of e -mail and the Internet as a means to make business and communication more effective. All e-mail originating from the Housing Opportunities Commission's e -mail systems are official agency documents . Any improper usage of the Internet or e -mail will not be tolerated and may result in d isciplinary action.

B. Policy

1. Official Use

- HOC electronic mail and internet services are HOC resources and are intended to be used in support of agency mission.
- HOC provides electronic mail and internet services to staff, and other authorized persons who are affiliated with HOC for their use when engaging in activities related to their roles in the agency.
- Access to electronic mail and internet a re valuable tools and are a privilege with certain accompanying responsibilities. The same standards of conduct th at are expected of staff regarding the use of other HOC facilities, services, and resources apply to the use of electronic mail and internet.

2. Personal Use

HOC electronic mail and internet services may be used for incidental personal purposes provided that such use:

- **Does not** directly or indirectly interfere with the agency operation of computing facilities or electronic mail services.
- **Does not** interfere with the electronic mail user's employment or other obligations to the agency.
- **Does not** violate this Policy, or any other applicable policy or law, including but not limited to use for personal gain, conflict of interest, harassment, defamation, copyright violation or illegal activities (see Misuse below).
- Electronic mail messages and internet browsing ari sing from such personal use shall, however, be subject to access consistent with this policy or applicable law. Accordingly, such use does not carry with it a reasonable expectation of privacy.

3. Confidentiality and Security

- HOC does not routinely monitor o r screen electronic mail and internet traffic. **However, HOC reserves the right, consistent with this policy and applicable law, to access, review and release all electronic information that is transmitted over or stored in HOC Systems or facilities, whether or not such information is private in nature, and therefore complete confidentiality or privacy of electronic mail or internet cannot be guaranteed.** Confidentiality cannot be guaranteed because of the nature of the medium, the need for authorized staff to maintain electronic mail systems, and HOC's accountability as a public institution, as well as in instances involving the health or safety of people or property; violations of HOC codes of conduct, regulations, policies, or law; other legal responsibilit ies or obligations of HOC; or the locating of information required for HOC business.
- Terminating employees will have their email accounts terminated on the last day of employment. Terminating employees need to be advised that their email accounts may be accessed by their departmental directors in order to continue to conduct HOC operations after

their departure. Departmental Directors must send a written request to the Help Desk requesting access to the account. All personal email correspondence must be deleted prior to leaving HOC.

- Users should exercise extreme caution in using email to communicate confidential or sensitive matters, and should not assume that their electronic mail is private or confidential.
- Users may not access, use, or disclose personal or confidential information without appropriate authorization, and must take necessary precautions to protect confidentiality of personal or confidential information in compliance with HOC policy and applicable law, regardless of whether the information is maintained on paper or whether it is found in electronic mail or other electronic records.
- Electronic mail users and operators must follow sound professional practices in providing for the security of electronic mail records, data, applications programs, and systems programs under their jurisdiction.
- Users are responsible for safeguarding their identification (ID) codes and passwords, and for using them only as authorized. Each user is responsible for all electronic mail transactions made under the authorization of his or her ID, and for all network electronic mail activity originating from his or her data jack.

4. Misuse

- Using electronic mail or internet for illegal activities is strictly prohibited. Illegal use may include, but is not limited to: obscenity; child pornography; threats; harassment; theft; attempting unauthorized access to data or attempting to breach any security measures on any electronic communications system; attempting to intercept any electronic communication transmissions without proper authority; and violation of copyright, trademark or defamation law.
- In addition to illegal activities, the following electronic mail practices are expressly prohibited: entry, examination, use, transfer, and tampering with the accounts and files of others, unless appropriately authorized pursuant to this policy; altering electronic mail system software or hardware configurations; or interfering with the work of others or with HOC or other computing agencies.
- HOC electronic mail and internet services may not be used for: commercial activities, personal financial gain or advancement of political agenda.
- Electronic mail and internet users shall not give the impression that they are representing, giving opinions, or otherwise making statements of behalf of HOC or any Division of HOC unless expressly authorized to do so. Where appropriate, the following explicit disclaimer shall be included: "The opinions or statements expressed herein are my own and should not be taken as a position, opinion, or endorsement of HOC."
- HOC electronic mail and internet services shall not be used for purposes that could reasonably be expected to cause, (directly or indirectly) strain on any computing facilities, or interference with others' use of electronic mail or internet systems. Such uses include, but are not limited to, the use of electronic mail services to:
  - Send or forward chain letters.
  - "Spam", that is, to exploit listservs or similar systems for the widespread distribution of unsolicited mail.
  - "Letter-bomb", that is, to resend the same e-mail repeatedly to one or more recipients.
  - Knowingly send or transmit computer viruses

5. Violations

Suspected or known violations of policy or law should be reported to the appropriate supervisory level for the operational unit in w hich the violation occurs. Violations will be processed by the appropriate HOC authorities and/or law enforcement agencies. Violations may result in various actions, including but not limited to revocation of electronic mail or internet service privileges; disciplinary action up to and including dismissal; referral to law enforcement agencies; or other legal action.

VII. Access, Security and Control of Data and Information

A. Purpose

To establish policy for the protection of HOC's computerized information systems, data, and software. To establish rights and responsibilities for the protection of staff who use these information systems.

B. Policy

Data contained in HOC's systems are the property of HOC and represent official HOC. Users who accept access to this data, whether on-line or in datasets, also accept responsibility for adhering to certain principles in the use and protection of that data:

- Information systems within HOC shall be used only for and contain only data necessary for fulfillment of HOC's mission.
- HOC data shall be used solely for the legitimate business of the agency.
- Due care shall be exercised to protect HOC data and information systems from unauthorized use, disclosure, alteration or destruction.
- HOC data, regardless of who collects or maintains it, shall be shared among those staff whose responsibilities require knowledge of such data.
- Applicable federal and state laws (i.e. the Privacy Act), and HOC policies and procedures concerning storage, retention, use, release, transportation, and destruction of data and/or all information systems contents and components shall be observed.
- Appropriate HOC procedures shall be followed in reporting any breach of security or compromise of safeguards.
- HOC computerized information systems shall be constructed in such a manner to assure that:
    - Accuracy and completeness of all system contents are maintained during storage and processing;
    - Data, text and software stored and processed can be traced forward and backward for audit ability;
    - Information systems capabilities can be re-established within an acceptable time upon loss or damage by accident, malfunction, breach of security or act of God; and
    - Actual or attempted breaches of security can be detected promptly.
- Any staff member engaging in unauthorized use, disclosure, alteration, or destruction of information systems or data in violation of this policy shall be subject to appropriate disciplinary action, including possible dismissal.
- Users may not use, query, release or print data in any application which they have not been given deliberate access to, which can include, but is not limited to:
    - Personnel, leave, salary reports;
    - Reports for government or funding agencies;
    - Personal information about clients within HOC properties ;
    - Mailing lists and labels;
    - Agency financial information

C. Responsibilities

Safeguarding of HOC information systems and data shall be the responsibility of each staff member with knowledge of the system or data. Specific responsibilities are as follows:

- Management - all levels of management are responsible for ensuring that system users within their area of accountability are aware of their responsibilities as defined in this policy. Specifically, managers are responsible for validating the access requirements of their staff according to their job functions, prior to submitting requests for the provision of access, and for ensuring a secure office envir onment with regard to HOC information systems.
- Users - are responsible for the protection, privacy, and control of all data, regardless of the data storage medium. Users must ensure that the data and data media are maintained and disposed of in a secure manner. Users are responsible for understanding the meaning and purpose of the data to which they have access, and may use this data only to support the normal functions of the users administrative duties. Users are responsible for all transactions occurring under his/her userid and/or password. Passwords and userids may not be shared with anyone under any circumstances unless the Director of Information Technology specifically approves an exception. Users are also responsible for reading and understanding this policy.
- Director of Information Technology - is responsible for ensuring that appropriate security controls are being provided, inc luding protection of all areas of risk or exposure.
- Information Technology Staff - are responsible for providing administrative, technical and educational support in the area of information security for all users of administrative systems. This support in cludes, but is not limited to:
    - Creation and deletion of userids and/or account numbers, after appropriate approval has been obtained.
    - Providing access to administrative systems, transactions, or production after appropriate approval.
    - Recommendations to the Director of Information Technology on appropriate training to ensure consistent practice among departmental support personnel.

VIII. Cell Phone Usage and Guidelines

A. Purpose

The purpose of this section is established to provide guidance to employees who, through the nature of their work, are required to be accessible by cell phone.

B. Policy

1. Usage Guidelines of HOC Owned Cell Phones

HOC provides cell phones for Agency business activities. Every user has the responsibility to use HOC cell phones in a responsible and productive manner.

Due to the cost associated with cell phone usage, only incidental personal (non – business related) use is permitted. Misuse or excessive personal use of agency cell phones is subject to management review and may result in reimbursement charges to the employee and/or disciplinary action.

2. Safety Issues for Cellular Phone Use

Employees whose job responsibilities include regular or occasional driving and who are issued a cell phone for business use are expected to refrain from using their phone while driving.

Regardless of the circumstances, including slow or stopped traffic, employees must pull off to the side of the road and safely stop the vehicle before making or accepting a call. Under no circumstances are employees allowed to place themselves at risk to fulfill business needs.

Employees whose job responsibilities do not specifically include driving as an essential function, but who are issued a cell phone for business use, are also expected to abide by the provisions above. Employees who are charged with traffic violations resulting from the use of their phone while driving will be solely responsible for all liabilities that result from such actions.

3. Losses and Repairs

Employees who are issued a HOC cell phone are expected to handle equipment with appropriate care, protecting it from loss or damage. If a cell phone is damaged, the employee must contact the Information Technology Division within one business day to arrange for a repair or replacement.

The Information Technology Division will contact the employee's Division Director regarding the damage. That Division Director will then decide whether or not the employee will be held responsible for the cost of the repair or replacement, depending on the circumstances surrounding the damage occurring.

Employees will not be held responsible for damage which occurred during the course of performing HOC work activities. If the damage occurred while NOT in the course of performing work activities, however, the employee may be held liable for the repair or replacement costs.

4. Management Responsibilities

Management must ensure that when personnel no longer are employed by the Agency, the department will recover the phone and return it to the Information Technology Division within one business day.

Management must submit a change request to the Information Technology Division when transferring cell phone from one employee to another within one business day.

Management will review cell phone charges and audit costs as necessary.

Information Technology Policy

I have received a copy of HOC's Information Technology Policy. I recognize and understand that HOC's Technology Systems are to be used for HOC business and that the use of this equipment for private purposes is strictly prohibited.

Technology Policy Acknowledgement

I have received and read HOC's Information Technology Policy regarding electronic systems.

Employee Name **(Printed)**	Employee Signature	Date