Prohibition of Illegal Discrimination in the Workplace Policy

PROHIBITION ON ILLEGAL DISCRIMINATION IN THE WORKPLACE

It is the policy of the New York State Housing Finance Agency, the Affordable Housing Corporation, the State of New York Mortgage Agency and its respective subsidiaries and affiliates (collectively the "Agency") to provide their respective employees with a work environment that is free from all forms of illegal discrimination in the workplace. Illegal discrimination is a violation of federal, state and local law and has potentially serious social and emotional impact on victims of such conduct.

It is a violation of law and this policy to fail or refuse to hire or to discharge any individual, or otherwise discriminate against any individual with respect to his/her compensation, terms, conditions or privileges of employment because of the individual's actual or perceived age, race, creed, color, national origin, religion, gender, sex, sexual orientation, disability, military status, predisposing genetic characteristics, marital status or alienage or citizen status.

It is also a violation of law and this policy for any employee employed by the Agency to engage in conduct that requires employees to work in a discriminatorily hostile or abusive environment. A hostile work environment is one in which the workplace is permeated with discriminatory intimidation, ridicule and insult that is sufficiently severe or pervasive to alter the conditions of the victim's employment.

It is the responsibility of all Agency employees to strictly adhere to and enforce the Agency's prohibition on illegal discrimination in the workplace. It is also the responsibility of supervisory personnel to be aware of and sensitive to conditions, situations or circumstances, which, if left unresolved, could potentially rise to the level of illegal discrimination in the workplace, and to take appropriate remedial action to appropriately address these conditions as soon as possible.

The Agency will not tolerate any form of illegal discrimination, and the Agency's prohibition on illegal discrimination will be strictly enforced. Engaging in illegal discrimination is a form of serious employee misconduct, and appropriate disciplinary action, potentially including dismissal from employment, will be taken against individuals determined to have engaged in this type of conduct. In addition, appropriate administrative or disciplinary action may be taken against supervisory personnel who fail to timely report such conduct to the Agency after receipt of a complaint from one of their employees.

Employees who believe that they or another employee are being subjected to any form of illegal discrimination should immediately report the incident to the Agency. Employees who believe that illegal discrimination may be occurring can report such

incidents to the Agency, free from retaliation or reprisal, by informing their immediate supervisor, the Director of Human Resources, the Deputy Director of Human Resources or any member of Agency management with the title of Assistant Vice President or higher. If the complaint concerns an employee's supervisor, the Agency may be notified via the Director of Human Resources or any member of management with the title of Assistant Vice President or higher outside the employee's department. Allegations of discrimination may be made by an employee either orally or in writing. Supervisory or managerial personnel receiving a complaint of illegal harassment, whether orally or in writing, should report the claim to the Agency's Director of Human Resources as soon as possible.

Any Agency employee who has been subjected to illegal discrimination in the workplace has rights of redress at the Agency. Any Agency employees who believe that they have been subject to illegal discrimination are strongly encouraged to report the facts and circumstances of the illegal discrimination as soon as possible after its occurrence. The Agency takes all complaints of illegal discrimination very seriously and will promptly and fully investigate all complaints of illegal discrimination which are brought to its attention. The investigation may include interviewing the parties and any potential witnesses and reviewing documentary or physical evidence. Employees desiring to provide information may be requested to provide a written statement, but will not be required to do so. Any employee possessing information about illegal discrimination in the workplace, whether directed at the employee herself or himself, or directed at a co-worker, is encouraged to make any such information known to the Agency. Employees who do not wish to participate in an interview will not be required to do so. No employee complaining of illegal discrimination or providing information concerning incidents of illegal discrimination will be the subject of any adverse personnel action or retaliation.

In addition to the employee's right to file a complaint of illegal discrimination with the Agency under this procedure, Agency employees also have the right, separate and apart from the Agency's policies and procedures concerning illegal discrimination claims, to file claims of illegal discrimination under federal, state and/or local law. Employees seeking to file a claim of illegal discrimination under these laws may contact the New York State Division of Human Rights ("NYSDHR"), the local office of the federal Equal Employment Opportunity Commission ("EEOC"), or a private attorney for guidance concerning their rights.

The Agency will take all appropriate action to prevent illegal discrimination from occurring in the workplace and will take all necessary steps to ensure that any established occurrence of illegal discrimination has permanently ceased and will not reoccur in the future. These may include a number of remedial actions including, but not limited to, appropriate administrative action or pursuing disciplinary action against any employee engaging in conduct violating the Agency's prohibition on illegal discrimination in the workplace.

Employees having any questions concerning the Agency's prohibition against illegal discrimination in the workplace or the procedures described in this policy and procedure are encouraged to direct any such questions to the Director of Human Resources or the Equal Opportunity Officer.

This policy and procedure shall apply to all employees, part-time employees, seasonal employees, temporary employees, officers, Members/Directors and interns of the Agency and the term "employee", for the purposes of this policy and procedures, shall include all of the foregoing positions.

Sexual Harassment Prevention Policy

SEXUAL HARASSMENT POLICY

It is the policy of the State of New York Mortgage Agency (the "Agency") to provide its employees with a work environment that is free from all forms of sexual harassment in the workplace. Conduct constituting sexual harassment is illegal and has potentially serious social and emotional impact on victims of such conduct.

Sexual harassment is defined as unwelcome sexual advances, requests for sexual favors, or other verbal or physical conduct of a sexual nature when:

> submission to the conduct is made either explicitly or implicitly a term or condition of an individual's employment; or
>
> submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual; or
>
> the conduct has the purpose or effect of unreasonably interfering with an affected person's work performance, or creating an intimidating, hostile or offensive work environment.

It is the responsibility of all Agency employees to strictly adhere to and enforce the Agency's prohibition of sexual harassment in the workplace. It is also the responsibility of supervisory personnel to be aware of and sensitive to conditions, situations or circumstances, which, left unresolved, could potentially rise to the level of sexual harassment in the workplace, and to take appropriate remedial action to appropriately address these conditions as soon as possible.

The Agency will not tolerate any form of sexual harassment, and the Agency's prohibition of sexual harassment will be strictly enforced. Sexual harassment is a form of serious employee misconduct, and appropriate disciplinary action, potentially including dismissal from employment, will be taken against individuals determined to have engaged in this type of conduct. In addition, appropriate administrative or disciplinary action may be taken against supervisory personnel who fail to timely report such conduct to the Agency after receipt of a complaint from one of their employees.

Agency employees who believe that they or another Agency employee are being subjected to any form of sexual harassment should immediately report the incident to the Agency. Employees who believe that incidents of sexual harassment may be occurring can report such incidents to the Agency, free from retaliation, by informing their immediate supervisor, the Personnel Director, the Deputy Personnel Director, or any member of Agency management with the title of Assistant Vice President or higher. If the complaint concerns an employee's supervisor, the Agency may be notified via the Personnel Director or any member of management outside the employee's department. Allegations of sexual harassment may be made by an employee either orally or in writing. Supervisory or managerial personnel receiving a complaint of sexual harassment, whether orally or in writing, should report the claim to the Agency's Personnel Director as soon as possible.

Any Agency employee who has been subjected to sexual harassment in the workplace has rights of redress at the Agency. Any Agency employees who believe that they have been subject to such harassment are strongly encouraged to report the facts and circumstances of the sexual harassment as soon as possible after its occurrence. The Agency takes all complaints of sexual harassment very seriously and will promptly and fully investigate all complaints of sexual harassment which are brought to its attention. The investigation may include interviewing the

parties and any potential witnesses and reviewing documentary or physical evidence. Employees desiring to provide information may be requested to provide a written statement, but will not be required to do so. Any employee possessing information about sexual harassment in the workplace, whether directed at the employee herself or himself, or directed at a co-worker, is encouraged to make any such information known to the Agency. Employees who do not wish to participate in an interview will not be required to do so. Each investigation, as well as any interviews required as part of an investigation, will be conducted in a manner that ensures as much confidentiality as possible. No employee complaining of sexual harassment or providing information concerning incidents of sexual harassment will be the subject of any adverse personnel action or retaliation. At the request of the employee furnishing information, female or male interviewers, as the case may be, can be arranged by the Agency.

The Agency will take all appropriate action to prevent sexual harassment from occurring in the workplace and will take all necessary steps to ensure that any established occurrence of sexual harassment has permanently ceased and will not reoccur in the future. These may include a number of remedial actions including, but not limited to, appropriate administrative action or pursuing disciplinary action against any employee engaging in conduct violating the Agency's prohibition on sexual harassment in the workplace.

In addition to the employee's right to file a complaint of sexual harassment with the Agency under this procedure, employees also have the right, separate and apart from the Agency's policies and procedures concerning sexual harassment claims, to file claims of sexual harassment under Title VII of the Civil Rights Act. Employees seeking to file a claim of sexual harassment under Title VII may contact the New York State Division of Human Rights ("NYSDHR"), the local office of the federal Equal Employment Opportunity Commission ("EEOC"), or a private attorney for guidance concerning his or her rights under Title VII.

Employees having any questions concerning the Agency's strict prohibition against sexual harassment in the workplace or the procedures described in this policy are encouraged to direct any such questions to the Personnel Director or the Equal Opportunity Officer.

Information Systems Policies

New York State Housing Finance Agency
State of New York Mortgage Agency
New York State Affordable Housing Corporation

INFORMATION SYSTEMS

POLICIES

August 21, 2000

TABLE OF CONTENTS

I. INTRODUCTION AND POLICY STATEMENT CONCERNING USE OF AGENCIES' INFORMATION SYSTEMS RESOURCES.

The Agencies' information systems resources ("Information Systems Resources") are the exclusive property of the Agencies, and are made available to employees as a tool in conducting the Agencies' business. The New York State Housing Finance Agency, New York State Affordable Housing Corporation, and The State of New York Mortgage Agency ("Agencies/Agency") depend on their information systems to carry out their missions. The purpose of these Policies is to ensure that the integrity of the Agencies' Information Systems Resources is maintained at all times, and that they are properly used by the Agencies' staff.

These Policies also have the purpose of placing all employees on notice that use of the Agencies' information systems is not private and is subject to monitoring by authorized Agencies' personnel and agents. Failure to adhere to these Policies can result in disciplinary action up to, and including, discharge from employment. Abuse-free, smooth and efficient information systems can only be achieved with the full cooperation of the entire Agencies' staff.

The Agencies' Information Systems Resources are administered and supervised by the Chief Operating Officer of the Agencies. The Management Information Systems ("MIS") Unit maintains all of the Agencies' information systems except the telephones, facsimile machines and voicemail, which are maintained by the Facilities Management and Administrative Services Unit ("Facilities Management"). The MIS Unit maintains only the Agencies' information systems and does not assist employees with their own personal computer equipment and software.

These Policies may be revised and supplemented on an as needed basis as determined by the Agencies.

These Policies apply to all Information Systems Resources in use at the Agencies. Information Systems Resources include, but are not necessarily limited to:

- **hardware** - Computer, communication and other electronic equipment used for the processing, communication or storage of data. This includes, but is not necessarily limited to, PCs, file servers, printers, tape drives, scanning equipment, facsimile machines, photocopiers, telephones, portable computing equipment (laptop computers, hand-held computers, etc.), pagers, modems and two-way radios.

- **software** - Programs, programming languages, instructions, or routines, which are used to perform work on a computer and to electronically input, access, process and retrieve information. This includes, but is not limited to, software that is purchased, licensed, or developed in-house.

- **data** - Data is any kind of information. It includes, but is not limited to, information that is stored on or accessible through a computer or electronic device and can take the form of records, numeric, textual, video or graphical material. Data includes, but is not necessarily limited to, word-processing files, spreadsheet files, database files, audio

files, pictorial video files, animation files, calendar files,, the Agencies' Web sites, faxes and voicemail messages.

- **storage media** - Storage media are any devices utilized to electronically store data. Storage media include, but are not necessarily limited to, fixed disk drives, removable disk drives, tapes, memory, back-up devices, CDs, and diskettes.

- **e-mail** - Written, graphical, audio, video or other information messages transmitted through electronic means. This includes, but is not limited to, messages sent and received by the Agencies' in-house e-mail system, which is GroupWise, as well as all messages sent and received over the Internet or via any other electronic communications medium.

- **information services** - Information services are any paid or unpaid services that provide information and are accessed through electronic means. They include, but are not necessarily limited to, the Internet, LRS, Lexis/Nexis, Westlaw, Telerate and alike.

- **Internet services** - Access to the World Wide Web through the use of electronic means.

- **computer network** - The hardware, software, data, storage media and services.

II. BUSINESS AND PERSONAL USE OF AGENCIES' INFORMATION SYSTEMS RESOURCES.

A. Business Purpose.

The Agencies' Information Systems Resources are to be utilized by employees to conduct the Agencies' business. Non-business use of the Information Systems Resources is expressly prohibited, except as specifically provided in these Policies. All employees must consistently exercise sound judgment in the use of the Agencies' Information Systems Resources, and must consistently use them for all purposes in a responsible, professional, ethical, and lawful manner. When employees are logged into the Agencies' Information Systems Resources from any location, employees are specifically prohibited from engaging in any communications or activities that violate these Policies or are improper or inappropriate. Employee use of the Agencies' Information Systems Resources, both for business and personal use, is conditional and a privilege, not a right. The Agencies expressly reserve the right, in their sole discretion, to determine employees' eligibility to utilize the Agencies' Information Systems Resources, or any part thereof, as well as the nature and extent of their utilization. The Agencies further reserve the right, in their sole discretion, to revoke or modify employees' usage privileges at any time.

B. Personal Use By Employees.

Personal use of the Agencies' Information Systems Resources is any use other than use for the Agencies' business. Personal use of the Agencies' Information Systems Resources is permitted only on a limited basis and never during working time. Such conditional personal use is accorded to employees by the Agencies as a privilege and accommodation, and is subordinate and subject to all business use

and the needs of the Agencies. Personal use can be revoked at will at any time by the Agencies. Personal use of the Agencies' Information Systems Resources, except the telephone system and voicemail (discussed below), must be authorized in advance by the employee's Department Head both as to time and usage. Personal use of Information Systems Resources cannot interfere with the Agencies' ability to conduct its business, and cannot violate other rules, regulations, policies and procedures governing employee conduct in the workplace. Personal use must be in strict accordance with these Policies and additional rules and procedures established by the Chief Operating Officer, the Chief Technology Officer, and the employee's Department Head; must not interfere with productivity or constitute a nuisance or distraction to the orderly conduct of the Agencies' business; cannot consume significant system resources or storage capacity; involve large file transfers; or otherwise materially deplete system resources. No personal data of any nature whatsoever shall be saved or otherwise stored in any manner on the Agencies' equipment, except as specifically authorized in advance by the employee's Department Head.

Personal use of the Agencies' telephone system and voicemail should be kept to a minimum and restricted to lunchtime and breaks wherever possible. Reimbursement is required for such things as personal long-distance telephone calls and fax usage. The Agencies may monitor telephone usage for both excessive personal usage and compliance with these Policies.

III. COMMUNICATIONS.

A. Generally.

These Policies cover all communications transmitted or received electronically over or through the Agencies' Information Systems Resources, including but not limited to, computers, telephones, and facsimile machines. Employees are reminded that communications transmitted electronically are also covered by all other Agencies' policies and procedures that apply to the content of the communications in general, including but not limited to, sexual harassment policies, e-mail policy, external communications procedures, prohibitions on political use and unauthorized use of the Agencies' name. Communications and transmissions, the content of which violate these other policies and procedures, constitute improper use of the Agencies' Information Systems Resources.

B. E-mail Policy.

The Agencies' e-mail policy, as originally distributed on October 11, 1996 and clarified on November 9, 1998, is set forth in its entirety in Attachment A of these Policies. The Agencies' e-mail policy remains in full force and effect. Violations of the Agencies' e-mail policy also violate these Policies.

C. Unauthorized Third Party Communications Using The Agencies' Information Systems Resources.

Electronic communications to third parties (other than those third parties with whom an employee does business in the ordinary course of legitimate Agencies' business) via the Agencies' Information Systems Resources, including but not limited to e-mails and instant messages, may also be covered by the Agencies' external communications and legislator and public official contacts policies. These policies are maintained in the Legal Department, which should be consulted concerning external or other third party communications utilizing the Agencies' information systems, including Internet and e-mail communications. Transmissions of electronic communications, the content of which violate these other policies and procedures, constitute improper use of the Agencies' Information Systems Resources.

D. Internet Use By Employees.

The Internet is a powerful communications tool and a valuable source of information relating to the Agencies' business. Access to the Internet is afforded to certain employees in order to conduct the Agencies' business. Time spent on the Internet for any personal use during work-time is prohibited. Non-business personal use of the Internet is strictly limited to breaks and lunch periods with the prior approval of the Department Head. The Agencies monitor Internet access and use of its equipment for compliance with these Policies.

Employees are prohibited from utilizing the Agencies' Internet access for the purpose of engaging in business other than that of the Agencies. Such prohibited use includes, but is not limited to, security trading, active investment activity, shopping, or any other business for personal profit. Employees are expressly prohibited from visiting inappropriate sites such as sexually graphic, lewd, lascivious or pornographic sites; sites which promote or involve hatred, violence or discrimination; sites permitting sounding off in public forums; inappropriate newsgroups; any sites having a political affiliation or subject matter in furtherance of a political position; chat rooms or any other site the visiting of which is inconsistent with proper and professional public employee conduct at work. Internet usage is no different from any other work functions and is subject to all other Agencies' rules, regulations, policies and procedures governing employee conduct.

The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and other inappropriate material. Users accessing the Internet for personal use do so at their own risk. The Agencies are not responsible for any material viewed or downloaded by users of the Internet.

Information sent or received over the Internet is not confidential or secure. In addition to the Agencies' monitoring of Internet traffic, there are a variety of ways an Internet communication can be disclosed to people other than the intended recipient.

IV. SYSTEM CARE AND SECURITY.

A. Protection And Care Of Equipment.

Damage to equipment causes disruption to the Agencies' business, the employee and the MIS technical support staff. The Agencies require that all employees take the following precautions:

- Keep food and drink away from computers and other equipment.
- Use care in handling portable storage media (diskettes, etc.) and other portable equipment.
- Take reasonable measures to keep equipment clean and dust free.

B. User ID And Passwords.

The Agencies' Information Systems Resources require that each user have one or more User IDs. Typically, each User ID is associated with individual passwords. Separate User IDs are used to access the Agencies' overall computer network as well as individual components on the network. The User ID provides functional access to software that is specifically based on each User ID. The misuse of a User ID may constitute forgery and misrepresentation. Improper conduct includes, but is not limited to, the following:

- Allowing an unauthorized individual, including but not limited to anyone not employed by the Agencies, access to a User ID and password.
- Sharing a User ID or password with another staff member unless authorized in advance, in writing, by the Chief Technology Officer.
- Using another user's ID or password even if the individual has neglected to safeguard his or her User ID and password.

Employees are responsible for maintaining the security and secrecy of their individual passwords. Employee misconduct or negligence in maintaining the security and secrecy of passwords may result in disciplinary action up to and including termination from employment. Passwords should never be written down and stored in a location that is accessible to others. The Agencies' computer network will require that each user change his or her sign-on password every 90 days. Other specialized passwords must also be changed on a periodic basis. Alphanumeric passwords should be used rather than passwords that are exclusively numbers or letters. The MIS Unit will notify users when certain specialized passwords must be changed. Failure to cooperate fully with MIS in changing the password may result in denial of access.

Occasionally, due to an error, a user may have access to a system or directory for which the user is not authorized. When this occurs, it is the user's responsibility to inform MIS management immediately so that corrective action may be taken.

There are additional precautions that each user should take in order to secure access to his or her PC. These precautions include:

- Using a password protected screen saver on the PC at all times. The screen saver should be set to activate after five minutes.
- Signing off all application systems and shutting down the PC each night when leaving the office. Each user must also sign off from all systems and log out of the network when the computer is unattended or not going to be used for an extended period of time during the day.

C. Portable Equipment.

Portable computer equipment, cellular telephones, hand-held computers, two-way radios and other business equipment are issued by the Agencies to employees who have obtained the prior written approval of the Department Head and the Chief Technology Officer for short-term use of computer equipment (i.e. overnight or the weekend); the Department Head and the Vice President of Facilities Management for short-term use of other portable equipment (i.e. cellular phones); and the Department Head and the Chief Operating Officer for long-term use of any portable equipment. All portable equipment must be returned in a timely manner. Once issued to an employee, portable equipment is the sole responsibility of the employee until returned to the custody of the Agencies. Employees issued portable equipment are responsible for the safety of the equipment and may be held liable for the cost of repair or replacement due to the employee's negligence. To avoid such liability:

- the user must ensure that all portable equipment (i.e., laptop computers, portable printers, cellular telephones, cameras, two-way radios, etc.) is placed in a secure area where the opportunities for theft are minimized;
- the user must keep confidential data and programs stored on diskettes, CDs and other storage media in a secure location where the opportunities for theft are minimized;
- the user must ensure that only authorized Agencies personnel have access to portable equipment and media;
- the user must take such other actions that are reasonably necessary to ensure that the equipment and media are not damaged, stolen or destroyed.

D. Remote Access.

Remote access of the Agencies' voicemail is available to all employees. Remote access of all other of the Agencies' Information Systems Resources is available to certain employees on a restricted basis, and only with the express written permission of the Department Head and the Chief Technology Officer. Unauthorized accessing of Agencies' Information Systems Resources through communication lines or otherwise is expressly prohibited.

E. Software.

1. Agencies' Oversight.

Only software purchased or otherwise obtained by the Agencies is to be installed on the Agencies' equipment, except as otherwise provided in these Policies. Employees are prohibited from incorporating software from any sources whatsoever outside the Agencies into the Agencies' Information Systems Resources without the express approval of the Department Head and the Chief Technology Officer. This includes, but is not limited to, personal software, business-related software belonging to the employee, games, programs, software downloaded from the Internet and screen savers. In the event authorization is obtained for software installation on Agencies' equipment, a member of the MIS Unit must complete the installation. Any software installed on the Agencies' equipment in violation of these Policies may be removed by the Agencies without notice. Properly authorized software that creates system problems or is used by an employee in a manner that violates these Policies or is otherwise inappropriate may also be removed by the Agencies without notice.

Employees are prohibited from copying Agencies-developed or licensed software from one computer to another without the prior written authorization of the Chief Technology Officer. Employees shall not in any manner alter or otherwise modify the network configurations, settings, preferences, set-up or overall operation of any Agencies' software, except as permitted by the Chief Technology Officer.

The Agencies' Information Systems Resources, or any part thereof, shall not be removed from the Agencies unless they are being used to conduct Agencies business and their removal has been authorized in advance in writing by the Chief Technology Officer.

2. Licensing/Copyright Protection.

The Agency's use or purchase/acquisition of hardware and software is conditioned on acceptance and agreement of licensing agreements and provisions of copyright laws. Licensing agreement(s) and or laws, which all computer users must adhere to, are found directly on the equipment or in accompanying software or hardware manuals. Material subject to licensing agreement(s) and/or copyright laws may be found on the Internet. Licensing agreement(s) and/or copyright laws generally prohibit the copying of programs for use on other computer installations. It is prudent to treat all software and other third party material as subject to agreement on use and/or copyright. All employee usage of the Agencies' Information Systems Resources shall be in strict accordance with applicable licensing agreements and copyright protections, and employees shall not engage in any conduct that creates liability to the Agencies for breach of these agreements or violations of law.

Certain software manuals may be borrowed from the Agencies' resource library for limited periods of time. Employees wishing to use the manuals should contact the MIS Help Desk.

3. Agencies' Owned Software.

Any software developed by an Agencies' employee through the use or means of the Agencies' Information Systems Resources is the exclusive property of the Agencies and is not to be sold or given to any person or organization without the prior written authorization of the Agencies' Chief Operating Officer.

F. Agencies' Data.

Except as otherwise determined by the Chief Technology Officer, all data owned by the Agencies or produced or generated by an employee on Agencies' equipment shall be stored on the centralized computer network. No such data is permitted to reside exclusively on the user's PC or individual data storage media without prior authorization from the Chief Technology Officer. Upon separation from Agencies' service or transfer to another assignment within the Agencies, employees shall not move or transfer any of the Agencies' data without the authorization of the Department Head and the Chief Technology Officer.

V. IMPROPER CONDUCT.

Improper conduct with respect to employee use of the Agencies' Information Systems Resources is strictly prohibited. Improper conduct includes, but is not limited to, the following:

- Using the Agencies' Information Systems Resources for personal use of any kind during working time or without the prior approval of the Department Head;
- Failure to adhere to the usage rules established by these Policies, the usage rules established by the Department Head, the Chief Technology Officer and the Chief Operating Officer;
- Utilizing the Agencies' Information Systems Resources for an unauthorized, unlawful or improper purpose, or a purpose prohibited by Agencies' rules, regulations, policies and procedures;
- Engaging in improper, illegal, fraudulent or malicious conduct, or using Agencies' Information Systems Resources in the commission of a crime;
- Utilizing the Agencies' Information Systems Resources to disparage the Agencies in any way or harm their reputations;
- Abusing or harassing another employee through the use of the Agencies' Information Systems Resources;
- Sending, receiving, storing, browsing or viewing material that is improper, illegal, discriminatory, harassing, defamatory, obscene or in any manner inappropriate or inconsistent with the professional standards of the Agencies;
- Visiting Web sites which are, in the sole opinion of the Agencies, inappropriate;
- Visiting and or participating in Web sites which promote or involve hatred, violence, discrimination or are sexually explicit, pornographic or the like;

- Knowingly accepting or using software, including but not limited to unlicensed software, or data which has been obtained by illegal or improper means;
- Unauthorized copying of software owned by or licensed to the Agencies;
- Obtaining, providing or using another employee's password without explicit authorization of the Department Head and the Chief Technology Officer;
- Installing software of any kind, including but not limited to screen savers, on the Agencies' computer network without the express written authorization of the Department Head and the Chief Technology Officer;
- Modifying any network configurations without the prior written approval of the Chief Technology Officer;
- Storing, saving or otherwise retaining on the Agencies' Information Systems Resources any personal data or information;
- Attempting to test, circumvent, or defeat security, firewalls, auditing systems, or protective features of the Agencies' Information Systems Resources or those of any other organization;
- Attempting to remove, modify, tamper with, damage, sabotage, vandalize or disrupt in any way the operation of the Agencies' Information Systems Resources including but not limited to, computer equipment, data communications equipment or data communications lines;
- Using the Agencies' Information Systems Resources for dissemination or storage of commercial or personal advertisements, solicitations, promotions, destructive programs (viruses or self-replicating codes), political material, or any other unauthorized use, including the unauthorized dissemination of any Agencies' information including but not limited to, trade secrets, confidential or proprietary material, e-mail addresses, and staff lists;
- Misusing, or using without proper authorization from the Department Head, paid information services such as Lexis/Nexis and other paid information services;
- Modifying or attempting to modify software developed by or licensed to the Agencies without prior written authorization of the Chief Technology Officer;
- Unauthorized attempts to access, remove, copy or modify data files, databases, directories or software programs;
- Removing Information Systems Resources computer equipment, or any part thereof, from the Agencies' premises without prior written authorization from the Chief Technology Officer;
- Utilizing Agencies' Information Systems Resources for the purpose of engaging in business other than the Agencies' business. This includes, but is not limited to, securities trading and other activity for personal profit;
- Using Real Player, Microsoft Video Clips or any other Internet-based audio and video

services for purposes other than the Agencies' business;

- Unauthorized transmission of personal instant messages or other communications not relating to the Agencies' business;
- Violations of the Agencies' e-mail policy;
- Bulk e-mailing, faxing, voice mailing or other electronic communication not authorized by the Department Head;
- Electronic transmissions of messages including, but not limited to, e-mails or instant messages that violate the Agencies' policies and procedures governing external communications;
- Requesting the Agencies' Information Systems Resources including, but not limited to, technical assistance from MIS technicians under false pretenses or requesting MIS assistance with respect to an employee's personal computer equipment or software.

Any violation of these Policies (as amended from time to time) as well as additional rules and regulations governing usage established by Department Heads, the Chief Technology Officer or the Chief Operating Officer may result in the suspension from use of the Agencies' Information Systems Resources, and disciplinary action, up to and including termination from employment. Employees are encouraged to report suspected misconduct and/or inappropriate computer use to the Personnel Unit.

VI. AGENCIES' MONITORING OF EMPLOYEE USE AND CONDUCT.

Any and all data stored on or transmitted through the Agencies' Information Systems Resources are not private and are the exclusive property of the Agencies. All data stored on or transmitted through the Agencies' Information Systems Resources is expressly subject to monitoring, review, reading and analyzing by authorized Agencies' management and its agents. This includes data stored on any medium or in any format of the Information Systems Resources including, but not limited to, fixed disk drives, removable disk drives, CDs, magnetic tape and diskette, e-mails and voicemails. This also includes data stored or retrievable from any Agencies' location including, but not limited to, network file servers, the user's desktop PC, and portable computing equipment (laptops, etc.), or information transmitted or sent through the Internet. Any activity engaged in by an employee on an Agencies' computer, using Agencies' software, or through Agencies' access lines, including the Internet and communication lines, is subject to monitoring and review by the Agencies to the full extent permitted by law and in accordance with Agencies' policies and procedures. Employees have no expectation of privacy in any computer-related activities, and the MIS Unit conducts periodic reviews of computer activities and files stored on the system. Telephone communications may be monitored for business use to ensure good service, or based upon a reasonable suspicion of misconduct.

Attachment A

NEW YORK STATE
HOUSING FINANCE AGENCY

STATE OF NEW YORK
MORTGAGE AGENCY

Inter-Office Correspondence

To: Agency Staff

From: Ralph J. Madalena **Date:** November 9, 1998

Subject: Use of Agencies' E-mail System

Staff is reminded that the Agencies' e-mail system is for the purpose of conducting the Agencies' business and carrying out employees' work related duties; it is not for personal use. Messages on the Agencies' e-mail system or other information on the Agencies' computers are not private and are subject to inspection and monitoring by the Agencies at any time. You should be aware that the Agencies' MIS Department possesses the capability to monitor intra-agency e-mail, as well as incoming and outgoing transmissions. The MIS Department monitors e-mail transmissions where suspicion of abuse or violation of the Agencies' e-mail policy is determined to exist. Any use of the e-mail system or materials with content which is illegal, violates standing Agency policies, is disruptive, inappropriate or offensive is not permitted.

Recent monitoring of the Agencies' e-mail system by the MIS Department has revealed some apparent misunderstandings and/or violations by employees of the Agencies' e-mail policy. For purposes of clarification and the avoidance of future problems, a copy of the Agencies' e-mail policy is attached. Please read it carefully and adhere to it so as to avoid the many and potentially serious consequences of violating the Agencies' policy concerning e-mail use. Employees are specifically cautioned that, as clearly stated in the attached policy, violations may result in disciplinary action.

You will note that the policy provides procedures for disseminating messages that are not strictly work-related, such as announcements and lost and found information. Please adhere to those procedures.

Also, for the protection of everyone and for the sake of a proper working environment, everyone should be conscious of the propriety of any and all messages they send *or receive* on the e-mail system whether such messages are in furtherance of the Agencies' business or pertain to non-work related matters. Employees are expected to immediately report any inappropriate messages received to the MIS Department.

Finally, employees are reminded that the Agencies' e-mail system, including the listings of e-mail addresses of its employees, are the property of the Agency and such e-mail addresses are not to be provided to any person, entity or organization without the prior express written approval of the Chief Operating Officer.

811093.px
81109

NEW YORK STATE
HOUSING FINANCE AGENCY

STATE OF NEW YORK
MORTGAGE AGENCY

Inter-Office Correspondence

To: All Staff

From: Ralph J. Madalena Date: October 11, 1996

Subject: Agency Policy with respect to use of electronic mail.

Transmitted herewith for your attention is the Agencies' electronic mail ("e-mail") policy. This policy incorporates and more fully expresses previously applicable practice and procedures as well as incorporating a number of technical updates.

There are certain aspects of the policy which need to be highlighted as follows.

The Agencies' e-mail system is for the purpose of conducting the Agencies' business and carrying out employees' work related duties; it is not for personal use. Employees should refrain from sending information of a personal nature on the e-mail system. Unauthorized use of the Agencies' systems may be subject to disciplinary proceedings.

Messages on the e-mail system or other information on the Agencies' computers are *not private* and are subject to inspection and monitoring by the Agencies at any time, and the same may be subject to further disclosure as determined by the Agencies.

You will note that the policy provides procedures for disseminating messages which are not strictly work related such as birth announcements and lost and found information. Please adhere to those procedures.

In addition, you are reminded that the Agencies have bulletin boards available for personal messages located in both cafeterias.

610072.px
61011

New York State Housing Finance Agency
State Of New York Mortgage Agency

Electronic Mail Policy

Purpose and Goals

Electronic mail ("e-mail") is one of HFA's and SONYMA's core internal and external communication methods for conducting the business of the Agencies. The e-mail software presently in use at the Agencies is called GroupWise. The purpose of this policy is to ensure that e-mail systems used by Agency staff support Agency business functions to their fullest capacity. This policy advises staff and management of their responsibilities and provides guidance in managing information communicated by e-mail.

Access to E-mail Service

E-mail service is provided to all HFA/SONYMA staff upon their start of employment at the Agency. To request any changes to e-mail access, prepare an MIS Access Request form and forward it to MIS. To obtain an Access Request form, call the MIS Help Desk (ext. 767).

Use of E-mail

E-mail service, like other means of communication is to be used to support Agency business. Staff may use e-mail to communicate informally with others in the Agency with respect to the matters of Agency business so long as the communication meets professional standards of conduct. Staff may use e-mail to communicate outside of the Agency when such communications are related to legitimate business activities and are within their job assignments or responsibilities. When using the e-mail system for any such permitted purpose employees should avoid transmission of offensive and unprofessional communications, including but not limited to; those of an ethnic or racial nature, off-taste comments about others or matters such as sex, characterizations which could be considered defamatory, or the like.

Staff **may not use** e-mail for illegal, disruptive, unethical or unprofessional activities or for personal gain or for any purpose that would jeopardize the legitimate interests of the State. Unauthorized use of the Agencies' system or use of the system for other than Agency purposes may be subject to disciplinary proceedings.

Privacy and Access

E-mail messages are **not** personal and private. E-mail system administrators will **not** routinely monitor individual staff member's e-mail and will generally take reasonable precautions to protect the privacy of e-mail from co-workers. However, department managers and technical staff may access an employee's e-mail for various reasons, including but not limited to:

- for a legitimate business purpose (e.g., the need to access information when an employee is absent for an extended period of time);
- to diagnose and resolve technical problems involving system hardware, software, or communications; and/or
- to investigate possible misuse of e-mail or other matters when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.

Except as provided above, staff members are prohibited from accessing other user's e-mail without that user's permission. E-mail messages sent or received in conjunction with Agency business may:

- be releasable to the public under the Freedom of Information Law;
- require special measures to comply with the Personal Privacy Protection Law.

Everyone should be aware that **all** e-mail messages may be subject to discovery proceedings in legal actions.

Security

E-mail security is a joint responsibility of Agency technical staff and e-mail users. Users must take all reasonable precautions, including safeguarding and changing passwords (if used), to prevent unauthorized use.

Management and Retention of E-mail Communications

- Applicable to all e-mail messages and attachments:

  Since e-mail is a communications system, messages should not be retained for extended periods of time. Users should remove all e-mail communications in a timely fashion. If a user needs to retain information in an e-mail message for an extended period, he or she should transfer it from the e-mail system to an appropriate electronic or other filing system (such as WordPerfect). Although GroupWise has a file folder system, that system is **not** an appropriate permanent filing system for this purpose. Unlike WordPerfect files, individual messages stored in GroupWise folders cannot now be restored from Agency backup tapes. If an individual message is inadvertently deleted from GroupWise, it can be recovered from the GroupWise "trashbin" for 30 days. After that it is purged from the system.

- Applicable to **records** communicated via e-mail:

  E-mail created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions are records subject to records management requirements under the appropriate statutes and specific program requirements.

  Examples of messages sent by e-mail that typically are **records** include:

- policies and directives,
- correspondence or memoranda related to official business,
- work schedules and assignments,
- agendas and minutes of meetings,
- drafts of documents that are circulated for comment or approval,
- any document that initiates, authorizes or completes a business transaction,
- final reports or recommendations.

Some examples of messages that **typically do not constitute records** are:

- informal messages and announcements,
- copies or extracts of documents distributed for convenience or reference,
- phone message slips,
- announcements of social events (which should be properly disseminated in accordance with this policy as provided further herein).

Record Retention

Records communicated using e-mail need to be identified, managed, protected, and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions should be retained, managed and accessible in an existing filing system **outside the e-mail system** in accordance with the department's standard practices (e.g., a department standard might be to save all board related documents in a shared WordPerfect directory under a standardized name).

Users should:

- dispose of copies of records in e-mail after they have been filed in a record keeping system;
- delete records of transitory or little value that are not normally retained in record keeping systems as evidence of Agency activity.

Roles and Responsibilities

Agency senior management will ensure that policies are implemented by the departments. **Department managers** will develop and/or publicize record keeping practices in their area of responsibility including the routing, format, and filing of records communicated via e-mail. They will also train staff in the appropriate use of e-mail.

MIS network administrators are responsible for e-mail security, backup, and changes to the overall network e-mail system.

Dissemination of Non-business Communications

There are times when there is information of a personal nature which generally affects a large number of employees and which may require a wide dissemination; announcements of births, deaths, marriages, the appearance of an Agency employee in a news event, solicitations, and the like. Such information, if deemed appropriate by the Agency, may be distributed to Agency employees at large through the "Bulletin List" on the e-mail system **after approval by the Agencies' Personnel Department to whom you are directed to submit the information for review.** Reminder: If you want to be deleted from the "Bulletin List" mailing list you should contact MIS.

The e-mail is also sometimes used for lost-and-found purposes. If you would like an e-mail message disseminated for lost-and-found purposes, **please contact the Facilities and Administrative Services Department which administers the Agencies' Lost-and Found.**

If there is an Agency related social event, birthday party, bridal shower, Holiday party or similar event, about which you would like to issue information **please contact the Chief Operating Officer or designee for permission to use Agency e-mail for such specific purpose.**

All e-mail users should:

- Be courteous and follow accepted standards of etiquette.
- Protect others' privacy and confidentiality.
- Consider organizational access before sending, filing, or destroying e-mail messages.
- Protect their passwords (if used).
- Remove informal messages, transient records, and reference copies in a timely manner.
- Comply with Agency and department policies, procedures, and standards.

Policy Review and Update

The Vice President of MIS unit will periodically review and update this policy as new technologies and organizational changes are planned and implemented. Questions concerning this policy should be directed to the Vice President of MIS.