APM 1-98: Use of the City's Communication Information Systems

Purpose

To establish the City's Communication Information Systems ("CCIS") user policy and provide guidelines regarding proper practices for use of the City's telecommunications devices and network resources.

Policy

The City of Miami provides telecommunication devices and network resources to employees to support the effective and efficient delivery of services to civilians. Such devices and resources include, but are not limited to, computers, cellular telephones, pagers, facsimile equipment, access points, switches, routers, data, data storage devices, network-capable devices, internet and e-mail service, phones, radios, scanners, printers, copiers, telecommunication equipment, wireless transmission equipment and devices, and any other related City owned or operated information technology hardware or software resources.

Privacy

Telecommunication equipment is provided to support official City business. Employees are not entitled to any rights of privacy should said equipment be used for personal purposes. The City reserves the right to monitor all internet/intranet use, e-mail, and other transmissions created or received by City employees with the CCIS. In addition, the City reserves the right to audit and/or review all computer data created or stored on City equipment or printed.

Florida Public Records Law

Unless otherwise exempt by Florida Statutes, all communications made in the course of official City business and/or through the use of City owned or operated telecommunication equipment are considered public records under Florida Statutes, Chapter 119. As such, upon request, the City must make available for inspection and/or provide copies of, all public records, including electronic documents.

Continued on next page

Continued

Prohibited Practices

All City employees shall abide by the standards for appropriate use established in this policy and confine their activities to the conduct of official City business. Prohibited practices include, but are not limited to:

1. Use of the technology and network resources in violation of Federal, State or local laws, regulations, administrative orders, or departmental rules.
2. Activities subjecting the City to civil or criminal activity, including:
    a. Illegal discrimination based upon protected status; or
    b. Copyright or software license violations; or
    c. False advertising.
3. Bypassing, or attempting to bypass, security measures ("hacking"), or exploiting vulnerabilities present in the City's network.
4. Use of the City's telecommunication and information systems for personal gain.
5. Violations of personnel or departmental rules.
6. Distributing messages that are political or religious in nature, or are abusive, threatening, pornographic or sexually explicit, discriminatory or convey hate, or are otherwise offensive or harassing to an employee or member of the public.
7. Disclosing a personal password or using any means to obtain and/or utilize the passwords of others without authorization.
8. Maliciously damaging or deleting another user's files.
9. Originating or intentionally propagating computer viruses, spam and/or chain letters.
10. Playing recreational games, except as part of an instructional tutorial.
11. Attempting to circumvent security restrictions, except when authorized.
12. Installing hardware or software onto the City's network or computers without the appropriate approvals.
13. Storing data files for unacceptable use as defined by this administrative policy or other Federal, State or local laws.
14. Broadcasting messages to all users, except when approval is obtained from the City Manager or his/her designee.
15. Any other use not in the course of conducting official City business.

Continued on next page

Continued

Enforcement Violations of this Administrative Policy subject the employee to disciplinary action up to, and including, termination.

Policy Number: **APM 1-98**
Date: 3/10/2010

Issued By: _____
Carlos A. Migoya
City Manager

REVISIONS

REVISED SECTION	*DATE OF REVISION*
Created	April 10, 1998
Revised	March 2010

Continued on next page

Notice to Employee

I have received a copy of the City of Miami's APM 1-98: Use of the City's Communication Information Systems ("CCIS") and have read said APM in its entirety. I recognize that City policy regarding use of the CCIS will continue to evolve and requires periodic review for any updated information.

I understand that all CCIS, including e-mail, facsimile, internet and intranet, shall be used for conducting only official City business in a professional manner and that use of such systems for personal purposes is strictly prohibited.

I agree to abide by the regulations as stated in this APM for the duration of my employment with the City of Miami and understand that failure to comply with the provisions contained herein may result in disciplinary action up to, and including, termination of employment and/or prosecution, if appropriate.

Employee Signature _____ Date _____

Employee Printed Name _____ Social Security No. _____

Department _____

City of Miami
City Communication Information Systems (CCIS)
Guideline Manual

January 12, 2000

1. Purpose / Scope

The City of Miami ("City") is making every effort to provide its employees with the best technology available to conduct the City's official business. In this regard, the City has installed, at substantial expense, equipment such as computers and advanced technological systems such as electronic mail (e-mail) for use to conduct its official business. This document was created to advise all users regarding the access to and the disclosure of information created, transmitted, received and stored via the use of the Internet, City e-mail, and other City Information Technology Systems (collectively referred to as the "City's information systems"). For purposes of these policies and guidelines, the City's information systems do not include those information systems designed to be confidential, so long as they are not put on the Internet or Web.

As a City employee, you are expected to make appropriate use of the provided computer resources. You must use computer resources only for authorized purposes following established procedures; be responsible for all activities on your assigned computer; access only files and data that are your own, which are publicly available, or to which you have been given authorized access; use only legal versions of copyrighted software; be considerate in your use of shared resources; abide by City policies. Employees must not make inappropriate use of computer resources provided by the City.

The City's policy regarding the use of information systems is, among other things, intended to guide you in the performance of your duties as a City employee. It is also intended to place you on notice that you should not expect the Internet and e-mail in your possession or those that you use from time to time, and their contents, to be confidential or private. All data, including any that is stored or data printed as a document is subject to audit and review. **THERE IS NO EXPECTATION OF PERSONAL PRIVACY IN THE USE OF THE CITY'S INFORMATION SYSTEMS (INCLUDING THE INTERNET AND E-MAIL.)**

Accordingly, the City reserves the right to monitor Internet use, all e-mail, and other computer transmissions, as well as any stored information, created or received by City employees with the City's information systems. The reservation of this right is to ensure that public resources are not being wasted and to ensure that the City's information systems are operating as efficiently as possible in order to protect the public interest. All computer applications, programs, work-related information created or stored by employees on the City's information systems, are City Property.

The use of public resources for personal gain and/or private use, such as but not limited to, outside employment or for political campaign purposes, by City employees, is prohibited and punishable by disciplinary action. The term public resource as used in this policy includes not only the unauthorized use of equipment, hardware, software or other tangible articles, but also the employee time engaging in the unauthorized use while on duty.

The Florida Public Records Act (FPRA) requires the City to make all public records available for inspection and to provide copies upon request. A public record is any writing (which includes electronic documents) relating to the conduct of the public's business prepared, owned, used, or retained by the City. The FPRA includes a number of exceptions from the disclosure requirement. Any information on the City's information system may be subject to disclosure under the FPRA. If there is some doubt, the employee should contact his or her department management or the City Attorney for advice as to whether the information is a public record.

This document addresses general City-wide information systems policies, specific issues related to appropriate use of the City's information systems, the content and use of departmental pages, and employee use of the Internet and e-mail. All departments and employees are required to follow these general policies and guidelines. Specific departments may have unique requirements and are encouraged to develop policies to cover those issues. The law and associated policy regarding the use of Internet, e-mail and voice **mail are** continually evolving. Accordingly, review of the policies and guidelines will **occur** with regularity, and changes shall be made as required.

Each designated department Internet liaison is responsible for their respective employees use of the Internet, and for the contents of their department's information presented using these media. Designated department Internet liaisons are encouraged to actively pursue electronic means of presenting information and services to the public, and to encourage cooperation and participation with the City's Web Council.

The intent of the policy is to permit maximum freedom of use consistent with State Law, City policy, and a productive working environment. The policy applies to all those who use City computers. Depending on the seriousness of an offense, violation of the policy can result in disciplinary action.

ALL CITY EMPLOYEES WITH ACCESS TO INFORMATION SYSTEMS ARE REQUIRED TO READ, UNDERSTAND AND ABIDE BY THE CITY'S POLICIES.

2. General Computer Use Policy

The following rules require strict adherence. Any infraction thereof could result in disciplinary action.

The use of computers is restricted to "official City business". Personal use of or time spent for personal gain is strictly prohibited. A user account name must be obtained through your department. Once a user account name has been issued, you are responsible for the security of your account password and you will be held responsible for all use or misuse of your account. You must maintain secure passwords and never use an account assigned to another user.

Hacking is the unauthorized attempt or entry into any other computer. Never make an unauthorized attempt to enter any computer. Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.

Never copy or transfer electronic files without permission from your department information technology liaison.
Copying a file from a diskette can bring viruses with it. Scan files from diskettes prior to copying to a hard drive with City standard virus prevention software. The City's technical support desk must approve all applications before they can be installed on a computer. No unauthorized applications may be installed on a computer.
Never send, post or provide access to any confidential City materials or information.

Almost all data and software is subject to the Federal copyright laws. Care should be exercised whenever accessing or copying any information that does not belong to you. Software, which requires purchase or reimbursement for its use, such as shareware (software which can be

downloaded for a certain period of time after which it has to be registered and purchased), requires strict adherence to the terms and conditions specified by the owner unless written permission for unrestricted use has been obtained. No software will be downloaded from the Internet onto any computer unless authorized by the City's technical support desk.

Information regarding access to City computer and communication systems, such as dial up modem phone numbers, is considered confidential. This information must not be made available to third parties without the authorization of the network administrator.

Anti-virus software is installed in file servers to limit the spread of viruses within the network. Scanning of all files and executables will occur daily on the file servers. Workstations will have memory resident antivirus software installed and configured to scan data as it enters the computer. Programs will not be executed nor files opened by applications prone to macro viruses without prior scanning.

All incoming mail and files received across a network must be scanned for viruses as they are received. Virus checking will be performed at firewalls that control access to networks.

All data imported on a computer (from floppy disk, e-mail, or file transfer) will be scanned before being used.

When a virus has been detected, the City's technical support desk will inform all users who may have accessed the same program or data that a virus may have also infected their system. The users will be informed of the steps necessary to determine if their system is infected and the steps to take to remove the virus.

Employees must notify the help desk and their department director if they lose a City computer (e.g., laptop computer, desktop, etc.) and file a police report.

Employees must never leave a laptop unattended. You are obligated to cooperate with any investigation regarding the use of your computer equipment and which your department director has authorized.

Users of City computers should conduct themselves in a manner that promotes a productive working environment. Conduct that creates a disturbance to other users is prohibited; this includes printing or displaying materials that are unsuitable for public display. Conduct that intentionally or negligently interferes with the proper operation of the system or its use by others is prohibited.

Users should consider the following when choosing passwords:
Include digits and punctuation characters as well as letters. **Choose something easily remembered so you don't have to write it down. Passwords should be easy to type quickly so that no one can ascertain what was typed by watching the keyboard. Use two short words and combine them with a special character or number (e.g., COMP#DEPT).** Put together an acronym that has special meaning to you (e.g. FMWSC 1997-Florida Marlins World Series Champions 1997). Passwords and user logon IDs are unique to each user. **Passwords must consist of a minimum of 6 characters (no common names or phrases). Passwords should not have the name of your spouse, child, or dog in it.**

You are responsible for keeping your account password confidential. Failure to do so could result in personnel action. It is required that account holders (authorized users who have been assigned a user code) change their password every 45 days.

Users should screen protect their computer by going to main\control panel\desktop and then clicking on the password protect box. Furthermore, set the screen saver delay to 15 minutes or less.

For users of computers that are accessible to the public (non-secure location), users must password lock their computers whenever they are away from their desks. To password lock your computer, press "Ctrl", "Alt" and "Delete" simultaneously. A menu will then appear that will allow you to password lock your computer.

Successful logons display the date and time of the last logon.

Employees' access to all systems/applications is removed upon termination from the City of Miami. This is in accordance with the Security Access Termination Procedure.

All City employees and other users which have received authorization from the Information Technology Department Director may use the City information systems, including both those facilities requiring an account and those, such as PC's, printers, etc., which may not require an account. Others are not authorized to use City facilities.

Access to either the mainframe systems or PC systems in the City requires a personal account on those systems. Access to any of these systems by any other means is not permitted. To obtain an account on either system, contact the City's Technical Support Desk in the Information Technology Department.

Users shall immediately change their passwords upon receiving a new account, or that account may be disabled.

Accounts on City information systems are to be used only by the rightful owner of the account. The owner of an account is expected to maintain the security of that account, and in no case may others be given the use of that account. Sharing of a computer account with other persons is prohibited; each user must have an individual account. Passwords must be protected, and the user must not leave a machine logged on when the user is not present.

In accepting an account on a City computer system, the owner of the account accepts all responsibility for the use of that account. The owner of an account will be held responsible for any use of an account in violation of the applicable policies, unless prohibited by law or superseding rulings.

In the event that the Information Technology Department technical staff finds a problem with a User's usage of the City's information systems, whether deliberate or inadvertent, and if this usage interferes with the work of other Users and is not immediately resolvable in another manner, the Information Technology Department technical staff may temporarily disable User access to the account and files. In that event, the User may check with the City's Technical Support Desk or the Director of the Information Technology Department to seek clarification and resolution of the problem.

All Users are required to cease their usage of the City's information systems upon termination of their employment in the City. Each account will be disabled immediately following termination of employment in the City, or at the specified expiration date, whichever comes first, unless prior arrangement for account extension is made through the Director of the Information Technology Department. Accounts that have been disabled may be reactivated by contacting the City's

Technical Support Desk in the Information Technology Department, if the User is once again employed in the City.

See the Password Security Procedures section for more information on procedures regarding password activation and termination.

It is the policy of the Information Technology Department to restrict access to a User's files, email, and network transmissions to that User; however, the Information Technology Department cannot guarantee absolute security or privacy of those items. Files are routinely accessed by the system for backup purposes.

Electronic mail, which cannot be delivered "bounces" to the postmaster, a system manager. Network traffic is often monitored for troubleshooting and performance monitoring purposes. System logins and User process initiations are regularly logged and examined. In diagnosing computer problems, it is often necessary for the system manager to look at the system information part of an item to find the problem.

Unfortunately, there is usually no "wrapper" around the User part of the item, so the system manager may see the contents. In addition, configuration files in the User's home directory (forward, login, etc.) may be examined to diagnose problems, or modified by a system manager to accommodate system changes.

Users are also warned that unauthorized access to their files, e-mail and network traffic is possible, and information which must be maintained secret against determined attempts should not be stored on networked systems or should be encrypted. For assistance with information requiring high security, the User should contact the Information Technology Department.

The City's Information systems may be used for any purpose not conflicting with this document, other applicable ordinances, administrative rulings, or laws.

The City's Information Systems may not be used for commercial purposes, except as related to City business or with written approval of the Information Technology Department Director.

Usage of printers and other I/O devices in the City is governed by the policies of the department responsible for the equipment.

Users of City computers shall not consume unreasonable amounts of limited resources. Resources that are in limited supply include laser printing, disk space and, in some cases, machine access itself. Laser printing should be used judiciously; it should not be used for large amounts of copies. The Information Technology Department may impose restrictions or limits on use of resources.
If you must reboot a workstation, wait at least thirty seconds before turning it back on, to avoid damage to the electronics.

Users finding a problem with hardware or software should report it as soon as possible to the City's Technical Support Desk, at the Miami Riverside Center (in person), by telephone (416_1083), or by e-mailing the help desk at XX HELP DESK (1083). The City's Technical Support Desk will handle the problem or forward it to the appropriate staff member for resolution.

Complaints about the City's information systems operations and support may be made to the Director of the Information Technology Department.

3. Password Security Procedures

3.1 Security Access Termination Procedure

An online copy of the form may be obtained by clicking on the following link:
Z: City of MiamiTemplatesAccess Termination Form4_5_99

To ensure that only authorized users have access to the City of Miami's computer applications and databases, a formal Security Access **Termination Procedure** for removing the security access of employees that are no longer authorized to have access has been developed by the Information Technology Department.

Effective immediately, all department directors are to utilize the Security Access Termination (SAT) form as soon as they are aware that an **employee in their department will be terminated from employment, granted an extended leave of absence or transferred to another City department, which results in the employee no longer requiring access to certain applications/databases.** Security changes within the individual department due to promotions or administrative transfers will be the responsibility of the individual department director to notify the appropriate database security administrator(s), and is not covered by this procedure. The form should be sent to the Information Technology Department (ITD) prior to the actual personnel change.

It is imperative that ***all*** systems to which the employee has access are specified on the form. This will prevent employees having access to systems that no longer pertain to their job responsibilities.

> Upon receiving the form from the employee's department director or designee, the ITD will then remove the user from any accounts to which they no longer require access, except for the systems in which ITD does not have control over user access. In these circumstances, the ITD will then forward the form to the appropriate departments (e.g., Police, Fire, and Finance) for processing. These departments will identify the user's account in the system, and remove the user's access to the system on the effective date.

The ITD will disable employees' NT accounts on the effective date listed on the SAT form. The NT account will become completely removed by the ITD 45 days after the effective date. Departments have 6 weeks from the effective date on the SAT to remove all files that will be needed after the 45 days have expired.

To add user access to an application/system, the user's department director or designee must send a memo to the department that maintains the application/system.

Location of the form:
The form can be found in the following location on the shared drive:
Z:\ City of Miami\Citywide Templates\Security Access Termination Form4_5_99

3.2 Password Reinstatement Procedure

Effective immediately, all employees who forget their passwords must submit an e-mail notification or a memo from their department liaison, department director or designee to the help desk. The e-mail should be sent to the help desk at "XX HELP DESK (1083)". Memos should be sent to the City's technical support desk. No passwords will be reinstated without a request from the department liaison, department director or designee.

4. Unacceptable Uses of City Computers

To use the computer for entertainment purposes, such as to play games or surfing to non-business related sites on the Internet.

To access another user's account, files, system or data unless authorized by that individual.

To use another person's password.

To seek information on passwords or data belonging to another individual unless authorized by that individual.

To copy proprietary program software, someone else's files, or programs, or examine such information unless authorized by the owner.

To make or use illegal copies of copyrighted software, storing such copies on city systems, or sending them over networks.

To seek access to or to attempt to circumvent computer security methods or operating systems

To use the City's computer accounts for commercial purposes.

To intercept or examine the content of messages or files in transit on a network.

To interfere with the work of other users of a network or with their host systems, to seriously disrupt the network, or to engage in any uses that result in the loss of another user's files or system.

To engage in any activity that might be harmful to systems or to any information stored thereon, such as creating viruses, damaging files, or disrupting service.

To use computer programs to decode passwords or to access control information.

To attempt to circumvent or subvert system security measures.

To waste computing resources.

Uses that are found to be malicious, harmful, obscene or unethical

Any uses that violate federal, provincial or municipal laws or regulations.

Engaging in any activity that does not comply with the general principles listed at the beginning of this document.

5. Complaint and Violation Resolution Procedure

1) If the Director of the Information Technology Department receives a complaint from a City user or has other reason to suspect a violation of the POLICIES AND GUIDELINES ON THE USE OF CITY INFORMATION SYSTEMS, the Director will initiate a preliminary investigation.

2) The Director of the Information Technology Department will then attempt to determine the legitimacy of the complaint, suspicion or allegation. If the investigation requires the examination of the files, programs, or passwords of individual users, the Director of the Information Technology Department will review the situation with the Assistant City Manager, and receive authorization before proceeding with the investigation.

3) If the investigation finds that a City user is in violation of the POLICIES AND GUIDELINES ON THE USE OF CITY INFORMATION SYSTEMS, one or more of the following actions will be taken:

a) If it appears that the user is in violation of federal, or municipal law or regulations, the Director of the Information Technology Department will consult with the Assistant City Manager, for authorization to refer the matter to the Police Department.

b) If the user is not in violation of federal, or municipal laws or regulations, the Director of the Information Technology Department will meet with the individual(s) and inform them that they are in violation of the City's POLICIES AND GUIDELINES ON THE USE OF CITY INFORMATION SYSTEMS and request that they discontinue any unacceptable usage.

c) If the violation is considered by the Director of the Department of Information Technology to be serious, or if the misuse continues, or if the individual refuses to comply as directed under 3.b, the Director of the Information Technology Department, with authorization from the City Manager, shall have the right to have the user's account suspended while the matter is referred to the appropriate officer or judicial process (e.g., the Department Director, Human Resources Department, Labor Relations Office).

6. City-Wide E-mail Policy

The City encourages its departments to use the e-mail to disseminate information to its employees (collectively called "users") and to carry out official business when such business can be accomplished consistent with the following e-mail policies and guidelines:

Official City Business. Use e-mail to accomplish official City business. Official City business conducted via e-mail shall comply with all statutory requirements as well as standards for integrity, accountability, and legal sufficiency. Thus, official City business conducted via e-mail should meet or exceed the standards of performance for traditional methods (such as meetings, use of telephone, etc.).

Reasons to use the e-mail. Departments should base decisions to use the e-mail on sound business practices. The conduct of business via the e-mail is particularly compelling where costs are reduced and/or services are improved in measurable ways.

Information Management. Disseminate information that is current, accurate, complete, and consistent with City policy. Information released via e-mail is subject to the same official City policies for the release of information via other media (such as printed documents).

Message Distribution. The Office of Labor Relations must first approve e-Mail directed to ALL EMPLOYEES before being sent. E-Mail must also follow the same chain of command rules applied when sending printed documents.

Privacy and Security. City management has the right to monitor and log all transactions in or out of the system.

Professional Image. Use e-mail to promote a professional image for the City.

Official Use. E-Mail resources are made available to City employees to support and promote official City business. It is inappropriate for employees to use these resources for personal use, private gain, to state as "city positions" those which are not officially endorsed by the City, illegal purposes, or for inappropriate use as defined in these policies and guidelines. Individuals sending e-mail will be held responsible for the content of their messages, for ensuring that the information provided relates to their department's official duties and responsibilities, and that its use is for official and not for personal purposes. Users of electronic mail and bulletin boards shall not send messages that are libelous, patently offensive, or that intimidate, threaten, demean, or harass individuals or groups, or that would otherwise bring discredit to the City. Accordingly, all City departments should conduct all existing City business using the above policies.

7. City-Wide Facsimile Policy

The City encourages its departments to use facsimile services to disseminate information to the public and its employees (collectively called "users") to improve communications with the public, and to carry out official business when such business can be accomplished consistent with the following policies and guidelines:

Official City Business. Use facsimile services to accomplish official City business consistent with the City's mission. Official City business conducted via facsimiles shall comply with all statutory requirements as well as standards for integrity, accountability, and legal sufficiency. Thus, official City business conducted via facsimiles should meet or exceed the standards of performance for traditional methods (such as meetings, use of telephone, etc.).

Reasons to use Facsimiles. Departments should base decisions to use facsimiles on sound business practices. The conduct of business via facsimiles is particularly compelling where costs are reduced and/or the services provided to the City's constituents are improved in measurable ways.

Information Management. Disseminate information that is current, accurate, complete, and consistent with City policy. Information released via facsimiles is subject to the same official City policies for the release of information via other media (such as printed documents).

Facsimile Distribution. The Office of Labor Relations must first approve facsimiles directed to ALL EMPLOYEES before being sent. Facsimiles must also follow the same chain of command rules applied when sending other documents.

Privacy and Security. Protect confidential and proprietary information entrusted to the City. City management has the right to monitor and log all transactions in or out of the system.

Professional Image. Use facsimile services to promote a professional image for the City.

Official Use. Facsimile resources are made available to City employees to support and promote official City business. It is inappropriate for employees to use these resources for personal use, private gain, to state as "city positions" those which are not officially endorsed by the City, illegal purposes, or for inappropriate use as defined in these policies and guidelines. Individuals sending facsimiles will be held responsible for the content of their facsimiles, for ensuring that the information provided relates to their department's official duties and responsibilities, and that its use is for official and not for personal purposes. Accordingly, all City departments should conduct all existing City business using the above policies.

8. City-Wide Internet Policies Purpose

The external (or public) City of Miami Official World Wide Web site is a fundamental communication tool for providing critical City information to Miami's residents and the world. The goal of the City Web site is to encourage increased "user" participation in City government and to help create a more vibrant community for residents and visitors alike. The internal (Intranet) web pages provide fundamental and critical information to all employees to assist in accomplishing the City's mission. Toward that end, the Web Site Policy guides the development and use of the City's sites:

8.1 Internet Policies

I. The Information Technology Department (ITD) via the Web Council is responsible for advising City departments regarding the creation and implementation of their respective web pages, helping City departments to comply with the City's Web policies, and maintaining and securing the City's Intranet and Web server and Web site. It is the responsibility of each department's designated Internet liaison to ensure that departmental staff adheres to the Web Site Policies.

II. To preserve the public nature of the City's Web site and to avoid any perception that the City endorses or provides favorable treatment to any private person or business enterprise (hereinafter collectively referred to as "vendor"), no corporate or commercial logos will be allowed on the City's Government section of the external Web site.

III. This requirement does not supersede any other policies or regulations regarding donations. Department Directors will be responsible for complying with those policies and regulations and seek any required City Commission approval for accepting such donations.

IV. It is the City's intent to provide electronic access to its information through a logical single point of entry. For the Internet, this logical point of entry is the City's officially registered domain name. The registration of an individual domain name for a City department or a City related organization is discouraged because each separate domain name fragments the single logical point of entry, would lead to public confusion, and would contribute to administrative, maintenance and mail delivery problems. In addition, statistics would be more difficult to compile.

V. The City's Web site is for "official use" only. All information disseminated through the City's Web site Government section must be related to the official duties and responsibilities of employees and City departments.

VI. The Florida Public Records Act applies to information processed, sent and stored on the Internet. Confidential information should not be posted on the City's external Web site. Each designated department Internet liaison must approve all posted information. For questions regarding the Florida Public Records Act contact the City Attorney.

VII. In addition to the requirements of policy 6 above, each designated department Internet liaison is responsible for the acceptability of the content contained in their respective Web pages.

VIII. No City official's web page may be used for campaign related purposes. No City employee or official may use any other City departmental Web page for campaign related purposes. Such campaign related purposes include, but are not limited to, the following: statements in support or opposition to any candidate or ballot measure; requests for campaign funds or references to any solicitations of campaign funds; and references to the campaign schedule or activities of any candidate. The City Clerk's Office is available to provide guidance and assistance to elected officials and their staffs in complying with this guideline. No City official's web page may link to any private web site related to a candidate's campaign for elective office, but it may link directly to the home page of the Office of the City Clerk's election related pages where general election and candidate information can be found. Further, the City Clerk's Office is available to provide similar guidance and assistance to the City's department Directors.

IX. To encourage participation in and heighten voter interest regarding City elections, the Office of the City Clerk will be responsible for providing candidate, ballot and voter information on its web page and will seek ways to provide similar election related information via that page.

9. Employee's Internet Usage Policy

The following rules require strict adherence. Any infraction thereof could result in disciplinary action. Disciplinary actions range from verbal warnings to termination; the severity of the misbehavior governs the severity of the disciplinary action.

- The use of Internet is restricted to "official City business". Personal use of or time spent for personal gain is strictly prohibited. Authorization for Internet access must be obtained through your department. Once authorization is approved you are responsible for the security of your account password and you will be held responsible for all use or misuse of your account. You must maintain secure passwords and never use an account assigned to another user.
- The City routinely monitors usage patterns for its e-mail/Internet communications. The reasons for this monitoring are many, including cost analysis/allocation and the management of the City's gateway to the Internet. All messages created sent, or retrieved over the City's e-mail/Internet are the property of the City and should be considered public information. The City reserves the right to access and monitor all messages and files on the City's e-mail/Internet system as deemed appropriate.

Employees should therefore, not assume electronic communications are totally private and should transmit highly confidential data in other ways.

- Hacking is the unauthorized attempt or entry into any other computer. Never make an unauthorized attempt to enter any computer. Such an action is a violation of the Federal Electronic Communications Privacy Act (ECPA) 18 U.S.C. § 2510.
- Sending threatening, slanderous, racially and/or sexually harassing messages is strictly prohibited.
- The representation of yourself as someone else, real or fictional, or a message sent anonymously is prohibited.
- Never copy or transfer electronic files without permission. Copyrighted materials belonging to entities other than the City may not be transmitted by employees on the City's e-mail/Internet system. All employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials, except with permission, or as a single copy to reference only. Failure to observe copyright or license agreements may result in disciplinary action.
- Downloading a file from the Internet can bring viruses with it. Scan all downloaded files with City standard virus prevention software. All software downloaded must be registered to the City. Employees should contact the City's Technical Support Desk if they have any questions.
- Never send, post or provide access to any confidential City materials or information.
- Almost all data and software is subject to the Federal copyright laws. Care should be exercised whenever accessing or copying any information that does not belong to you. Software that requires purchase or reimbursement for its use, such as shareware, requires strict adherence to the terms and conditions specified by the owner unless written permission for unrestricted use has been obtained. When in doubt consult your designated department Internet liaison or designee.

You are obligated to cooperate with any investigation regarding the use of your computer equipment and which your department's Director has authorized.

Chain letters are letters that are sent to several people with a request that each person sends copies of the letter to an equal number of people. Chain letters are illegal and may not be transmitted through e-mail. Users should notify the ITD if they receive any chain letters. They should indicate who sent the letter, and the nature of the letter. The network administrator can then remind all City employees that chain letters are illegal, and to immediately discard any letters sent to them.

E-mail requires extensive network capacity. Sending unnecessary e-mail, or not exercising constraint when sending very large files, or sending to a large number of recipients consumes network resources that are needed for critical City business. When the City grants an individual employee access to the network, it is the responsibility of the employee to be cognizant and respectful of network resources.

Any employee found to be abusing the privilege of City facilitated access to e-mail or the Internet, will be subject to corrective action up to and including termination. If necessary, the City also reserves the right to advise appropriate legal officials of any illegal violations.

10. Employee's Internet Usage Guidelines

10.1 Internet Sites

If you are using information from an Internet site for strategic City business decisions, you should verify the integrity of that information. You should verify whether the site is updated on a regular basis (the lack of revision date might indicate out-of-date information) and that it is a valid provider of the information you are seeking. Just because it is there does not mean that it is accurate or valid.

ITD has no control or responsibility for content on an external server not under the control of the City. Information may be offensive and/or unsuitable for dissemination.

10.2 Electronic Mail (E-mail)

The following guidelines apply to the use of e-mail

MAIL ON THE INTERNET IS NOT SECURE. Never include in an e-mail message anything that you want to keep private and confidential because e-mail is sent un-encrypted and is easily read.

Management has the right to access all e-mail files created, received or stored on City-funded systems and such files can be accessed without prior notification.

Be careful if you send anything but plain ASCII text as e-mail. Recipients may not have the ability to translate other documents, for example Word or Word Perfect documents, or encoding in UUENCODE or MIME.

Be careful when sending replies-- make sure you are sending to a group when you want to send to a group, and to an individual when you want to send to an individual. It is best to address directly to a sender(s). Check carefully, the "To" and "From" before sending mail. It can prevent unintentional errors.

Include a signature (an identifier that automatically appends to your e-mail message) that contains the method(s) by which others can contact you. (Usually your e-mail address, phone number, fax number, etc.)

For important items, let senders know you have received their e-mail, even if you cannot respond in depth immediately. They need to know their e-mail is not lost.

Watch punctuation and spelling. It can reflect on your professionalism. Use automatic checking programs if available.

Each employee is responsible for the content of all text, audio or images that they place or send over the City's e-mail/Internet system. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else. All messages communicated on the City's e-mail/Internet system should contain the employee's name.

Any messages or information sent by an employee to another individual outside of the City via an electronic network (e.g., bulletin board, on-line service or Internet) are statements that reflect the City.

While some users include personal "disclaimers in electronic messages, there is still a connection to the City, and the statements may be tied to the City.

All communications sent by employees via the City's e-mail/Internet system must comply with this and other City policies and may not disclose any confidential or proprietary City information.

Do not attach files over 5MB in size to e-mail messages. Instead, copy the file to an appropriate share point visible to the intended recipients(s). Once the recipients have secured the file, ensure that it has been removed from the share point. E-mail the file to the recipient, and request that the recipient(s) download the file to their local machine(s).

- All communications sent by employees via the City's e-mail/Internet system must comply with this and other City policies and may not disclose any confidential or proprietary City information.
- Do not attach files over 5MB in size to e-mail messages. Instead, copy the file to an appropriate share point visible to the intended recipients(s). Once the recipients have secured the file, ensure that it has been removed from the share point. E-mail the file to the recipient, and request that the recipient(s) download the file to their local machine(s).

11. Internet Mailing Lists and Usenet Groups

The e-mail guidelines apply here as well.

Actively disclaim speaking for the City unless you have authority to do so. Note that if you use a City system to post an article, the City's name is carried along with what you post in (at least) the headers. Users posting messages to newsgroups or Internet mailing lists must include a disclaimer as part of each message stating that the opinions expressed are not necessarily those of the City of Miami.

However, if the message posted is considered offensive, the disclaimer will become meaningless.

- Managers are responsible for ensuring that employees understand Internet acceptable use policy.
- Access to the Internet from a City computer used at home must adhere to all the same policies that apply to use from within the City's facilities. Employees must not allow access to family members or other non-employees of company computer systems.
- Be sure to change your mailing address if your account changes. Do not simply forward your e-mail from your old account to your new one. This creates a burden on the City's information systems. Be careful when using auto reply features in e-mail when you belong to mailing lists. Auto-reply replies are often sent to the entire list indiscriminately and your reply may not be important to all on the list (e.g. most do not care that you are on vacation, and worse, your message may have been intended for only one recipient).
- As a new member of a ***news group***, monitor the messages for a while to understand the history and personality of the group. Jumping right into the discussion may make you look foolish if you lack background information.

- Do not re-post any messages without permission. Even messages may have copyright protection.
- Do not post personal messages to a mailing list or USENET news group.
- If you survey the group, as a courtesy, post a summary of the results.
- Be sure to properly acknowledge with quotations any material borrowed from others. Be careful of plagiarism.
- Do not post any messages anonymously. The professional community views this practice as bad form. As a matter of policy the USENET community and system managers are asked to track down offenders.
- Be careful when you re-post any requests. Some requests are fraudulent.
- State the subject of your message clearly in the subject line.
- Before joining mailing lists and news groups give thought to how much time these activities require. Also, for USENET, look at the *news. Announce. new users* group. It contains information to assist you.
- Be sure to read the Frequently Asked Questions (FAQs) for your group(s).
- Never send angry messages (flames). If you receive a "flame", do not over react. Remember that not everyone is as polite as you are.

12. Unacceptable Uses of Internet and E-mail

- The City's e-mail and Internet systems may not be used for transmitting, retrieving or storage of any communications of a discriminatory or harassing nature or materials that are obscene or X-rated.
- Harassment of any kind is prohibited.
- No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted.
- No abusive, profane or offensive language is to be transmitted through the City's e-mail or Internet system.
- Electronic media may also not be used for any other purpose that is illegal or against City policy or contrary to the City of Miami's best interest. Solicitation of non-City business or any use of the City's e-mail or Internet for personal gain is prohibited.

13. File Transfer Protocol (FTP)

These guidelines cover use of FTP (or download) sites.

- Do not FTP to any system on which you do not have an account, or which does not advertise anonymous FTP services.
- Downloaded files may contain viruses. Scan all downloaded files with the City's standard virus prevention software.
- Observe working hours or posted hours for FTP sites. Most sites request that you NOT FTP between their local hours of 8 am_5 pm
- Do not FTP during your site's prime hours due to network impact on other users.
- Look locally before downloading a file from a geographically remote site. Your department's designated Internet liaison can help you find the closest site.

- Do not download on the off chance you will "need it someday." Conversely, do not search for "neat stuff' to FTP. If you discover that you do not need what you have downloaded, delete it. You can always get it again if you discover you need it later.
- Observe any posted restrictions on the FTP server.
- Login using your real user name and node address as your password on anonymous FTP servers.

14. Netiquette

These are Netiquette (see Glossary) guidelines:

- Be cognizant of system etiquette. The computer you use may have limits regarding disk space usage. E-mail takes up space; therefore, you should regularly delete and/or archive any messages you wish to save.
- Remember that the recipient is a person with feelings. Since they cannot see you, they may not know when you are joking. Be sure to include visual or verbal clues. Convention indicates the use of the smiley" face. :) (Look sideways).
- DO NOT SEND MESSAGES ALL IN CAPITALS. It looks as if you are shouting. Use initial capitals or some other symbol for emphasis. For example: That IS what I meant. That *is* what I meant.
- Remember that some people have to pay for each byte of data they receive. Please keep messages to the point without appearing terse or rude.

15. Glossary

Account: An assigned user code and password that gives authorization and access to a City Communication Information System. Internet/Intranet, E-Mail, and general PC sign on accounts are issued by the Information Technology Department.

Domain Name: A domain name is the way to identify and locate an address on the Internet. The domain name, also called the fully qualified domain name or FQDN, is a computer's name in text form, for example: ci.miami.fl.us. The domain name is used to send e- mail, make FTP requests, etc. Before any message is sent on the Internet, the domain name is converted internally to a numerical address, an Internet protocol address, which is what computers on the Internet deal with directly.

Electronic Mail: Electronic Mail (e-mail) may include non-interactive communication of text, data, images or voice messages between a sender and designated recipient(s) by systems utilizing telecommunications links. It may also include correspondence transmitted and stored electronically using software facilities called "e-mail", "facsimile", or "messaging" system; or voice messages transmitted and stored for later retrieval from a computer system.

FTP (file transfer protocol): A program that allows you to transfer data between different computers on a network.

Guidelines: Recommendations derived from experience and which should be used.

Hacking: Attempting to break into another system on which you have no account or authorization.

Internet: A worldwide network of networks, connecting informational networks communicating through a common communications language, or "protocol".

Intranet: A private TCP/IP based network using browser technology (which means it works just like the (Internet) that allows everyone in an organization the capability to review or update information that would normally be placed on an organization bulletin board (e.g., a calendar of events, a status board, pictures of events or employees, policy changes, employee phone directory, etc.).

I/O Devices: Input/Output devices such as printers, scanners, etc.

Mailing list: A service that sends e-mail to everyone on a list whenever e-mail is sent to the service, permitting a group of users to exchange e-mail on a particular topic.

MIME: A protocol that lets Internet users attach non text files to e-mail messages. Stands for Multipurpose Internet Mail Extension, lets users send mail in any format including graphic images, formatted documents, and audio, video and compressed data files.

Netiquette: A combination of "network" and "etiquette". It is the practice of good manners in a networked environment.

News groups: Discussion groups with common themes on USENET.

Policy: Primary objectives of the City as contained in this document. Postmaster: A person responsible for administering Internet E-mail. Resources: Any part of the computer system that can be shared, such as directories, printers, hard drives and CD ROM drives.

Shareware: Software that can be downloaded for a specified period of time (usually for evaluation purposes) after which it has to be bought and/or registered, or removed.

Standards: Departmental directions or instructions describing how to achieve policy. It is a mandatory statement of direction.

System Manager: A person responsible for the administration of computer systems. TELNET: A program that allows remote login to another computer.

TCP/IP: Transmission Control Protocol/Internet Protocol; the communication protocol used by computers connected to the Internet.

USENET: A collection of computer discussion (news) groups. Users: The public and City employees.

UUENCODE: A utility that converts binary files on PC into ASCII files. Stan~ for UNIX to Unix Encode and was first developed for use with UNIX computers.

Vendors: Any private person or business enterprise.

Web Pages: Comparable to pages within a book, these are documents within a web site that can contain links to other pages on the web.

Web Site: Comparable to a book, it is a collection of web pages containing a home page (table of contents) on the World Wide Web.

World Wide Web: Comparable to a big library on the Internet of web sites throughout the world giving you a graphical, easy-to-navigate interface for looking at documents.

16. Client Agreement

ALL CITY EMPLOYEES ARE REQUIRED TO READ, UNDERSTAND AND ABIDE BY THE CITY'S POLICIES.

I have read and understand all of the policies in the City of Miami City Communication Information Systems Guideline Manual (CCIS). I understand that failure to abide by policies within this manual can result in sanctions against me, up to and including termination from employment with the City of Miami.

Employee's printed name : _____
Employee's Signature : _____
Date : _____