City of Monroe, Georgia

Information Technology Policy

I. Section 1: Information Security

A. Overview: Information Security policies aim to preserve:

1. **Confidentiality** - Access to Data shall be confined to those with appropriate authority.

2. **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.

3. **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

B. Purpose: The aim of this section is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by City of Monroe by:

1. Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.

2. Describing the principals of security and explaining how they shall be implemented in the organization.

3. Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.

4. Creating and maintaining within the organization a level of awareness of the need for Information Security as an integral part of the day to day business.

5. Protecting information assets under the control of the organization.

C. Scope: This section applies to all information, information systems, networks, applications, locations and users of the City of Monroe or supplied under contract to it. This policy applies to all equipment that is owned or leased by the City of Monroe.

D. Responsibilities for Information Security

1. Ultimate responsibility for information security rests with the Chief Executive of City of Monroe, but on a day-to-day basis the Network Administrator shall be responsible for managing and implementing the policy and related procedures.

2. Supervisors are responsible for ensuring that their permanent and temporary staff and contractors are aware of:

a. The information security policies applicable in their work areas

b. Their personal responsibilities for information security

c. How to access advice on information security matters

3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

4. The Information Technology Policy shall be maintained, reviewed and updated by the Network Administrator. This review shall take place annually.

5. Supervisors shall be individually responsible for the security of their physical environments where information is processed or stored.

6. Each member of staff shall be responsible for the operational security of the information systems they use.

7. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

8. Agreements with external contractors that allow access to the organization's information systems shall be in operation before access is allowed. These agreements shall ensure that the staff or sub-contractors of the external organization shall comply with all appropriate security policies.

E. Information Security Awareness Training

1. Information security awareness training shall be included in the staff induction process.

2. An ongoing awareness program shall be established and maintained by the Network Administrator in order to ensure that staff awareness is refreshed and updated as necessary.

F. Security Control of Assets

1. Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset (i.e., if you are assigned a specific piece of equipment/software, you are responsible for it). All assets not so designated shall be the responsibility of the Network Administrator

G. Access Controls: Only authorized personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

H. User Access Controls: Access to information shall be restricted to authorized users who have a bona-fide business need to access the information unless otherwise provided for by law.

I. Computer Access Control: Access to computer facilities shall be restricted to authorized users who have business need to use the facilities.

J. Application Access Control: Access to data, system utilities and program source libraries shall be controlled and restricted to those authorized users who have a legitimate business need (i.e., systems or database administrators). Authorization to use an application shall depend on the availability of a license from the supplier.

K. Equipment Security: In order to minimize loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

L. Computer and Network Procedures: Management of computers and networks shall be controlled through standard documented policy and procedures that have been authorized by the Mayor and/or City Council.

M. Information Security Events and Weaknesses: All information security events and suspected weaknesses are to be reported to the Network Administrator. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

N. Protection from Malicious Software: The organization shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organization's property without permission from the Network Administrator. Users breaching this requirement may be subject to disciplinary action.

O. System Change Control: Changes to information systems, applications or networks shall be reviewed and approved by the Network Administrator.

P. Intellectual Property Rights: The organization shall ensure that all information products are properly licensed and approved by the Network Administrator. Users shall not install software on the organization's property without permission from the Network Administrator.

II. Section 2: Acceptable Use

A. Overview

1. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP; are the property of the City

of Monroe. These systems are to be used for business purposes in serving the interests of the government, and of our citizens in the course of normal operations.

2. Effective security and efficient operation is a team effort involving the participation and support of every City of Monroe employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

B. Purpose: The purpose of this policy is to outline the acceptable use of computer equipment and systems at the City of Monroe. These rules are in place to protect the employee and the City of Monroe. Inappropriate use exposes the City of Monroe to risks including virus attacks, compromise of network systems and services, and legal issues.

C. Scope: This section applies to employees, contractors, consultants, temporaries, and other workers at the City of Monroe, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the City of Monroe.

D. General Use and Ownership

1. While the City of Monroe's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the government systems remains the property of the City of Monroe. Because of the need to protect the City of Monroe's network, and the availability of information to the public under the Open Records Act, we cannot guarantee the confidentiality of information stored on any network device belonging to the City of Monroe.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3. Any information that users consider sensitive or vulnerable should be encrypted.

4. For security and network maintenance purposes, authorized individuals within the City of Monroe may monitor equipment, systems and network traffic at any time.

5. The City of Monroe reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

E. Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

2. All PCs, laptops and workstations are secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off (control-alt-delete for Win2K+ users) when left unattended.

3. Because information contained on portable computers is especially vulnerable, special care should be exercised.

4. Postings by employees from a City of Monroe email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not those of the City of Monroe, unless posting is in the course of business duties.

5. All hosts used by the employee that are connected to the City of Monroe Internet/Intranet/Extranet, whether owned by the employee or the City of Monroe, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

6. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

F. Unacceptable Use

1. The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

2. Under no circumstances is an employee of the City of Monroe authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the City of Monroe-owned resources.

3. The lists contained herein below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

G. System and Network Activities

1. The following activities are strictly prohibited unless required by the scope of your assigned job duties:

    a. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or

regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City of Monroe.

b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City of Monroe or the end user does not have an active license is strictly prohibited.

c. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

d. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

e. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done from home.

f. Using a the City of Monroe computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

g. Making fraudulent offers of products, items, or services originating from any City of Monroe account.

h. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

i. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

j. Port scanning or security scanning is expressly prohibited unless prior notification to the Network Administrator is made.

k. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

l. Circumventing user authentication or security of any host, network or account.

m. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

n. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

o. Providing information about, or lists of, the City of Monroe employees to parties outside the City of Monroe.

H. General Internet Policy

1. Internet Use Limited to City Business: The City's Internet capabilities may be used for City business purposes only. The term "Internet" means the electronic information system of that name which connects smaller groups of linked computer networks. The term "City's Internet Capabilities" means any and all access to the Internet obtained through City sponsorship, ownership, or financial contribution, or by any employee or officer as a representative or agent of the City. The term "City business purposes" means the official work of City government undertaken for public benefit, as opposed to activities undertaken for personal, non-City or private purposes. Unacceptable sites or uses include, but are not limited to the following:

a. Pornographic sites and access to pornographic materials.

b. Use of the City Internet to harass employees, vendors, customers, and others.

c. Sports or games.

d. Online wagering or gambling sites.

e. Use of the City Internet for partisan political purposes.

f. Unauthorized transfer of copyrighted materials utilizing City Internet capabilities.

g. Any site that charges a fee (unless there has been prior written approval of justified City expense item by supervisor).

h. Vendor sites to purchase personal items.

i. Marketing of personal or private business.

2. Employees may be provided with access to the Internet to assist them in performing their jobs. Use of the Internet, however, must be tempered with

common sense and good judgment. To that end, employees' use of the internet shall not in any way interfere with their job performance; therefore, employees shall not waste time on the Internet.

3. Duty not to waste computer resources. Employees must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic. Because audio, video and picture files require significant storage space, files of this or any other sort may not be downloaded unless they are business-related.

4. If you abuse your right to use the Internet, it will be taken away from you. In addition, you may be subject to disciplinary action, including possible termination, and civil and criminal liability.

5. Disclaimer of liability for use of Internet. The City of Monroe is not responsible for material viewed or downloaded by users from the Internet. Users are cautioned that many internet pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. In addition, having an email address on the Internet may lead to receipt of unsolicited email containing offensive content. Users accessing the Internet do so at their own risk.No expectation of privacy. The computers and computer accounts given to employees are to assist them in performance of their jobs. Employees should not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to the City and may only be used for business purposes.

6. Monitoring computer usage. The City has the right, but not the duty, to monitor any and all of the aspects of its computer system, including, but not limited to, monitoring sites visited by employees on the Internet, monitoring chat groups and news groups, reviewing material downloaded or uploaded by users to the Internet, and reviewing email sent and received by users.

7. Blocking of inappropriate content. The City may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by City networks. In the event you nonetheless encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to company blocking software.

8. Prohibited activities. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise

unlawful, inappropriate, offensive (including offensive material concerning sex, race, color, national origin, religion, age, disability, or other characteristic protected by law), or violative of the City of Monroe's equal employment opportunity policy and its policies against sexual or other harassment may not be downloaded from the Internet or displayed or stored in the City's computers. Employees encountering or receiving this kind of material should immediately report the incident to their supervisors.

9. The City of Monroe's equal employment opportunity policy and its policies against sexual or other harassment apply fully to the use of the Internet and any violation of those policies is grounds for discipline up to and including discharge.

10. Games and entertainment software. Employees may not use the company's Internet connection to download games or other entertainment software, including wallpaper and screen savers, or to play games over the Internet.

11. Illegal copying. Employees may not illegally copy material protected under copyright law or make that material available to others for copying. You are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to copy or download. You may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of your supervisor.

12. Accessing the Internet. To ensure security and to avoid the spread of viruses, employees accessing the Internet through a computer attached to the City's network must do so through an approved Internet firewall. Accessing the Internet directly by modem is strictly prohibited unless the computer you are using is not connected to the City's network.

13. Virus detection. Files obtained from sources outside the City, including disks brought from home; files downloaded from the Internet, newgroups, bulletin boards, or other online services; files attached to e-mail; and files provided by customers or vendors may contain dangerous computer viruses that may damage the City's computer network. Employees should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from sources outside of the City of Monroe, without first scanning the material with City-approved virus checking software. If you suspect that a virus has been introduced into the City's network, notify your supervisor immediately.

14. Sending unsolicited e-mail (spamming). Without the express permission of their supervisors, employees may not send unsolicited e-mail to persons with whom they do not have a prior relationship.

15. Amendments and revisions. This policy may be amended or revised from time to time as the need arises. Users will be provided with copies of all amendments and revisions.

16. Violations of this policy will be taken seriously and may result in disciplinary action, including possible termination, and civil and criminal liability.

17. Use of the Internet via the City of Monroe computer system constitutes consent by the user to all of the terms and conditions of this policy.

I. Email and Communications Activities

1. Unless otherwise stated, all directives below apply to use of city government provided email accounts.

2. Limited occasional use of personal email accounts is acceptable during business hours and using city resources. However, the email system shall not be used for:

a. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

b. Any form of harassment via email, whether through language, frequency, or size of messages.

c. Unauthorized use, or forging, of email header information.

d. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

e. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

f. Use of unsolicited email originating from within the City of Monroe's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the City of Monroe or connected via the City of Monroe's network.

g. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

3. No expectation of privacy. The email accounts given to employees are to assist them in the performance of their jobs. Employees have no right of personal privacy in any matter stored in, created, received, or sent over the City of Monroe’s email system.

4. The City of Monroe, in its discretion as owner of the email system, reserves and may exercise the right to monitor, access, retrieve and delete any matter

stored in, created, received, or sent over the email system, for any reason and without the permission of any employee.

5. Even if employees use a password to access the email system, the confidentiality of any message stored in, created, received, or sent from the City of Monroe email system still cannot be assured. Use of passwords or other security measures does not in any way diminish the City of Monroe's rights to access materials on its system, or create any privacy rights of employees in the messages and files on the system. Any password used by employees must be revealed to the City of Monroe as email files may need to be accessed by the company in an employee's absence.

6. The City of Monroe's policies against sexual or other harassment apply fully to the email system, and any violation of those policies is grounds for discipline up to and including discharge. Therefore, no email messages should be created, sent, or received if they contain intimidating, hostile, or offensive material concerning race, color, religion, sex, age, national origin, disability or any other classification protected by law.

7. The email system may not be used to solicit for religious or political causes, commercial enterprises, outside organizations, or other non-job related solicitations.

8. Management approval is required before anyone can post any information on commercial online systems or the Internet. Any approved material that is posted should obtain all proper copyright and trademark notices. Absent prior approval from the City of Monroe to act as an official representative of the City of Monroe, employees posting information must include a disclaimer in that information stating, "Views expressed by the author do not necessarily represent those of the City of Monroe."

9. Employees are reminded to be courteous to other users of the system and always to conduct themselves in a professional manner. Emails are sometimes misdirected or forwarded and may be viewed by persons other than the intended recipient. Users should write email communications with no less care, judgment and responsibility than they would use for letters or internal memoranda written on City of Monroe letterhead.

10. Because email records and computer files may be subject to discovery in litigation, the City of Monroe employees are expected to avoid making statements in email or computer files that would not reflect favorably on the employee or the City of Monroe if disclosed in a litigation or otherwise.

11. Any employee who discovers misuse of the email system should immediately contact their supervisor.

12. Violations of the City of Monroe's email policy may result in disciplinary action up to and including discharge.

13. The City of Monroe reserves the right to modify this policy at any time, with or without notice.

J. Blogging and Social Networking

1. Blogging and Social Networking by employees, whether using the City of Monroe's property and systems or personal computer systems attached to the city network, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of the City of Monroe's systems to engage in blogging and social networking is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the City of Monroe's policy, is not detrimental to the City of Monroe's best interests, and does not interfere with an employee's regular work duties. Blogging and social networking from the City of Monroe's systems is also subject to monitoring.

2. The City of Monroe's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any City of Monroe confidential information.

3. Employees shall not engage in any blogging or social networking that may harm or tarnish the image, reputation and/or goodwill of the City of Monroe and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging and social networking or otherwise engaging in any conduct prohibited by the City of Monroe's Non-Discrimination and Anti-Harassment policy.

4. Employees may also not attribute personal statements, opinions or beliefs to the City of Monroe when engaged in blogging or social networking. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the City of Monroe. Employees assume any and all risk associated with blogging and/or social networking.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the City of Monroe's trademarks, logos and any other the City of Monroe intellectual property may also not be used in connection with any blogging or social networking activity.

K. Definitions

1. Blogging – Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

2. Spam – Unauthorized and/or unsolicited electronic mass mailings.

3. Social Networking – Membership and participation in a social structure made of nodes (which are generally individuals or organizations) that are tied by one or more specific types of interdependency, such as values, visions, ideas, financial exchange, friendship, sexual relationships, kinship, dislike, conflict or trade. (i.e.: MySpace, Facebook, Twitter, Ebay).

L. Voice Mail Policy

1. Every City of Monroe employee is responsible for using the Voice Mail system properly and in accordance with this policy. Any questions about this policy should be addressed to your supervisor.

2. The Voice Mail system is the property of the City of Monroe. It has been provided by the City of Monroe for use in conducting official business. All communications and information transmitted by, received from, or stored in this system are official records and property of the City of Monroe.

3. Employees have no right of personal privacy in any matter stored in, created, received, or sent over the City of Monroe Voice Mail system.

4. The City of Monroe, in its discretion as owner of the Voice Mail system, reserves and may exercise the right to monitor, access, retrieve, and delete any matter stored in, created, received, or sent over the Voice Mail system, for any reason without the permission of any employee and without notice.

5. Even if employees use a password to access the Voice Mail system, the confidentiality of any message stored in, created, received, or sent from the City of Monroe Voice Mail system still cannot be assured. Use of passwords or other security measures does not in any way diminish the City of Monroe's rights to access materials on its system, or create any privacy rights of employees in the messages and files on the system. The City of Monroe may request employee’s passwords as Voice Mail messages may need to be accessed by the City in an employee's absence.

6. Even though the City of Monroe reserves the right to retrieve and read any Voice Mail messages, those messages should still be treated as confidential by other employees and accessed only by the intended recipient.

7. The City of Monroe’s policies against sexual or other harassment apply fully to the Voice Mail system, and any violation of those policies is grounds for discipline up to and including discharge. Therefore, no Voice Mail messages should be created, sent, or received if they contain intimidating, hostile, or offensive material concerning race, color, religion, sex, age, national origin, disability or any other classification protected by law.

8. The Voice Mail system may not be used to solicit for religious or political causes, commercial enterprises, outside organizations, or other non-job related solicitations.

9. Employees are reminded to be courteous to other users of the system and always to conduct themselves in a professional manner. Voice Mails are sometimes misdirected or forwarded and may be heard by persons other than the intended recipient. Users should create Voice Mail communications with no less care, judgment and responsibility than they would use for letters or internal memoranda written on City of Monroe letterhead.

10. Employees should also use professional and courteous greetings on their Voice Mail boxes so as to properly represent the City of Monroe to outside callers.

11. Because Voice Mail records and messages may be subject to discovery in litigation, City of Monroe employees are expected to avoid making statements in Voice Mail that would not reflect favorably on the employee or the City of Monroe if disclosed in a litigation or otherwise.

12. Any employee who discovers misuse of the Voice Mail system should immediately contact your supervisor.

13. Violations of the City of Monroe's Voice Mail policy may result in disciplinary action up to and including discharge.

14. The City of Monroe reserves the right to modify this policy at any time, with or without notice.

City of Monroe, Georgia

Employee Statement of Policy Acceptance

I, the undersigned, hereby acknowledge receipt of the Information Technology Policy. I understand that I am expected to read and abide by said policies as a result of my employment by the City of Monroe, Georgia.

_____ Employee Signature

_____ Witness

_____ Date

City of Monroe, Georgia

Intellectual Property Rights Statement Agreement

Definition: Intellectual properties (IP) are legal property rights over creations of the mind, both artistic and commercial, and the corresponding fields of law. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; ideas, discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property include copyrights, trademarks, patents, industrial design rights and trade secrets.

Intellectual property rights are a bundle of exclusive rights over creations of the mind, both artistic and commercial. The former is covered by copyright laws, which protect creative works, such as books, movies, music, paintings, photographs, and software, and gives the copyright holder exclusive right to control reproduction or adaptation of such works for a certain period of time.

The second category is collectively known as "industrial properties", as they are typically created and used for industrial or commercial purposes. A patent may be granted for a new, useful, and non-obvious invention and gives the patent holder a right to prevent others from practicing the invention without a license from the inventor for a certain period of time. A trademark is a distinctive sign which is used to prevent confusion among products in the marketplace.

An industrial design right protects the form of appearance, style or design of an industrial object from infringement. A trade secret is an item of non-public information concerning the commercial practices or proprietary knowledge of a business. Public disclosure of trade secrets may sometimes be illegal.

The term *intellectual property* denotes the specific legal rights described above, and not the intellectual work itself.

Policy: It shall be the policy of the City of Monroe, Georgia that all employees agree in writing that they will not use previous employers or clients intellectual property in a manner or degree which would violate Federal, State, or Local laws during the official discharge of their associated duties with the City of Monroe.

_____ Employee Signature

_____ Date

_____ Witness