City of Hammond

IT Policy and Procedure Manual
(Chapter XI of the Employee Handbook)

Adopted: May 18, 2010 by Ordinance N^{o} 10-5702 C.S.

Table of Contents

Rule XI-1 Appropriate Use of Information Technology Resources

A. PURPOSE

The purpose of this policy is to provide direction to members of TEAM Hammond regarding safe and responsible use of technology resources and the responsibilities they have for protecting and efficiently using such resources at the City.

B. DEFINITIONS

Intellectual Property:
Anything that fits into one or more of the following categories:

- A potentially patentable machine, article of manufacture, composition of matter, process, or improvement to any of these; or
- An issued patent; or
- A legal right that inheres in a patent; or
- Anything that is copyrightable (in legal terms, this means anything that is an original work of authorship, fixed in a tangible medium or expression)

System Security Mechanism:
A procedure or program used with a computer to implement or enforce access controls, auditing, authentication, confidentiality, authorization, policy enforcement and other security issues.

User ID:
The name you use to identify yourself when logging onto a computer system or online service. Both a username (user ID) and a password are required. In an Internet e-mail address, the username is the left part before the @ sign.

Domain Name:
A human readable name used to describe a computer network (e.g. www.hammond.org) whose registration is coordinated by the Internet Corporation for Assigned Names and Numbers (ICANN). Each name corresponds to an IP address (e.g. 192.168.1.57) used for Internet addressing and routing.

C. APPLICABILITY

This policy is applicable to all individuals (whether full-time or part-time and including but not necessarily limited to, the following: administrators, staff, interns, affiliates, vendors) who have been given or obtained access to computer equipment, systems and networks owned or operated by the City of Hammond. The policy further includes any and all methods or means of access, whether initiated from on or off site. The policy applies to all City IT resources and all privately owned resources that are connected to City systems or networks.

D. POLICY

Access to computer equipment, systems and networks owned or operated by The City of Hammond is a privilege granted by the city and governed by certain regulations and restrictions. These include rules defined by the City as well as all applicable local, state, and federal laws. This policy provides general guidance and may be supplemented by additional

regulations governing particular sub-systems of the City computing environment or network.

In case of conflict, the regulations in this policy supercede the supplemental policies. The City has provided these systems and networks to support its mission or service to the citizens of Hammond, and their intended uses are grounded by being robust and secure in pursuit of that mission.

The City, through its IT department, pledges to provide its authorized users the most reliable system and network access possible. In return, the user agrees to abide by the regulations set forth by this Appropriate Use Policy. This means that the user agrees to behave ethically, appropriately, and responsibly while using these systems and network resources. In particular, the City expects all users to:

- Respect intellectual property
- Respect the ownership and confidentiality of computer-based data, services, and system security mechanisms
- Respect individuals' rights to privacy and to freedom from intimidation and/or harassment
- Use and operate computing resources in a manner that minimizes the risk to privacy, data, services, and network operations
- Responsibly use shared resources in a way that does not adversely affect their availability to others
- Upon notification of activity or behavior that violates this policy or any supplemental policy, to discontinue such activity immediately
- Report inappropriate use, and
- Use resources and systems for their intended purposes
- Respect the integrity of data

Any person who has a question about this policy, or is concerned about a potential violation by him/herself or by another person, is encouraged to contact the IT Department. Individuals who witness a violation of the Appropriate Use Policy should report the incident immediately to the IT Department.

E. PROCEDURES

By using the City's information technology resources, each and every user accepts responsibility for his/her behavior, the operation of their computer, and all activities performed using their user ID. He or she also agrees to conduct him or herself appropriately, especially as follows:

Respect intellectual property

Individuals shall:

- Not make or use illegal copies of copyrighted software or music, store such copies on City systems, or transmit such copies over City networks
- Follow all vendor software and hardware licensing requirements
- Not otherwise infringe upon the copyrights of others
- Ensure that all use of copyrighted material accords with the fair-use provision (see http://en.wikipedia.org/wiki/Fair_use)
- Protect from unauthorized use any copyrighted material to which he or she has authorized access.

Respect the ownership and confidentiality of computer-based data, services, and system security mechanisms

Individuals shall:

- Access only files, data, and services that he/she owns
- Access only files, data, and services to which he/she has been given authorized access by the owner or official designee
- Not attempt or assist in attempts to gain unauthorized access to:
  - Passwords
  - Access control information
  - Data, services, computing resources, or network resources
  - Computing facilities
- Not use another person's password
- Not divulge passwords and other access control information to others
- Not conduct unauthorized scanning of computer network connected devices and systems

Respect individuals' rights to privacy and to freedom from intimidation and harassment

Individuals shall:

- Not use computing resources, including the City network and e-mail system, with the intention to harass, intimidate, threaten, or otherwise harm another person, whether directly or indirectly
- Not use unauthorized electronic means to eavesdrop, collect, or disclose information about others.

Use and operate computing resources in a manner that minimizes the risk to privacy, data, services, and network operations

In the cases where the City's systems or network is accessed remotely, it is important to notice that improper operation of a computer accessing the City remotely can result in the compromise of or operational disruption of the City network and attached services and data. Thus there are special requirements related specifically to remotely connected computers. They are as follows:

- Ensure that available protection mechanisms, such as anti-virus software, are used on all computers connecting remotely to the City Network
- Ensure that software on computers connecting to or accessing the City network is regularly updated to preclude exploits of know defects
- Ensure that software on computers connecting to or accessing the City network is not configured in such a way that it allows the compromise of the computer
- Ensure that operators of computing resources connecting or accessing the City network use and operate those resources in ways that are appropriate

Responsibly use shared resources in a way that does not adversely affect their availability to others

Many City of Hammond computing and network resources are shared. In order for these resources to be available to the entire team, individuals must show cooperation and respect in their use.

Individuals shall:

- Refrain from monopolizing system or network resources
- Respond to official requests to desist from activity that monopolizes resources by ceasing the activity causing the problem
- Not waste computer time, connection time, disk space, printer paper, manuals, or other resources
- Not attempt or assist in attempts to adversely affect shared resources

Upon notification of activity or behavior that violates this policy, to discontinue such activity immediately and immediately report inappropriate use

In the case that inappropriate computer activity is observed, contact the IT department at ext. 5666 or ext. 5665 as soon as possible.

Use resources and systems for their intended purposes

Individuals shall:

- Not use another person's password
- Not divulge passwords or other access control information to others
- Not use the City's systems or network for personal gain, for example:
  - By selling access to his/her user ID and/or password, to City computing or to network resources to anyone
  - By performing work for profit or by another commercial action, using the City's systems or network resources in a manner not authorized by the City.
- Not conduct political activity in a manner not authorized by the City using the City's computer systems or network.
- Abide by:
  - All rules, regulations, policies and procedures adopted by the City,
  - All instructions given by staff members
- Not use City resources or computers attached to the City network to falsify identity for example by:
  - Providing "pass through" service
  - Sending electronic mail under forged names
- Not engage in any activity that alters wired or wireless network connections, access points, topology, or the physical wiring of City-owned resources
- Register network connected computers as current rules, regulations, policies, and procedures specify
- And, as City employees
  - Not install or operate computer games on City-owned machines for ANY reason, for example: Yahoo Games, etc.
  - Not violate any statute or regulation of the State of Louisiana or any of its agencies applicable to municipalities.

Respect the integrity of data

- Refrain from intentionally creating any false record or entering any information incorrectly in any City computer system.

F. RESPONSIBILITIES

Because of their leadership positions and control over resources, TEAM leaders play a critical role in the protection of the City of Hammond's information resources. Specifically, their influence should be used to:

- Ensure that security is given appropriate consideration, along with functionality, performance, ease-of-use, cost, and availability, in the planning and implementation of new projects and services.
- Make computer security a staffing, funding, and training priority.
- Change attitudes and behaviors within the units they lead by communicating the importance of addressing security issues and by requiring all staff members to be responsible and accountable for the security of their network connected devices and their use of City computer resources.
- Ensure device owners and overseers in their units take swift action should a security breach or violation of these policies occur and that they seek help from IT if needed.

By using the City's information technology resources, each and every user accepts responsibility for his/her behavior, the operation of their computer, and all activities performed using their user ID.

G. SANCTIONS

The City considers any violation to be a serious offense in its efforts to preserve the privacy, data, and services of individuals and the City. In the case an investigation is begun related to policy and/or legal violations, the IT department reserves the right to access, examine, intercept, monitor, and copy the files, network transmissions, and/or actual terminal sessions of any user. The IT department may choose to suspend a user's access to its resources in connection with the investigation of any of the following:

- Violations or suspected violations of security and/or policies
- Terminal interactions which may be contributing to poor computer performance
- Computer malfunctions

In connection with such investigations, users whose files, network transmissions, or terminal sessions are affected are deemed to have acknowledged that:

- They are not entitled to any expectation of privacy with regard to their files, data, or communications, which may be shared with the appropriate investigating officials. In general, the City will exercise discretion as far as is appropriate given the case
- The Director of Human Resources and the violator's Supervisor will be notified of the violation and provided with information and materials relating to the investigation and/or violation

The responses for violation of this policy may include, but are not necessarily limited to the following:

- Notification: alerting a user to what appears to be an inadvertent violation of this policy in order to educate the user to avoid subsequent violations.
- Warning: alerting a user to the violation, with the understanding that any additional violation will result in a greater penalty.
- Loss of computer and/or network privileges: limitation or removal of computer and/or network privileges, either permanently, partially, or for a specified period of time.
- Restitution for damages: requiring reimbursement for the costs of repairs to or replacement of computer-related material, equipment, hardware, software, data and/or facilities.

In addition, violators may be subject to disciplinary action (which may include suspension or termination) as may be prescribed by other rules, regulations, handbooks, procedures or policies applicable to the violator. Furthermore, the violator may be subject to civil suit or ordinances, laws, statutes, or regulations of the City of Hammond, the State of Louisiana, or the United States of America.

Sanctions will be commensurate with the severity and/or frequency of the offense and may include termination of employment; however termination of employment does not fall under the realm of the IT Department.

H. EXCLUSIONS

None.

I. INTERPRETATION

Authority to interpret this policy rests with the Mayor and Director of Administration, and is generally delegated to the Director of the IT department.

Rule XI-2 Password Management

A. PURPOSE

This policy promotes effective password management and assigns specific responsibilities for password selection and use.

B. DEFINITIONS

Password management:
The selection, distribution, protection, use, modification, and testing of computer system passwords.

C. APPLICABILITY

This policy applies to passwords for access to all City owned systems and networks and the persons who hold them.

D. POLICY

Effective password management is the most important single element in assuring the overall security of the City's information systems and the protection of its information assets.

All individuals who use information technology resources of the City shall adhere to the principles of good password management.

E. PROCEDURES

These procedures will provide guidelines for selecting good passwords, minimum requirements for password length, characteristics and renewal cycles, testing procedures, and other information. All computer users are required to familiarize themselves with these procedures and adhere to their content. The IT department will assure that these procedures are periodically reviewed and that their content is appropriate to support the overall password management and information security environment of the City.

E.1 Minimum Standards for Un-privileged Accounts (normal users)

Un-privileged accounts are those created for a specific individual and purpose and that do not include the ability to create or modify additional accounts; modify system data or files or those belonging to other users; or perform application or database functions outside the control of the application system for which the account was issued.

Following are the **minimum** standards for passwords to un-privileged accounts on all multi-user systems and for all Microsoft Windows workstations. Multi-user systems are those where more than one user accesses or shares the resources (ex: MUNIS, Alpha, Remote,). These standards shall be used on all systems unless there is a technical reason why they cannot be used. In such cases, the reasons and impacts of deviating from the standard will be documented and reviewed by IT before such a system is installed and/or connected to the City network.

For unprivileged access to a system or application, the **minimum** password standards are:

- Minimum password length: 7 characters
- Specific Characteristics: All passwords must contain a combination of uppercase letters, lowercase letters, numbers, and punctuation. Passwords must include at least 3 of the 4 types of characters.
- Passwords may not contain any part of your name.
- Passwords will expire every 90 days.
- The last 5 passwords used are retained and may not be reused.

E.2 Minimum Standards for Privileged Accounts (system administrators)

Privileged accounts are those created with elevated capabilities and are generally used by system or application administrators. Privileged accounts may include the ability to create or modify additional accounts; modify system data or files or those belonging to others; or perform application or database functions outside the control of the application system for which the account was issued. Because of the additional capabilities associated with privileged accounts, they carry additional responsibilities for their owners. Privileged accounts should be used only when their additional capabilities are truly necessary. Routine work should be done with unprivileged accounts whenever possible.

In light of the potential impact of a breach or misuse of a privileged account, the following, more rigorous, minimum requirements must be strictly observed:

- An approval request must be on file. Elevated privileges must be appropriately documented, approved, and acknowledged.
- An annual review of the status of privileged accounts must be performed to assure/validate that the additional privileges remain necessary and are being used wisely.
- Minimum password length: 10 characters
- Specific Characteristics: All passwords must contain a combination of uppercase letters, lowercase letters, numbers, and punctuation. Passwords must include at least 3 of the 4 types of characters.
- Passwords will expire every 90 days.
- The last 5 passwords used are retained and may not be reused.

E.3 Additional Requirements

If a technical complication exists that prevents these standards from being implemented on a system or in an application, the IT department will review the situation, make a decision, and document what was decided in the event that an exception must be made.

E.4 Guidelines for selecting good passwords

The responsibility for effective password management is shared by all users of the City's computer resources and begins with selecting good passwords. To assist in this process, consider the following general guidelines:

- Good passwords are passwords that are difficult for either a human or a machine to guess. They have the following characteristics:
    - They are not a word found in any dictionary
    - They have no significance in the real world ex: pet names, license numbers
    - They contain both upper and lower case letters

    - They contain at least one numeral
    - They contain at least one punctuation mark
    - They are of sufficient length (7 characters for unprivileged accounts/10 characters for privileged accounts)
- Use a phrase or sentence to assist you in remembering character strings. For example, add a number or symbol "I like to fish for bass" can be iltFfB1 as a password.
- **NEVER share your personal passwords!** Do not give out your passwords to IT or system personnel or technical support (ex: MUNIS support) during help sessions. The password is your protection that only you have access to your data and data owned by the City and accessed from your account. **The owner of the login credentials is responsible for ALL activity that occurs under its use.**
- If you have several computer accounts, you may wish to have the same password on every machine and/or application. However, if you have the same password on many accounts and it is compromised, all of your accounts are compromised. Therefore, be sure to select passwords appropriately and **NEVER** use the same password for both privileged and non-privileged accounts.

F. RESPONSIBILITIES

All who access or administer the City's information technology resources share responsibility for effective password management. Specific responsibilities are assigned as follows:

- Password testing and monitoring will be conducted by IT staff through ongoing review and evaluation of system and network security. This will include vulnerability scans, testing the strength of passwords, or performing other activities aimed at evaluating overall risk.
- All users experiencing problems with logging on due to invalid, expired, or forgotten passwords are to contact IT staff at ext. 5665 or 5666 to have the problem checked into and if necessary have their password reset.
- Users who suspect that their password or account has been compromised should immediately contact IT staff at ext. 5665 or 5666

G. SANCTIONS

Sanctions will be commensurate with the severity and/or frequency of the offence and may include termination of employment for severe offenses; however, termination of employment does not fall under the realm of the IT department.

H. EXCLUSIONS

None.

I. INTERPRETATION

Authority to interpret this policy rests with the Mayor and Director of Administration and is generally delegated to the Director of the IT department.

Rule XI-3 Electronic Messaging

A. PURPOSE

Electronic messaging systems at the City of Hammond provide a medium for information exchange and are provided for support service and administrative activities.

This policy sets forth responsibilities and procedures that shall direct the use of the City of Hammond's electronic messaging systems, both internally and in conjunction with the global electronic community.

B. DEFINITIONS

Electronic Messaging:
The use of communications mechanisms such as electronic mail (e-mail), bulletin boards, lists, websites, blogs, etc. to deliver or circulate information electronically.

C. APPLICABILITY

This policy applies to all individuals and/or technical mechanisms that use information technology resources of the City for electronic messaging functions.

D. POLICY

All members of TEAM Hammond are encouraged, if they are available, to use electronic messaging resources and are expected to do so in an appropriate manner.

Since electronic messaging systems may carry information in the form of personal and/or casual communication as well as official City of Hammond data, care must be taken to ensure that the two are clearly distinguished. Explicit statements of content or format shall distinguish all official City correspondence distributed electronically. **Electronic forms of communication at the City of Hammond are NOT for personal use. They shall also not be used for anything not directly related to City of Hammond business.**

E. PROCEDURES

In order to assure a level of common understanding and have an effective policy, all those who use electronic messaging systems must familiarize themselves with and abide by procedures that govern their individual and common use of electronic messaging systems. These procedures include the following:

- Technical constraints: Messages are sent through electronic messaging systems using store and forward technology. This means that the messages typically pass through multiple systems, some of which may not be fully secure or reliable.
- While privacy cannot be assured on all systems in a particular message route, IT will work to assure system security and availability on the computer systems it administers. Additionally, IT personnel who carry advanced privileges will not read private messages except as required in pursuit of security or system management anomalies and will do so under the direction of IT management. Recipients of electronic messages must also be aware that the identity of the

message may or may not be authentic. Even though the identity of the message sender is not authenticated by many of the current messaging systems, forgeries are nonetheless unacceptable. Also, senders must be aware that delivery of a message cannot be fully assured. As with paper mail, response from the recipient is the only reliable way to determine that a message has been read.

- Transportation versus storage: While there is a limited amount of storage space for new/incoming messages contained in the messaging systems, it is not to be used for long-term storage or archive. Instead, electronic messaging systems are to be considered a transportation mechanism. As with any transportation mechanism, the related issues of system failure and recovery should be considered. While IT will perform periodic backups of messages in transit, these should be viewed as insurance against system failure, not as a mechanism to restore individual messages except in the case of a public records request. Local backups of message originals should be made for any critical communications. Individuals are responsible for the long-term storage of electronic messages ensuring that they reside in areas that are adequately protected. **Backups will not be used to restore copies of messages that were deleted or lost.**
- Cost: The costs associated with electronic messages are unlike those for traditional paper-based mail. The cost of electronic messages is born primarily by the recipient(s), not the sender. Therefore, no junk/spam mail shall be sent using City messaging systems. Specific examples of junk mail are: chain letters, advertisements, and other unsolicited mass mailings as well as excessive or inappropriate postings to message boards or websites.
- Shared Resource: Messaging systems use many network and computing resources that are shared by all of TEAM Hammond, as well as services shared by the world. The individual services, collectively referred to as electronic messaging, each evolved to address a particular need and are designed to make efficient use of resources in a given situation. Therefore, messages should be sent using the technology appropriate to the task and in keeping with City policies regarding appropriate use (see Appropriate Use Policy). Some typical guidelines for various services include:
    - E-Mail: person-to-person communication
    - Mass E-mail: small group discussions
    - WWW: information distribution
- Message Content: The content of any message sent through the messaging system is the sole responsibility of the individual sending the message. Harassment, obscenity, forgery, and other illegal forms of expression are not acceptable use of City resources. The only enforceable restrictions on content of electronic messages are those that apply generally to verbal or written communication (slander, harassment, etc.). When such restrictions need to be enforced, the same administrative, judicial, and criminal processes as for non-computer communication may be invoked; use of electronic messaging systems does not change what is and is not an illegal communication.
- The City will not censor or regulate messages based on content or views expressed by the sender or implied by the receipt. Transmission of information by electronic means does not negate intellectual property rights, copyrights or other protections.
- Public Records: All electronic documents at the City are considered public record just like any paper document. All electronic messages are saved for this purpose by the City's messaging and backup software. Any communication made through an electronic system must be provided if a public records request for them is made. At any time electronic files, data, or communications may be reviewed as

necessary for these requests; therefore, individuals are not entitled to an expectation of privacy with regard to their files, data or communication.

F. RESPONSIBILITIES

Electronic messaging systems by their very nature depend on the shared effort and responsibility of all who participate in and manage their use. Disruptions, whether by technical or behavioral means, can impact availability and usefulness for an entire community of users.

The IT Department is responsible for ensuring reliable, secure and efficient operation of the City's electronic messaging systems. IT shall also give access to those TEAM members who require it, and will provide instruction on its use, if and when it is needed, to those users that require it.

TEAM members have additional responsibilities by virtue of their access to a variety of data stored in City computer systems and applications. All laws governing the access of City information by the public shall be followed in use of City electronic messaging systems.

G. SANCTIONS

This policy pertains to electronic messaging specifically, but as with other computing and communications resources, users are subject to the City's policy regarding appropriate use of information technology resources and other City policies and procedures (e.g. public records requests), state and federal laws as applicable.

The IT department reserves the right to manage its electronic messaging resources to ensure overall utility and accessibility. This includes, but is not limited to suspension or revocation of access to electronic messaging resources if they are abused.

Sanctions will be commensurate with the severity and and/or frequency of the offense and may include termination for severe offenses; however, termination of employment does not fall under the realm of the IT department.

H. EXCEPTIONS

None.

I. INTERPRETATION

Authority to interpret this policy rests with the Mayor and Director of Administration, and is generally delegated to the Director of the IT Department.

Rule XI-4 Electronic Mail (E-Mail) Retention

A. PURPOSE

The purpose of this policy is to ensure that electronic mail is maintained in accordance with approved records retention policies, accepted record keeping practices and laws as required by LA R.S. Title 44.

B. DEFINITIONS

Transitory e-mail:
E-mails having limited or no administrative value to the City of Hammond and not essential to the fulfillment of statutory obligations or to the documentation of the City of Hammond

C. APPLICABILITY

This policy applies to all that use City of Hammond electronic messaging systems. This policy does not apply to transitory e-mail records generated or received by the City or its employees.

Transitory information includes the following: unsolicited and junk e-mails not related to city work, Listserv and other e-mail broadcast lists that require subscription (including newspapers), reminders for meetings and events (e.g. cake in the conference room, staff meeting moved from 2:00 p.m. to 3:00 p.m.), and personal non-work related e-mails received by employees.

There is no retention requirement for transitory messages. Public officials and employees receiving such communications may delete them immediately.

It should be noted that e-mail should NOT be used for personal purposes. This includes things such as personal online bill payment notifications, e-mails from friends or relatives, jokes and chain messages, memberships to non-work related websites (e.g. Facebook, Twitter, etc.), or to receive special offers or “coupons” from retailers.

D. POLICY

Retention of electronic mail must be based on content, not on media type, artificial duration (e.g. 90 days) or on storage limitations. E-mail should be retained for the same duration as other records of similar content included in a given record series on an approved retention schedule. If the message cannot be classified by content, then it must be maintained for at least three years before it is removed from the messaging system.

E. PROCEDURES

Electronic messages must be classified by content and kept according to the retention schedule of their respective departments.

F. RESPONSIBILITIES

In order to keep e-mail systems functioning efficiently, it is the responsibility of the IT Department to maintain a basic e-mail retention schedule. Any e-mail in someone’s mail

box (e.g. Inbox, Deleted Items, Sent Items, etc.) will automatically be deleted from the mail server when it becomes three years old. All items placed in the Deleted Items area of a user's mailbox will be automatically deleted a day after they have been placed there.

The e-mail user's responsibility is to categorize their e-mail and archive the items required to be kept longer than three years in their respective department's document archive. This can be in the form of an Outlook .pst file, a Word document, or any other means deemed adequate by their department. If the user or department does not wish to archive e-mails, then they will be removed from the e-mail system according to the basic e-mail retention schedule setup by the IT Department.

Each user should remove transitory messages from their mail box each day. All transitory and/or personal messages left in a mailbox are considered public record at the initiation of a public records request and are also subject to discovery should they be requested in the course of litigation. E-mail users should have no expectation of privacy should one of these requests be made.

G. SANCTIONS

The IT department reserves the right to change the basic retention schedule at any time to fulfill at least the minimum requirements set forth by the State of Louisiana and/or the City of Hammond.

Sanctions will be commensurate with the severity and/or frequency of the offence and may include termination of employment for severe offences; however, termination of employment does not fall under the realm of the IT department.

H. EXCLUSIONS

None.

I. INTERPRETATION

Authority to interpret this policy rests with the Mayor and Director of Administration, and is generally delegated to the Director of the IT department.

Rule XI-5 Access Control

A. PURPOSE

This policy outlines how computer access is granted and terminated and defines specific responsibilities of those involved in the account creation and termination process.

B. DEFINITIONS

Access Control:
Mechanisms and policies that restrict access to computer, network and information resources.

Remote Access:
The ability to log onto a network from a distant location. Generally, this implies a computer, an internet connection, and some remote access software such as Microsoft Terminal Services Client, to connect to the network.

C. APPLICABILITY

This policy is applicable to all individuals (whether full-time or part-time and includes, but is not limited to, the following: administrators, staff, interns, affiliates, vendors) who are to obtain or be removed from access to computer equipment, systems and networks owned or operated by the City of Hammond. The policy further includes any and all methods or means of access, whether initiated from on or off site. The policy applies to all City IT resources and all privately owned resources that are connected to City systems or networks.

D. POLICY

Access control is an important part of the City of Hammond's computer resource security. All access given to City employees, interns, vendors, etc. will be given though a well documented "paper trail" process. When access is to be terminated, it will be done in a speedy manner that is also well documented on paper.

E. PROCEDURES

Gaining Access

Access to the City's computer and network resources is granted in 2 ways. Generally, when a new or current employee needs access, a form supplied by the IT department shall be completed by the Human Resources department or the employee's supervisor and delivered to the IT department for review and activation of the account. Access may also be granted on an as needed basis by the IT department. This is for special cases only and all forms must be completed and signed before access is given. The IT department reserves the right to create multiple accounts for system administration and testing purposes at any time.

At times it is necessary that third party vendors have access to the City's systems and network for the purpose of hardware and software upgrades, implementation of new hardware or software, or to gather information from the City's computer systems for other purposes. These vendors must fill out a Vendor Access Request form and agree to the

vendor confidentiality and indemnity agreement (*see Appendix*). The forms should be turned in to the IT department after completion for review and activation of access. Access will be given for no more than the length of time the vendor will be providing services to the City.

Remote Access

Sometimes it is required that remote access is available to those holding normal access to the City's computer network and systems. Each request is reviewed on an individual basis before access is given. Access from the outside of the City's network is kept at a minimum to maintain security. To get remote access a Remote Access Request form (*see Appendix*) must be filled out and signed by the required parties. Depending on the case, remote access may be granted on a permanent basis or may only be allowed for a specified amount of time. The IT department reserves the right to decide how long access will be granted. **Submission of a remote access request form does not guarantee that remote access will be granted.**

Termination of Access

When an employee ceases employment with the City for any reason, the Human Resources department shall notify the IT department that the employee's computer access be terminated. This should take place before the employee's last day so that the account may be disabled the evening of their last day. It is sometimes necessary for an account to remain active after the employee ceases employment with the City. Many times this is the case with system administrator accounts. In these cases the same notification from the Human Resources department should be sent. The IT department will change the passwords on the user's accounts and continue to use them for administrative purposes. Any time someone with system administrator privileges ends employment with the City, all system passwords shared in the IT department shall also be changed. Access given to vendors and remote access given to users will terminate automatically on the day specified when the access was first given.

F. RESPONSIBILITIES

The Human Resources department and/or employee supervisor is responsible for making requests that access be granted or terminated for employees. The IT department is responsible for making sure new access requests are filled in a prompt manner, for making sure accounts are disabled at their scheduled times, and for assuring that all paperwork is completed correctly and completely before any access is given. The IT department will keep track of all forms turned in to the department and give a copy of all access forms for employees to Human Resources to be placed in employee files.

G. SANCTIONS

The IT department reserves the right to manage access to maintain system security. This includes, but is not limited to suspension or revocation of access to City information resources, networks, or systems if they are abused.

Sanctions will be commensurate with the severity and/or frequency of the offence and may include termination of employment for severe offences; however, termination of employment does not fall under the realm of the IT department.

H. EXCLUSIONS

None.

I. INTERPRETATION

Authority to interpret this policy rests with the Mayor and Director of Administration, and is generally delegated to the Director of the IT department.

Rule XI-6 Information Security

A. PURPOSE

This policy assigns responsibility for the security of departmental, administrative and other critical City of Hammond information. Components of security include confidentiality, availability, and integrity.

B. DEFINITIONS

Information technology resources:
Specific items such as telecommunications devices, computer systems, media, and other equipment, goods, services, and personnel related to the collection, storage or transport of electronic information.

Critical data:
Data that is so important to the City of Hammond that the loss or unavailability is unacceptable.

C. APPLICABILITY

This policy applies to all information collected, and/or processed using the City's information technology resources.

D. POLICY

City information and information technology resources must be recognized as sensitive and valuable and be protected. Depending on the scope and nature of the information, integrity constraints and special procedures for access and handling may be required.

One of the fundamental requirements and goals of City information processing, whether manual or automated is to manage a single resource: information. This goal drives all others as the City works to define, manage, guard the integrity of, bring access to, and mobilize this resource. The individual data elements and their interface to the larger process must be protected and managed.

E. PROCEDURES

Departments shall develop, manage and review their own operating policies and procedures and include information security as part of their department's processes. Integrity constraints, procedures that ensure correct processing of correct data, shall be written as departmental procedure. Such procedures should be reviewed as required, at least once a year.

F. RESPONSIBILITIES

The IT department is responsible for:

- Ensuring the security, confidentiality, and availability of data and software stored on individual computers and on centrally-managed computer systems.
- Ensuring the backup of critical data and software
- Providing account management

- Establishing and maintaining the physical security of the central computing facilities.
- Establishing and maintaining the physical security of the communications network.
- Establishing and maintaining the physical security of data for which the Information Technology Department (IT) is the custodian.

This policy also places responsibility on TEAM Leaders to:

- Encourage appropriate computer use as specified in the Appropriate Use of Information Technology Resources policy
- Ensure compliance with information technology policies and standards by people and services under their control
- Implement and monitor additional procedures as necessary to provide appropriate security of information and technology resources within their area of responsibility.

G. SANCTIONS

Sanctions will be commensurate with the severity and/or frequency of the offense and may include termination of employment; however, termination of employment does not fall under the realm of the IT department.

H. EXCLUSIONS

None.

I. INTERPRETATION

Authority to interpret this policy rests with the Mayor and Director of Administration, and is generally delegated to the Director of the IT department.

Rule XI-7 Communications Use

A. PURPOSE

The purpose of this policy is to provide direction to members of TEAM Hammond regarding safe and responsible use of Communications systems and the responsibilities they have for protecting and efficiently using such resources at the City.

B. DEFINITIONS

Collect Call:
A call received where the caller is requesting that the City be charged for the call.

Communications Equipment:
Equipment such as radios, postage machines, etc. that does not fit into the category of telecommunications equipment.

Operator Assisted Call:
Calls or services requiring the assistance of an outside operator.

Telecommunications Equipment:
Telephones, fax machines, modems, or any device that connects and operates on the City's telecommunications network or cellular telephones owned by the City.

C. APPLICABILITY

This policy is applicable to all individuals (whether full-time or part-time and including but not necessarily limited to, the following: administrators, staff, interns, affiliates, vendors) who have been given or obtained access to communications or telecommunications equipment, systems and networks owned or operated by the City of Hammond. The policy further includes any and all methods or means of access, whether initiated from on or off site. The policy applies to all City communications resources and all privately owned resources that are connected to City systems or networks.

D. POLICY

Access to communications equipment, systems and networks owned or operated by The City of Hammond is a privilege granted by the city and governed by certain regulations and restrictions. These include rules defined by the City as well as all applicable local, state, and federal laws. As a general rule, telecommunications equipment is to be used for City business only.

E. PROCEDURES

Telecommunications equipment is to be used for City business only. The following rules should also be followed.

- Employees may make local, non-charged telephone calls for personal business during lunch or "break" periods only.

- Emergency calls regarding illness, injury, or injury to family members, changed family plans, or calls for similar reasons, may be made at any time. Incoming calls or an urgent and personal nature shall be directed to the employee.
- Using city systems for conducting business related to outside employment or business ownership is strictly prohibited.
- Disclosing confidential information over the phone is strictly prohibited.
- No employee may use the City's long distance telephone service for personal use.
- No employee may accept collect calls except those from a City employee on official business, or as otherwise directed by a superior ranking employee or official.
- There is a charge for using directory assistance (411 or "information"). Use of this service should be kept to a minimum and used only as a last resort, not as a convenience. Printed or online phone listings are to be used first. Use of this feature will be monitored.
- No employee may use city postage meters or equipment for personal mail.

F. RESPONSIBILITIES

By using the City's telecommunications and communications resources, each and every user accepts responsibility for his/her behavior, and the operation of their equipment and services.

The IT Department is responsible for determining the level and type of telephone service each employee member needs to do his/her work. IT is also responsible for regularly reviewing monthly telephone billing statements and investigating odd calling patterns, unexpected charges or unusual frequency of numbers called. IT will direct reimbursement of charges for personal calls and consult with Human Resources regarding potential disciplinary action.

Employees are responsible for informing supervisors of any regular need to make personal calls in connection with family care situations. They are also responsible for timely reimbursement of charges for personal long distance calls.

G. SANCTIONS

Sanctions will be commensurate with the severity and/or frequency of the offense and may include termination of employment; however, termination of employment does not fall under the realm of the IT department.

H. EXCLUSIONS

None.

I. INTERPRETATION

Authority to interpret this policy rests with the Mayor and Director of Administration, and is generally delegated to the Director of the IT department.

APPENDIX A:

FORMS

Data Processing

Access Request Form

First Name: _____ MI: _____ Last Name: _____

Department: _____

Needs Access to (check all that apply):

Windows: _____

MUNIS: _____

Alpha: _____

Terminal Services: _____ (must be accompanied by Remote Access Request Form)

Kronos: _____

E-Mail: _____

PTS: _____

Other (Please Specify): _____

_____

_____

_____

_____

Employee Signature: _____

Supervisor Signature: _____

Data Processing Signature: _____

Date: _____

IT Department

Elevated Privileges Request Form

First Name: _____ MI: _____ Last Name: _____

Department: _____

Reason for elevated access: _____

_____

_____

_____

_____

Employee Signature: _____

Supervisor Signature: _____

IT Department Signature: _____

Date: _____

Data Processing

Remote Access Request Form

Name:_____ User Account:_____

Department: _____

From where will you be accessing our network? (multiple locations, single location, etc.)

_____

Reason for access:

_____

_____

_____

IP Address(es) you will be accessing from:

_____

How long will you need access?

_____

Employee Signature: _____

Data Processing Signature: _____

Administration Signature: _____

Date: _____

Data Processing

Vendor Access Request

Name: _____ User Account:_____

Company: _____

Reason for access:

_____

_____

_____

IP Address(es) you will be accessing from:

_____

How long will you need access?

_____

Vendor Signature: _____

Data Processing Signature: _____

Administration Signature: _____

Date: _____

Data Processing

Vendor Confidentiality & Indemnity Agreement

This Confidentiality Agreement ("Agreement") is entered into on this _____ day of _____, 20____, by and between the City of Hammond ("City") and _____ ("Vendor").

1. "Confidential Information." For the purposes of this Agreement, Confidential Information shall mean all strategic and development plans; data; personnel records and information; liability reports; business records; customer lists; project records; employee lists; policies and procedures; information relating to processes, technologies, or theory; and all other information made available to Vendor _____.
2. Non-Disclosure Obligations. Vendor promises and agrees to receive and hold the Confidential Information in confidence. Without limiting the generality of the foregoing, Vendor further promises and agrees:
    - To protect and safeguard the Confidential Information against unauthorized use, publication, or disclosure.
    - Not to use any of the Confidential Information except for the purposes of City business.
    - Not to - directly or indirectly - in any way, reveal, report, publish, disclose, transfer, or otherwise use any of the Confidential Information except as specifically authorized by the City in accordance with this Agreement.
    - Not to use any Confidential Information to compete or obtain any advantage against the City in any commercial activity, which may be comparable to the commercial activity contemplated by the parties in connection with the business purposes.
    - To comply with any other reasonable security measures requested by the City.
3. Exceptions. The confidentiality obligations hereunder shall not apply to Confidential Information which: is, or later becomes, public knowledge other than through a breach of the provisions of this Agreement; is in the possession of the Vendor, outside of his/her involvement with the City, as evidenced by written records; or is independently received by the Vendor from a third party outside of their involvement with the City, with no restrictions on disclosure.
4. Return of Confidential Information. The Vendor agrees, upon completion of service or contract, or upon written request of the City, whichever is earlier, to promptly deliver to the City all records, notes, and other written, printed, or tangible materials in the possession of the individual, pertaining to the Confidential Information.

5. Indemnity. Vendor agrees to indemnify and hold the City harmless from any claim, demand, loss or damage, including attorney fees and costs of defense, arising out of the disclosure of Confidential Information by Vendor or arising out of Vendor's breach of this Agreement.
6. Each party warrants and represents that the person signing below is duly authorized to enter into this Agreement on behalf of such party. This Agreement shall be binding on the heirs, successors and assigns of each party.
7. Vendor's obligations under this Agreement shall extent to Vendor's employees and agents. Vendors shall make each employee and agent with access to any Confidential Information aware of the existence of this Agreement.

CITY OF HAMMOND

_____ _____
City Representative Date

_____ _____
VENDOR Signature Date

_____ _____
Department Head Signature Date