

BUYSPEED/GREAT PLAINS SERVICES

BuySpeed Support

FUNCTION: To provide end-user support when using the financial systems

PROCEDURES: When an end-user experiences an issue with the financial system he/she is requested to send a screen-print of the error message as well as a clear and concise description of what the user was trying to accomplish when they had their issue. These issues should be sent to the Help Desk at 658-7800

STANDARDS: Users should contact the help desk at 658-7800 to report issues with BuySpeed.

FORMS: None

Great Plains Support

FUNCTION: To provide end-user support when using the financial systems

PROCEDURES: When an end-user experiences an issue with the financial system he/she is requested to send a screen-print of the error message as well as a clear and concise description of what the user was trying to accomplish when they had their issue. These issues should be sent to the Help Desk at 658-7800

STANDARDS: Users should contact the help desk at 658-7800 to report issues with Great Plains.

FORMS: None

HELPDESK SERVICES

Computer Installation Request

FUNCTION: Provides users with a computer.

PROCEDURES: Submit request to Helpdesk 658-7800, for computer installation.

STANDARDS: Backup documents to H: Drive. Computer has to be purchased or available. Computer is to be a Dell Inc. model.

FORMS: Inventory Management Custody Sheet and Electronic Work Order

Blackberry Service Request

FUNCTION: Provides users with blackberry configuration and activation and service.

PROCEDURES: Submit request to Helpdesk 658-7800.

STANDARDS: Blackberry has to be purchased by customer.

FORMS: Electronic Work Order

Printer Installation Request

FUNCTION: Provides users with access to a printer.

PROCEDURES: Submit request to Helpdesk 658-7800, for printer installation.

STANDARDS: Network Printer or USB (Universal Serial Bus) type

FORMS: Inventory Management Custody Sheet and Electronic Work Order

Software Installation Request

FUNCTION: This service provides users with installed software used to perform their job.

PROCEDURES: Submit request to Helpdesk 658-7800, for software installation.

STANDARDS: Must be listed on the authorized software list.

FORMS: Software Authorization Testing and Request Form and Electronic Work Order

Application Support Request

FUNCTION: This service provides users with support for authorized installed software.

PROCEDURES: Submit request to Helpdesk 658-7800 for software support.

STANDARDS: Software must be required in the performance of job.

FORMS: Electronic Work Order

Hardware Support Request

FUNCTION: This service provides users with support for authorized installed hardware.

PROCEDURES: Submit request to Helpdesk 658-7800, for hardware support.

STANDARDS: Hardware must be required in the performance of job.

FORMS: Electronic Work Order

Password Reset Request

FUNCTION: This service provides users with the ability to reset domain passwords.

PROCEDURES: Submit request to Helpdesk 658-7800, for password reset support.

STANDARDS: Must be approved by supervisor or verification of identity successful.

FORMS: Electronic Work Order, Email from supervisor's account or Physical identity verified.

Audio Visual Setup Request

FUNCTION: This service provides audio visual equipment setup for customers

PROCEDURES: Submit request to Helpdesk 658-7800.

STANDARDS: Customer must have equipment that requires setting up.

FORMS: None

MAINFRAME SUPPORT SERVICES

Data Request

FUNCTION: Provide ad-hoc report or data.

PROCEDURES: Submit request via email to the Mainframe team lead. (Currently, Joe Ballmann at jballmann@cityofno.com)

STANDARDS:

1. If applicable, forward to the appropriate user contact for approval. Payroll/Finance – Kim T. Delarge NOPD – Stephanie Landry or James Gallagher NOFD – Gwen Wiggins
2. Determine extent of request. Most are satisfied using the standard extract files. If not, go to step 3, else go to step 4.
3. If necessary, prioritize and assign to a programmer for resolution. Notify the requestor of the anticipated completion date.
4. Verify requestor acceptance and close request.

FORMS: N/A.

NETWORKING SERVICES

Data Connectivity Request

FUNCTION: This service provides users with access to the city data systems.

PROCEDURES: The Networking team is informed of new users through help desk tickets. Generally, if the new user is replacing a former user, no action is necessary.

For new locations, the team is informed when the organization has secured the new location. The team then works with the organization to identify the locations for network drops and the necessary equipment.

For existing locations, the team is notified of the need for new networking drops through the help desk.

The actual labor for new network drops is performed by the current cabling vendor.

STANDARDS: User should contact the help desk at 658-7800 for new requests.

Department head must approve all request forms.

FORMS: Form can be downloaded from Janice Darby.

Voice Connectivity Request

FUNCTION: This service provides users with access to the city's phone systems.

PROCEDURES: The Telecommunications team is informed of new users through help desk tickets. Generally, if the new user is replacing a former user, no action is necessary.

For new locations, the team is informed when the organization has secured the new location. The team then works with the organization to identify the locations for network drops and the necessary equipment.

For existing locations, the team is notified of the need for new networking drops through the help desk.

Phones are generally Cisco 7940 or 7941 for most users. Other users may require a 7960/7961 phone.

STANDARDS: User should contact the help desk at 658-7800 for new requests.

Department head must approve all request forms.

FORMS: Form can be downloaded from Janice Darby.

311 Services Request

- FUNCTION:** This service provides 311 call functionality to callers and users.
- PROCEDURES:** The Telephony team is informed of new users through help desk tickets. Generally, if the new user is replacing a former user, no action is necessary.
- For script changes or message prompt changes, the requestor initiates the request through the help desk.
- New phones are typically Cisco 7940/7941 phones. These phones are tied into the Call Manager system.
- STANDARDS:** User should contact the help desk at 658-7800 for new requests.
- FORMS:** NONE

NOPD Services Request

- FUNCTION:** These services are fairly broad in nature. These services involve liaison with State Police regarding applications like AFIS, NCIC, and LEMS. These services also involve maintenance and assistance with NOPD Records systems and MDT systems as well as interaction with other local LE organizations.
- PROCEDURES:** The team is informed of requests through help desk tickets.
- STANDARDS:** User should contact the help desk at 658-7800 for new requests.
- FORMS:** NONE.

Network Security Request

FUNCTION: This service attempts to minimize the threats of malicious users and software from impacting the City's systems.

PROCEDURES: The Networking team monitors daily the logs from all networking devices, such as routers, switches, firewalls, VPN Concentrator, etc. The team also monitors and maintains Intrusion Protection Systems (IPS) that is strategically placed within the City's infrastructure.

Through the analysis of the logs, the team is able to identify unauthorized equipment such as rogue access points or switches, as well as occasionally identifying a workstation that has been infected with a virus. In such instances, the help desk is informed and we also disable access to the network for those devices.

The team also monitors for brute force attackers that attempt to gain unauthorized access to City systems.

STANDARDS: None. We continue to seek development and approval of a security policy.

FORMS: NONE

TELECOMMUNICATIONS SERVICES

Telephone Request

- FUNCTION:** Provides telephones to city agencies.
- PROCEDURES:** Contact the MIS/Telecommunications division or call the Help Desk at 658-7800 to request telephones. If it is a city agency the Telecommunication is responsible to supply telephones to city agencies.
- STANDARDS:** All telephones must be Cisco IP 7940, 7941, 7960 or 7961 sets.
- FORMS:** NONE

New Sites Connecting to City's Networking Infrastructure

- FUNCTION:** Provides connects structures to the City of New Orleans WAN.
- PROCEDURES:** Requests are received via email from the departments when they are in the planning stages of bringing a building on line.
- STANDARDS:** Wiring must be included in the build out and marked on drawings for each site.
- FORMS:** NONE

Wiring Request

FUNCTION: Provides network, telephone and fax wiring for city agencies.

PROCEDURES: Users should complete and submit a Wiring Request Form to MIS for approval.

STANDARDS: All network, telephone and fax wiring request must be submitted for approval to the MIS department. All wiring shall be completed by an authorized wiring vendor and supervised by an employee of the City of New Orleans MIS department or their designate in charge. At no time shall a department solicit a vender to complete wiring for any city agency without the approval and supervision of the MIS department or their designate in charge. No vendors, non city agencies, or unauthorized personnel shall be allowed to connect devices to the city's networking infrastructure without prior approval from MIS department. All switch sites shall be secured and unauthorized personnel shall not have access to equipment. All vendors, non city agencies, and unauthorized personnel are required to contact the MIS/ Telecommunications department prior to gaining access to city networking infrastructure.

If you have any questions or need additional information please contact Telecommunications Department 504 658 7704.

FORM: NONE

SECURITY

Buyspeed User Request

FUNCTION: Provide security setup for all city employees using the City Purchasing Portal (BUYSPEED) for the purchasing of software, equipments, supplies etc and password changes.

PROCEDURES: Fill out the Buyspeed user request form and forward to MIS for approval. .

Access the City Purchasing Portal by login to the city website, www.cityofno.com. Click on City Purchasing Portal, this will bring you to the Department of Purchasing. Click on the message below that states: [click here to begin using the new City of New Orleans Online Purchasing Portal.](#)

If you have any questions about Buyspeed contact the security unit at 658-7620.

STANDARDS: Contact the security unit at 658-7620 for login or password issues.

Department should fill out the Buyspeed User Request Form to remove a user whenever a user leave the city or move to another department.

FORMS: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://newuser/>.

Buyspeed Department Request

FUNCTION: Provides new department or modify current department organizational codes.

PROCEDURES: Fill out the Buyspeed Department Request form and forward to MIS for approval.

If you have any questions about Buyspeed contact the security unit at 658-7620.

STANDARDS: Form must be sign and approve by Department Head.

FORMS: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://newuser/>.

Buyspeed Approval Path Request

FUNCTION: Provides new approval path or changes to current approval path for organizational codes in the Buyspeed Purchasing Portal.

PROCEDURES: Fill out the Buyspeed Approval Path Request form and forward to MIS for approval. .

If you have any questions about Buyspeed contact the security unit at 658-7620.

STANDARDS: Form must be approved by the Department Head.

FORMS: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://newuser/>.

AHRS User Request

FUNCTION: Provides requested access to the City of New Orleans Online Human Resource System (AHRS)

PROCEDURES: Fill out the AHRS Security Request Form and forward to MIS for approval.

If you have any questions about AHRS security contact the security unit at 658-7620.

STANDARDS: User should contact the security unit at 658-7620 for login or password issues.

Form must be approved by Department Head.

Department should fill out the AHRS Security Request Form to remove a user whenever a user leave the city or move to another department.

FORMS: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://newuser/>.

HRTS User Request

FUNCTION: Provides requested access to the City of New Orleans Online Human Resource Time System (HRTS)

PROCEDURES: Fill out the HRTS Security Request Form and forward to MIS for approval.

If you have any questions about HRTS security contact the security unit at 658-7620.

STANDARDS: User should contact the security unit at 658-7620 for login or password issues.

Form must be approved by Department Head.

Department should fill out the HRTS Security Request Form to remove a user whenever a user leave the city or move to another department.

FORMS: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://newuser/>.

AFIN User Request

FUNCTION: Provides requested access to the City of New Orleans Online Financial System (AFIN)

PROCEDURES: Fill out the AFIN Security Request Form and forward to MIS for approval.

If you have any questions about AFIN security contact the security unit at 658-7620.

STANDARDS: User should contact the security unit at 658-7620 for login or password issues.

Form must be approved by Department Head.

Department should fill out the AFIN Security Request Form to remove a user whenever a user leave the city or move to another department.

FORMS: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://newuser/>.

ECRS
Electronic Contract Routing System

FUNCTION: Provide service for user to access the city Electronic Contract Routing System and track all City contracts.

PROCEDURES: Fill out the ECRS Departmental Setup form and forward to MIS for approval.

If you have any questions contact the Help Desk unit at 658-7800.

STANDARDS: User should contact the Help Desk at 658-7800 for training if needed, for login and password issues, or other ECRS issues.

FORMS: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://newuser/>.

Great Plains User Request

FUNCTION: Provides security setup for all city employees using the Great Plains Financial System. Allow employees to review their budget and run financial reports.

PROCEDURES: Fill out the Great Plain user request form and forward to MIS for approval. User must call the helpdesk at 657-7800 to put in a workorder to have the Great Plains software install.

If you have any questions about Great Plains contact the security unit at 658-7620.

STANDARDS: User should contact the security unit at 658-7620 for login or password issues.

Form must be approved by Department Head

Department should fill out the Great Plains User Request Form to remove a user whenever a user leaves the city or moves to another department.

FORMS: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://newuser/>.

Crystal Reporting

- FUNCTION:** Provides assistance to departments in creating reports, using the Crystal Reporting tool that can be connected to most Microsoft Access and SQL databases.
- PROCEDURES:** Department should contact the Security/Database unit at 658-7620 and setup a meeting to discuss the issue.
- STANDARDS:** The Crystal report may be exported to a Microsoft Excel spreadsheet or an Adobe PDF file.
- FORMS:** NONE

Database Design and Support Request

FUNCTION: Provides assistance to departments in creating new database and maintains current databases. Assist users in creating new queries and reports.

PROCEDURES: Department should contact the database unit at 658-7620 and setup a meeting to discuss the issue.

STANDARDS:

FORMS: NONE

**AS400
User Request**

FUNCTION: Provides user access to the AS/400 Systems.

PROCEDURES: Fill out the AS/400 User Registration Form and forward to MIS department for approval. Please answer yes/no to all questions regarding which system access is needed. To access the AS/400, double click on the AS/400 icon on your pc desktop.

If you have any questions contact the Security/Database unit at 658-7620.

STANDARDS: User should contact the Security/Database unit at 658-7620 for training if needed, for login and password issues, or other AS/400 issues.

FORMS: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://newuser/>.

SYSTEM

USER CREATION REQUEST

FUNCTION: Provides supervisors the means to seek access to the cityofno.com domain on behalf of new or currently disabled staff members. This access is to include an account, a mailbox associated with that account, and a home drive for reliable data storage.

PROCEDURES: The supervisor will access the request form from the local intranet at <http://newuser/> and complete the form. Upon submission, the form will prompt the supervisor to print out the completed form. The supervisor and the user will sign the form and submit it to MIS (room 3E05) via fax or the drop off of a hard copy to the secretary in 3E05.

Once the form has been signed off on by MIS administration, the Systems team will create the user account and an email will be automatically sent to notify the supervisor who initially requested the user form.

STANDARDS: Form must be approved by Department Head

FORM: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://newuser/>.

User Drive Access Request

FUNCTION: Provides supervisors the means to seek access to specific shared group drives on the cityofno.com domain. These drives are a central storage point for departmental resources where authenticated users may collaborate on documents necessary to the functionality of their given departments.

PROCEDURES: The user or the supervisor of the user in need may call the helpdesk and place the request. The helpdesk technician then places a work order in Track-IT! This work order must have the following fields defined in Track-IT! As follows:

Type: ACCOUNTS OR SECURITY

Lookup #1: ACCESS

The ticket must be assigned to an employee of the helpdesk, preferably the employee who created the work order.

STANDARDS:

FORMS: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://userlookup/access>. The forms are only visible once the Helpdesk has placed the work order meeting the aforementioned criteria.

Folder/Mailbox Access Requests

FUNCTION: This service exists to provide access to individual folders and files belonging to other users or entities that are no longer capable of permitting access to those files and folders. For example, home drives of former employees.

PROCEDURES: The user or the supervisor of the user in need may call the helpdesk and place the request.

The helpdesk technician then places a work order in Track-IT! This work order must have the following fields defined in Track-IT! As follows:

Type: ACCOUNTS OR SECURITY
Lookup #1: ACCESS

The ticket must be assigned to an employee of the helpdesk, preferably the employee who created the work order. Once the aforementioned criteria have been met, the helpdesk technician will navigate to <http://userlookup/access> via the intraweb or VPN access. Once there, the technician will select their given work order number from a pull down menu and enter the email address of the supervisor who is to authorize the request. An email will be sent to the supervisor, and the ticket is automatically relocated to the SYSTEMS queue in Track-IT! Upon receipt of the email, the supervisor will click the embedded link to access the form. The supervisor will be prompted for authentication (a digital signature) using their cityofno.com user id and password. The form will be completed by the supervisor, and Systems will be notified via email. Upon notification that the supervisor has digitally signed the request (via their submission of the completed form), a member of Systems will grant any access requested. The ticket will be closed automatically via a link in the email received by Systems administrators. The supervisor will receive email notification that the request has been fulfilled. On a case by case basis, the data will be relocated or the requestor provided access directly to the original network store that housed the data.

STANDARDS:

FORMS:

Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://userlookup/access>.

Disable User Accounts & Mailbox Archiving for Disabled Users Request

FUNCTION: It is the responsibility of each department to notify the help desk that their employees are no longer employed by the city, or that they have relocated to another department. In the event that a user is no longer employed by the city, or an account expires, the account is disabled. Disabled accounts may not log in to the domain, check email; access files associated with their account, or perform any other task familiar with authenticated use of domain resources.

As a supplement to these disabled accounts, mailboxes which are no longer accessible will be archived off of the Exchange server. This serves to generate critical storage space on the Exchange server and the process may be reversed in the event that these mailboxes must be accessed.

PROCEDURES: The supervisor of the employee is to notify the help desk that the employee is no longer affiliated with the city. A work order is to be placed in the Systems queue to notify the Systems administrators.

Upon notification that an employee is no longer affiliated with the city, the Systems administrators will disable the account and archive the user's mailbox.

This entire process is reversible in the event that the employee returns.

STANDARDS:

FORMS: Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://userlookup/access>.

VPN Request

- FUNCTION:** Provides City users a method to request VPN access
- PROCEDURES:** A user should go to <http://newuser/vpn> and fill out the VPN request form and forward to MIS for approval.
- If you have any questions about VPN Request contact the Help Desk at 658-7800
- STANDARDS:** User should contact the Help Desk at 658-7800 for VPN request
- FORMS:** Accessible only from within the city's network, or via VPN access from outside of the city's network, the forms can be accessed from a web browser at <http://newuser/>.

Backup and Restore Request

FUNCTION: Provides City users a method to request data (files and folders) from backup tape. This request will cover data that have become corrupted, misplaced or deleted.

PROCEDURES: To request a restore of data the user should contact the Help Desk and provide to the technician the exact path to the location of where the file or folder is or was before deletion. The Help Desk will create a Work Order and forward it to the Systems team. Data backups request will follow the same procedure as that of a restore.

If you have any questions about Backup and Restore Request contact the Help Desk at 658-7800.

STANDARDS: User should contact the Help Desk at 658-7800 for Backup and Restore Request.

FORMS: NONE.

Change Control Forms Request

FUNCTION: Purpose of the change control form is to ensure business continuity prior to the implementation of proposed amendments to the existing Systems infrastructure. The form requires authorization from all parties impacted by a given circumstance initiated by proposed changes. Input is required from all parties potentially impacted by the set of changes.

A pre-requisite to the implementation of change is that the change may be tested in an environment outside of the live domain.

PROCEDURES: Those implementing the change are to initiate dialogue with the Systems team. The systems team will perform discovery with the customer's input to ascertain those who may be impacted by the proposal.

All parties deemed to be impacted by the change will then be contacted by the systems team to collaborate on the proposal. Once all necessary parties have been notified and terms for the implementation of said change have been agreed upon, authorization will be sought from the CTO.

Once authorization has been established from all parties, testing may begin, and change implemented upon successful testing.

STANDARDS:

FORMS: Pending approval.

WEB DESIGN

WEB Project Request

FUNCTION: Provide web project support for all of the City Departments for building new website pages/portals, re-designing existing websites, or developing a web application in support of a city departmental goal or objective. A meeting to discuss and design the web layout is the first steps in initiating a new project.

PROCEDURES: **Project Initiation - Discuss and Design Session**

The goal of the Discuss and Design Session is to engage everyone from all disciplines (Project Sponsor, Development Team, etc) and focus on discussion of the project deliverables. The size or work effort required for the project will be determined once the requirements are defined..

Standards

Project Manager - Developing the Project Plan

Review the specifications and identify in detail the tasks required to meet the goals of the project.

Identify or confirm the work effort and assign the appropriate skilled resources.

The size or work effort required for the project will be determined based on the detailed requirements. Projects can be Small, Medium or Large.

Once the required resources are identified, a determination of the availability of resources will be performed.

Once all the information is assembled - establish the timeline (project plan) for completing the project (ROM - Rough Order of Magnitude at 75%).

FORMS: The Project Manager in accordance with the guidelines provided by the Mayor's Office of Technology will provide all project documentation. The Project Sponsor is expected to provide sign off and approval of the Functional Specifications before any work is started. Web Project Request questions can be directed to the webmaster@cityofno.com

Web Content Management Services Request

FUNCTION: Provide web content management services for the entire City departments for content additions, changes, or deletions.

The **WEBSITE CONTENT CHANGE REQUEST FORM** is used for the following types of web content request:

Press Releases	Bulletin Boards
Photos	Video Publishing Request
News Articles	Board Meeting Notices
Job Ad Postings	Content Updates
Public Notices	News Letters
Meeting Agendas	Content Rotators
Public Schedules	Event Calendars

Assistance with content layout and design is also available.

PROCEDURES

An authorized representative of the department is requested to complete a **WEBSITE CONTENT CHANGE REQUEST FORM**. The information requested on the form describes where on the city website the change is to be made and what is being added, changed or deleted as required by the department.

When completed, the form can be sent via E mail to webmaster@cityofno.com

Attachments or Documents –

Any document (Press Releases, Job Ads, Event Agendas, Bulletins, etc) related to the **WEBSITE CONTENT CHANGE REQUEST FORM** should be embedded on the form when submitted.

In any Microsoft Suite Product, follow these instructions:

- Select the tab titled “Insert”
- Select “Object”
- Select Tab for “Create from File”
- Select Radio Button “Display as Icon”
- Browse to locate the file
- Select “Insert”

STANDARDS

Once the form has been submitted to the webmaster, an assessment of the work effort is performed.

FORMS

The **WEBSITE CONTENT CHANGE REQUEST FORM** can be downloaded from the City of NO website on the Mayor's Office of Technology web page.

**Email Guidelines and Policies for
The City of New Orleans**

TABLE OF CONTENTS

A. Overview.....	44
B. City Of New Orleans Acceptable Use Policy	44
1.0 Overview	44
2.0 Purpose	44
3.0 Scope	44
4.0 Policy	44
5.0 Enforcement.....	49
6.0 Definitions	49
C. Automatically Forwarded Email Policy.....	49
1.0 Purpose	49
2.0 Scope	49
3.0 Policy	49
4.0 Enforcement.....	50
5.0 Definitions	50
D. Email Retention Policy	50
1.0 Purpose	50
2.0 Scope	51
3.0 Policy	51
4.0 Enforcement.....	52
5.0 Definitions	52

City of New Orleans' Email Policies

A. Overview

The following sections state the City of New Orleans' Email Policies for Acceptable Use, Forwarded Email, and Email Retention. These policies apply to employees, consultants, temporaries, and other workers at the City of New Orleans.

B. City Of New Orleans Acceptable Use Policy

1.0 Overview

Our intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to City of New Orleans established culture of openness, trust and integrity. The City of New Orleans commits to protecting its employees and partners from illegal or damaging actions by individuals, either knowingly or unknowingly.

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 City of New Orleans. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every City of New Orleans' 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.

2.0 Purpose

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

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at City of New Orleans, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by City of New Orleans.

4.0 Policy

4.1 General Use and Ownership

1. While City of New Orleans's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of City of New Orleans. Because of the need to protect City of New Orleans's network,

management cannot guarantee the confidentiality of information stored on any network device belonging to City of New Orleans.

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.
3. The City of New Orleans recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within City of New Orleans may monitor equipment, systems, and network traffic at any time.
5. City of New Orleans reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts.
 - a. Authorized users are responsible for the security of their passwords and accounts.
 - b. System level passwords should be changed quarterly.
 - c. User level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. Employees are prohibited from posting from a City of New Orleans' email address to newsgroups, unless posting is in the course of business duties.

4.2.1 Virus and SPAM Control

All hosts used by the employee that are connected to the City of New Orleans Internet/Intranet/Extranet, whether owned by the employee or City of New Orleans, shall be continually executing approved virus-scanning software with a current virus database.

4.2.2 Attachment Filters

The Internet Mail Gateway is currently configured to block incoming attachments with the following file extensions:

.ade	.com	.inf	.mst	.vb
.adp	.cpl	.ins	.nsw	.vbe
.asp	.crt	.isp	.pcd	.vbs
.asx	.dll	.js	.pif	.wav
.bat	.eml	.jse	.rar	.wsc
.bin	.exe	.mp3	.reg	.wsf
.chm	.hlp	.msi	.scr	.wsh
.cmd	.hta	.msp	.shs	

The City of New Orleans reserves the right to apply filters on certain types of files if the file type in question poses a risk to resources on the network.

4.2.3 Quarantine

These incoming files will be quarantined for 7 days. .vsd .zip. Customers will be notified that an attachment was quarantined and may request that attachments be forwarded to their inbox. This will allow customers to receive work related attachments while protecting them from potentially malicious attacks.

4.2.4 3rd Party Messaging Applications

Email applications such as AOL Instant Messenger, Microsoft HotMail and any other free web-based/instant messaging email products are a security risk to an agency's network and to the citywide messaging network. Much time and expense has been invested in ensuring that messages are free from virus attacks. Messages from products such as Instant Messenger and Hotmail are not scanned for viruses or malicious program; therefore these programs provide a backdoor for intrusions and infections. As such, these products put the entire citywide messaging system at risk by exposing the network to potential malicious code. In addition to these risks, the installation of these applications often causes other desktop applications to malfunction. For these reasons, 3rd party messaging applications are prohibited unless approved by the Mayor's Office of Technology.

4.2.5 Maintenance

Scheduled Maintenance

Scheduled maintenance shall mean any maintenance on the messaging network to which User's network is connected 1) of which User is notified, or 2) that is performed during a standard maintenance window on Sundays from 6 PM to 12 AM. Notice of Scheduled Maintenance will be provided to Customers by email message.

Backups

A full backup is run every night on the messaging server database. Tapes are stored offsite for 30 days. Backups are not intended to be used to restore messages that were accidentally deleted. These backups are used to restore corrupted databases, recreate the email environment in the case of a disaster, and retain an archived (30 days) copy in the event proper authorities request information.

Restores will require 1) a written request by agency upper management, and 2) approval by the Mayor's Office of Technology. Special charges will apply for user-requested restores. Only files stored on the citywide messaging server will be backed up. Personal (.PST) and offline (.OST) folders on the departmental computers will not be backed up.

4.3 Storage and Transaction Limitations

Amount of storage on the mail server by default is set to 50 MB per user. Remember, storage includes Inbox, Sent Items, Deleted Items, Calendar, Tasks and Contacts. Larger storage limits can be configured, but will require approval by agency appointed authority since additional storage may increase agency costs.

1. Warning notifications are sent when you are within 5 MB of your limit.
2. Sending email is prohibited when a mailbox exceeds the storage limit.
3. Maximum send size is 15 MB per message.
4. Maximum receive size is 15 MB per message.
5. Exceptions to these limits will be considered on a business case basis.

4.4 Age Limits

The following age limits are set on messages stored on the email system:

1. Inbox - No age limit. Removed only by mailbox owner.
2. Sent Items- No age limit. Removed only by mailbox owner.
3. Deleted Items - 7 Days
4. Deleted item retention is 7 days. (Mail deleted from Deleted Folder is held for 7 days.)

4.5 Authentication

To eliminate dual logons, a domain trust relationship can be configured and maintained. The trust will also allow customers to enforce their own password policies and

administration. Agencies that choose the no trust option are subject to the City Email password policy, as follows:

1. Maximum age: 30 days
2. History: 5
3. Complexity: 3 out of 4 of the following characters: Uppercase, lowercase, numbers or symbols

4.6 Account Creation Standards

1. Names in the Address List will be displayed as "Firstname Lastname". Duplicate names will be distinguished by the use of an agency identifier. (Example: "Firstname Lastname -DPS")
2. The Company field is used for City agency name and must be completed for each user profile.
3. The Department field is optional if an agency wants to distinguish different sections for billing purposes.
4. 10 digits must be used in the phone number. (Example: 225-555-5555)

4.7 Unacceptable Use

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).

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

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

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. 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 City of New Orleans.
2. 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 City of New Orleans or the end user does not have an active license is strictly prohibited.
3. 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.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
 5. 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 at home.
 6. Using a City of New Orleans computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
 7. Making fraudulent offers of products, items, or services originating from any City of New Orleans account.
 8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
 9. 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.
 10. Port scanning or security scanning is expressly prohibited unless prior notification to the City is made.
 11. 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.
 12. Circumventing user authentication or security of any host, network or account.
 13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
 14. 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.
 15. Providing information about, or lists of, City of New Orleans employees to parties outside City of New Orleans.
 16. Using any messenger programs (i.e. AIM, Microsoft Messenger, Trillion etc ...) or personal profile spaces to include (MYSPACE, FACEBOOK, HOTMAIL, MATCH, ETC ...).
 17. Employees may view video from You Tube or other similar programs only if they pertain to the City of New Orleans' business. These videos should not be saved without approval from the Mayor's Office of Technology.

Email and Communications Activities

1. 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).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. 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.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within City of New Orleans's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by City of New Orleans or connected via City of New Orleans's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated the above policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

<u>Term</u>	<u>Definition</u>
<i>Spam</i>	Unauthorized and/or unsolicited electronic mass mailings.

C. Automatically Forwarded Email Policy

1.0 Purpose

To prevent the unauthorized or inadvertent disclosure of sensitive company information.

2.0 Scope

This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of City of New Orleans.

3.0 Policy

Employees must exercise utmost caution when sending any email from inside City of New Orleans to an outside network. Unless approved by an employee's manager, City of New Orleans email will not be automatically forwarded to an external destination. Sensitive information will not be forwarded via any means, unless that email is critical to business and is encrypted.

4.0 Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms

Email

Definitions

The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora and Microsoft Outlook use SMTP.

Forwarded email

Email resent from internal networking to an outside point.

Sensitive information

Information is considered sensitive if it can be damaging to City of New Orleans or its customers' dollar value, reputation, or market standing.

Unauthorized Disclosure

The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

D. Email Retention Policy

1.0 Purpose

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to the Mayor's Office of Technology.

2.0 Scope

This email retention policy is secondary to City of New Orleans policy on Freedom of Information and Business Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. All City of New Orleans email information is categorized into four main classifications with retention guidelines:

Administrative Correspondence (4 years)

Fiscal Correspondence (4 years)

General Correspondence (1 year)

Ephemeral Correspondence (Retain until read, destroy)

3.0 Policy

3.1 Administrative Correspondence

City of New Orleans Administrative Correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only shall be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox info@City of New Orleans has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

3.2 Fiscal Correspondence

City of New Orleans Fiscal Correspondence is all information related to revenue and expense for the company. To ensure Fiscal Correspondence is retained, a mailbox fiscal@City of New Orleans has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

3.3 General Correspondence

City of New Orleans General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence.

3.4 Ephemeral Correspondence

City of New Orleans Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

3.5 Encrypted Communications

City of New Orleans encrypted communications should be stored in a manner consistent with City of New Orleans Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

3.6 Recovering Deleted Email via Backup Media or re-managing for data recovery or Forensic reasons.

City of New Orleans maintains backup tapes from the email server and once a quarter a set of tapes is taken out of the rotation and they are moved offsite. No effort will be made to remove email from the offsite backup tapes. If data is needed for business continuity or Forensics the City State or Local government must designate a representative to re-manage the suspect account maintaining a strict chain-of-custody on said documents until the needs of the city our met.

4.0 Enforcement

Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms

Definitions

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here...]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within City of New Orleans is done via a license. Please contact the appropriate support organization if you require a license.

Approved Instant Messenger

The Jabber Secure IM Client is the only IM that is approved for use on City of New Orleans computers.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use

man chmod to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of City of New Orleans.

Encryption

Secure City of New Orleans Sensitive information. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your Page 53 of 53manager and/or corporate legal services for further guidance.