City of Memphis
Information Services Division

Policies and Procedures

Please Note: All policies and procedures included in this manual have been approved by the current Chief Administrative Officer, Jack Sammons and the current Chief Information Officer, Brent J. Nair. (12/10/2015)

Table of Contents

IS-100-01	Encryption Policy
IS-100-02	Acceptable Use Policy
IS-100-03	Bluetooth Security Policy
IS-100-04	Backup and Restoration Policy
IS-100-05	Audit Policy
IS-100-06	Anti-Virus Policy
IS-100-07	Data Line Usage Policy
IS-100-08	Computer & Mobile Device Disposal Policy
IS-100-09	Internet Use Monitoring and Filtering Policy
IS-100-10	Internet DMZ Equipment Policy
IS-100-11	Information Sensitivity Policy
IS-100-12	Guest Access Policy
IS-100-13	Email Use Policy
IS-100-14	DB Credentials Policy
IS-100-15	DMZ Lab Security Policy
IS-100-16	Incident Response Policy
IS-100-17	Confidential and Sensitive Data Transmission Policy
IS-100-18	Extranet Use Policy
IS-100-19	Password Policy
IS-100-20	Virtual Private Network Policy
IS-100-21	Personal Communication Device and Voicemail Policy
IS-100-22	Removable Media Disposal Policy
IS-100-23	Router Security Policy
IS-100-24	Server Security Policy
IS-100-25	User Account Deletion Policy
IS-100-26	Server Malware Protection Policy
IS-100-27	Removable Media Policy
IS-100-28	Risk Assessment Policy
IS-100-29	Remote Access Policy
IS-100-30	Stolen Computer Equipment Policy
IS-100-31	Personal Computer Device Usage Policy
IS-100-32	Wireless Communication Policy
IS-100-33	Physical Access Policy
IS-100-34	Geographic Information Data Dissemination Policy
IS-100-35	Intrusion Detection Policy
IS-100-36	Mobile Device Management Policy
IS-100-37	PCI Compliance Policy
IS-100-38	Patch Management Policy
IS-100-39	Electronic Data Retention Policy

APPENDIX

IS-101-01	Anti-Virus Guidelines
IS-101-02	Bluetooth Guidelines
IS-101-03	Data Line Usage Guidelines
IS-101-04	Password Guidelines
IS-101-05	Virtual Private Network Guidelines
IS-101-06	Wireless Communication Standard
IS-101-07	Patch Management Process

Forms for the following policies:

IS-100-16 Incident Response Policy - ‘‘Security Incident Report Form’’
IS-100-30 Stolen/Lost Computer Equipment Policy – “Stolen or Missing Computer Equipment Form”

Policy & Procedures Signature Approval

Encryption Policy
IS-100-01

Purpose:
The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. The City of Memphis will utilize encryption to protect confidential and personal identifiable information that pertains to individual citizens, employees and businesses.

Scope:
This policy applies to all City of Memphis employees, contractors, and affiliates that transmit store and access information of any kind.

Policy:
- The City will only utilize encryption algorithms that have received substantial public scrutiny such as DES, Blowfish, RSA, RC5 and IDEA.
- Symmetric cryptosystem key lengths must be at least 256- bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength.
- The City's key length requirements will be reviewed annually and upgraded as technology allows.
- The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Information Services Division

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, possible civil/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
Proprietary Encryption:	An algorithm that has not been made public and/or has not undergone public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem:	A method of encryption in which the same key is used for both encryption and decryption of the data. Asymmetric
Cryptosystem:	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

Acceptable Use Policy
IS-100-02

Purpose:

Inappropriate use exposes the City of Memphis to risks including virus attacks, compromise of network systems and services, and legal issues. Information Services is committed to protecting the City's employees, partners, assets and the organization itself 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 the City of Memphis. These systems are to be used for business purposes in serving the interests of the City and citizens.

Purpose:

The purpose of this policy is to outline the acceptable use of computer equipment at the City. These rules are in place to protect the employee and City from improper usage of computer equipment.

Scope:

This policy applies to all equipment that is owned or leased, to all employees, contractors, consultants, temporaries, and other workers at the City of Memphis, including all personnel affiliated with third party service providers that utilize equipment owned or leased by the City of Memphis.

Policy:

General Use and Ownership

1. The data created on the City's systems is the property of the City of Memphis.
2. For security and network maintenance purposes, authorized individuals within the City may monitor equipment, systems and network traffic at any time.
3. The City of Memphis reserves the right to audit networks and systems on a periodic basis to ensure compliance.

Security and Proprietary Information

1. Examples of confidential information include but are not limited to: City private data, organizational strategies, confidential citizen data, and law enforcement

data. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords, accounts, or other computer and/or network authentication confidential at all times. This information **should not** be shared with any other individuals. Report unauthorized use of your account to the Information Services Division immediately.
3. Authorized users are responsible for the security of their passwords and accounts.
4. System and user level passwords should be changed quarterly.
5. All PCs, laptops and workstations must 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 Windows users) when the user is not actively using the PC, laptop, or workstation.
6. All city issued hosts used by the employee that are connected to the City Internet/Intranet/Extranet, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
7. Employees must use caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. If you suspect that the email might be malicious, please do not open or forward it and contact the help desk immediately.

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 or contractor of the City of Memphis authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City-owned resources.

System and Network Activities

The following activities are prohibited:

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 the City of Memphis.
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 the City or the end user does not have an active license is 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-owned 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 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 unless this activity is a part of an employee's normal job functions/duties.
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.

(The foregoing is not an all-inclusive list; the City of Memphis reserves the right to determine what activity is permissible.)

Email and Communications Activities that are prohibited

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, content, 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 user'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 networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the City or connected via the City's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Internet Activities

1. Accessing and/or sharing pornographic, socially offensive, violent information, or other objectionable materials from the Internet via the City's Network.
2. Accessing chat rooms and social networks such as face book and twitter.
3. The City of Memphis is not responsible for the content, accuracy, or reliability of information accessed from the Internet.

Blogging

1. Blogging by employees, whether using the City's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of City systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate City policy, is not detrimental to the City's best interests, and does not interfere with an employee's regular work duties. Blogging from City systems is also subject to monitoring.
2. Employees are prohibited from revealing any confidential or proprietary information and any other material covered by the *City's Confidential Information Policy* when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the City of Memphis and/or any of its employees.
4. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the *City's Non-Discrimination and Anti-Harassment Policy.*
5. Employees may also not attribute personal statements, opinions or beliefs to the City when engaged in blogging. The employee should include a disclaimer stating that the opinions expressed are strictly his/her own and not the City of Memphis, unless posting is in the course of the employee's business duties. Employees assume any and all risk associated with blogging.
6. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, City trademarks, logos and any other

City intellectual property may also not be used in connection with any blogging activity

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	**Definition**
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Spam	Unauthorized and/or unsolicited electronic mass mailings.

Bluetooth Security Policy
IS-100-03

Purpose:
The purpose of this policy is to outline the requirements for secure Bluetooth operations.

Scope:
This policy covers all City-owned Bluetooth Devices.

Policy:
- No Bluetooth Device shall be deployed on City-owned equipment that does not meet Bluetooth v2.1 specifications. The City Information Services Management must provide written authorization for any exception.
- Any Bluetooth equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.
- Bluetooth users must only access City information systems using approved Bluetooth device hardware, software, solutions, and connections.
- Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.
- Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
- Bluetooth users are required to report to the Help Desk, any misuse, loss, or theft of Bluetooth devices or systems immediately to Information Services.
- Bluetooth users must comply with the *Bluetooth Setup Guidelines*.

Security Audits
Information Services shall perform audits to ensure compliancy with this policy. In the process of performing such audits, the auditor shall not eavesdrop on any phone conversation.

Unauthorized Use
The following is a list of unauthorized uses of City-owned Bluetooth devices:
- Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.
- Using City-owned Bluetooth equipment on non-City-owned Bluetooth enabled devices.
- Unauthorized modification of Bluetooth devices for any purpose.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Data Backup and Restoration Policy
IS-100-04

Purpose:
The purpose of this policy is as follows:

- To safeguard the information assets of the City of Memphis
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the media employed in the process.

Scope:
This policy applies to all servers and databases in the data center (including the Network Attached storage (NAS)).

Policy:
- Data stored on the NAS appliance will be regularly backed up as follows:
    1. Incremental backup daily (Mon.-Fri.) and data located on-site.
    2. Full backups weekly (Sat.) and data located off-site.
- Exchange Mailbox stores will be regularly backed up as follows:
    1. Full backups daily (Mon.-Fri.) and data located on-site.
    2. Full backups weekly (Sat.) and data located off-site.
- Windows Servers will be regularly backed up as follows:
    1. Incremental backup daily (Mon.-Fri.) and data stored on-site.
    2. Full back-up weekly (Sat.) and data located off-site.

NOTE: A full backup contains every file on the system whereas an incremental backup only includes those files that have been changed since the last full backup.

Data Recovery

- In the event of a catastrophic system failure, off-site backed up data will be made available to users within 3 working days if the destroyed equipment has been replaced by that time.
- In the event of a non-catastrophic system failure or user error, on-site backed up data will be made available to users within 1 working day.

Restoration Requests

In the event of accidental deletion or corruption of information, requests for restoration of information will be made through a trouble ticket completed by the user and submitted to the Information Service's Help Desk.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Audit Vulnerability Scan Policy
IS-100-05

Purpose:
The purpose of this policy is to set forth the City of Memphis policy regarding network security scanning offered by the City. Information Services-approved software will be utilized to perform electronic scans of networks and/or firewalls or on any system used by the City.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents to ensure conformance to City security policies
- Monitor user or system activity where appropriate.

Scope:
This policy covers all computer and communication devices owned or operated by the City of Memphis. This policy also covers any computer and communications device that are present on City premises, but which may not be owned or operated by the City or its designate. The auditors will not perform Denial of Service activities.

Policy:
When requested, the City shall provide consent for members of the audit group to access its networks and/or firewalls to the extent necessary to allow the performance of the scans authorized in this policy. The City shall provide protocols, information, and network connections sufficient for the auditors to utilize the software to perform network scanning.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on City equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on City networks.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Anti-Virus Policy
IS-100-06

Purpose:
The purpose of the Anti-Virus Policy is to establish the requirements for protection from malware infection, prevention, detection and cleanup. A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, CDs, or thumb/pin drives. A virus infection can be very costly to the City in terms of lost/corrupted data, lost staff productivity, lost reputation and citizen's confidence.

Scope:
This policy applies to all City employees (part-time and full-time), consultants, and any other third party service provider that utilizes any City computer. It applies to all city issued computers that are connected to network, wireless connection, or Virtual Private Network (VPN) connection. The definition of computer means all City-owned computers that are connected to the City of Memphis network, including desktop workstations, laptop computers, hand held computing devices and servers.

Policy:
The City will use a single anti-virus product for anti-virus protection:

- All City of Memphis computers, whether connected to the network or standalone must utilize Information Services management-approved virus protection software and configuration.
- The virus protection software must not be disabled or bypassed at any time.
- The settings for the virus protection software must not be altered in any manner that will reduce the effectiveness of the software.
- The automatic update frequency of the virus protection software must not be altered to reduce the frequency of the updates.
- The email server will have Information Services management approved virus protection software which includes but is not limited to scanning of all inbound and outbound emails.
- A user may become aware that a virus has not been automatically cleaned upon receipt of a pop-up message from the virus protection software. Every malware that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the City of Memphis' Help Desk immediately.

- Virus-infected computers are removed from the network until they are verified as virus-free by the ISD field technician, MPD RTCC IT-Technician, and or the ISD Desktop Engineering team.

- Any activities with the intention to create and/or distribute malicious programs into the City's network (e.g., virus, worms, Trojan horses, e-mail bombs, etc.) are prohibited.
- All users must comply with the Anti-Virus Guidelines.

Enforcement:

Any employee who is found in violation of this policy may be subject to disciplinary action, up to and including termination of employment, possible civil and/or criminal prosecution to the full extent of the law.

Data Line Usage Policy
IS-100-07

Purpose:
This policy explains the City of Memphis analog and data line acceptable use and approval policies and procedures. This policy covers two distinct uses of analog/data lines: (i) lines connected for the sole purpose of fax sending and receiving, and (ii) lines connected to computers.

Scope:
This policy covers only those lines that are to be connected to a point inside City building and testing sites. It does not pertain to data/phone lines that are connected into PBX desktop phones, and those lines used by Telecom for emergency and non-City information purposes.

Policy:

Facsimile Machines
As a rule, the following applies to requests for fax and analog lines:

- Fax lines are to be approved for departmental use only.
- No fax lines will be installed for personal use.
- No analog lines will be placed in a personal cubicle.
- The fax machine must be placed in a centralized administrative area designated for departmental use, and away from other computer equipment.
- A computer which is capable of making a fax connection is not to be allowed to use an analog line for this purpose.

Waivers for the above policy on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect to the level of sensitivity and security posture of the request.

Computer-to-Analog Line Connections
The general policy is that requests for computers or other intelligent devices to be connected with analog or data lines from within the City will not be approved for security reasons. Waivers to the policy above will be granted on a case-by-case basis. Replacement lines, such as, those requested because of a move, fall under the category of "new" lines. These requests will also be considered on a case-by-case basis and shall comply with the requirements in the *Data Line Usage Guidelines*.

Use of an analog/data fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized users to enforce at all times:

- The fax line is used solely as specified in the request.
- Only persons authorized to use the line have access to it.
- When not in use, the line is to be physically disconnected from the computer.
- When not in use, the computer is to be physically disconnected from the City's internal network.
- The line will be used solely for City business, and not for personal reasons.
- All downloaded material, prior to being introduced into City systems and networks, must have been scanned by an approved anti-virus utility (e.g., Symantec Endpoint Protection) which has been kept current through regular updates.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Computer/Mobile Device Disposal Policy
IS-100-08

Purpose:
The purpose of this policy is to define the process and procedures for proper disposal of City-owned computers and mobile devices.

Scope:
This policy applies to all City-owned portable computers and mobile devices to include but not limited to:

- Laptops,
- Netbooks,
- iPads,
- Tablets,
- Other mobile data devices such as iPhones

Policy:
- Only obsolete and un-repairable/discontinued computer equipment and/or mobile data devices will be considered for disposal. The decision to dispose of the asset will be made by Information Services only.
- Information Services will be responsible for ensuring all City data is completely removed/erased from the hard drives of City-owned computer and mobile devices before physical disposal. Information Services will wipe or devices in accordance with US Department of Defense Standards which provide guidelines and/or recommendations for overwriting data to ensure that no data may later be recovered from the equipment or storage media.
- Information Services will identify each asset ready for disposal and update the status to "inventory" in the asset database.
- Information Services will maintain a record of all equipment sent for disposal and the method in which information was removed (*i.e.*, date of information removal, overwriting or physical destruction) from each device.
- Assets ready and approved for disposal will be picked up, transferred to a secure facility, and destroyed professionally by the City's current vendor, who is designated to properly dispose of computer equipment and mobile devices.
- Once assets are removed by the current vendor, their status will be changed to "OBSOLETE" in the asset database.

Note:
All assets marked for disposal must never be thrown in the trash. They must be disposed of securely and safely.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action which may include losing the privilege of utilizing personal computers or other data devices on the City's network, up to and including termination of employment, with possible civil and/or criminal prosecution to the full extent of the law.

Internet Use Monitoring and Filtering Policy
IS-100-09

Purpose:
The purpose of this policy is to define standards for systems that monitor and limit web use from any host within the City's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

Scope:
This policy applies to all City of Memphis employees, contractors, vendors and agents with a City owned computer connected to the City's network. This policy applies to all end user initiated communications between the City's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

Policy:

Web Site Monitoring
The Information Services Department shall monitor Internet use from all computers and devices connected to the corporate network. For all traffic the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system should record the User ID of the person or account initiating the traffic. Internet use records will be preserved for 180 days.

Internet Use Filtering System
The Information Services Department shall block access to Internet websites and protocols that are deemed inappropriate for the City's environment. The following protocols and categories of websites should be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- SPAM, Phishing and Fraud
- Spyware
- Violence, Intolerance and Hate

Internet Use Filtering Rule Changes
The Information Services Department shall periodically review and recommend changes to web and protocol filtering rules are to be made. Changes to web and protocol filtering rules will be updated in the *Internet Use Monitoring and Filtering Policy*.

Internet Use Filtering Exceptions
If a site is mis-categorized, employees may request for the site to be un-blocked by submitting a trouble ticket to the Information Services help desk. An IT employee will review the request and un-block the site if it is mis-categorized. Employees may access blocked sites with permission if appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorized, they must submit a request to their supervisor. Upon receiving the appropriately signed form(s), Information Services will unblock that site or category for that employee(s) only. Information Services will track approved exceptions and report on them upon request.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
Filtering:	Using technology that monitors each instance of communication between devices on the City's network and the Internet and blocks traffic that matches specific rules.
User ID:	User Name or other identifier used when an employee logs into the City's network.
IP Address:	Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.
SMTP:	(Simple Mail Transfer Protocol). The Internet Protocol that facilitates the exchange of mail messages between Internet mail servers.
Peer to Peer File Sharing:	Services or protocols such as BitTorrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts.

SPAM:	Unsolicited Internet Email. SPAM sites are websites link to from unsolicited Internet mail messages.
Phishing:	Attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.
Hacking	Sites that provide content about breaking or subverting computer security controls.

Internet DMZ Equipment Policy
IS-100-10

Purpose:
The purpose of this policy is to define the requirements for all equipment owned and/or operated by the City of Memphis and located outside the City's Internet firewalls. Devices that are Internet facing and outside the City firewall are considered part of the "de-militarized zone" (DMZ) and subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet.

These requirements are designed to minimize the potential exposure to the City from the loss of sensitive or City confidential data, intellectual property, damage to public image, etc., which may result from unauthorized use of City resources.

The policy defines the following requirements:

- Ownership responsibility
- General configuration requirements
- Operational requirements
- New installations and Change control requirements

Scope:
All equipment or devices deployed in a DMZ owned and/or operated by the City (including hosts, routers, switches, etc.) and/or registered in any Domain Name System (DNS) domain owned by the City, must follow this policy.

This policy covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in the City's various Internet domains or appears to be owned by the City.

All new equipment which falls under the scope of this policy must be configured according to the general configuration requirements set forth in this policy, unless a waiver is obtained from Information Services. All existing and future equipment deployed on the City's Un-trusted Networks must comply with this policy.

Policy:

Ownership and Responsibilities
Equipment and applications within the scope of this policy must be administered by Information Services.

Support groups will be responsible for the following:

- Equipment must be documented in the City-wide enterprise management system. At a minimum, the following information is required:
    - Host contacts and location.
    - Hardware and operating system/version.
    - Main functions and applications.
    - Password groups for privileged passwords.
- Network interfaces must have appropriate Domain Name Server records (minimum of A and PTR records).
- Password groups must be maintained in accordance with the City-wide password management system/process.
- Immediate access to equipment and system logs must be granted to members of Information Services upon demand in accordance with the *Audit Policy*. To verify compliance with this policy, Information Services will periodically audit DMZ equipment.
- Changes to existing equipment and deployment of new equipment must follow change management processes/procedures.

General Configuration Policy

All equipment must comply with the following configuration policy:

- Hardware, operating systems, services and applications must be approved by Information Services as part of the pre-deployment review phase.
- Operating system configuration must be done according to the secure host and router installation and configuration standards.
- All patches/hot-fixes recommended by the equipment vendor and Information Services must be installed. This applies to all services installed, even though those services may be temporarily or permanently disabled. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
- Services and applications not meeting business requirements must be disabled.
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by Information Services.
- Services and applications not for general access must be restricted by access control lists.
- Remote administration must be performed over Secure Channels (e.g., encrypted network connections using SSH, SSL, or IPSEC) or console access independent from the DMZ networks. Where a methodology for Secure Channel connections is not available, one-time passwords (DES/Token) must be used for all access levels.
- All host content updates must occur over Secure Channels.

- Security-related events must be logged and audit trails saved to Information Services-approved logs. Security-related events include, but are not limited to the following:
    - User login failures.
    - Failure to obtain privileged access.
    - Access policy violations.

- Information Services will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

New Installations and Change Management Procedures
All new installations and changes to the configuration of existing equipment and applications must follow the following policies/procedures:

- New installations must be completed via the *DMZ Equipment Deployment Process*.
- Configuration changes must follow the City Change Management (CM) Procedures.
- Information Security must have written authorization to perform system/application audits prior to the deployment of new services.
- Information Security must be engaged, either directly or via CM, to approve all new deployments and configuration changes.

Equipment Outsourced to External Service Providers
The responsibility for the security of the equipment deployed by external service providers must be set forth in the contract with the service provider. Additionally, information related to security contacts, and escalation procedures should be addressed in the contract. The Legal Department is responsible for ensuring that contracts with third party services providers contain provisions that ensure third party compliance with this policy.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, possible civil and/or criminal prosecution to the full extent of the law.

External service providers found to have violated this policy may be subject to financial penalties, up to and including termination of contract.

Definitions:

Term	Definition
DMZ (de-militarized zone)	Any Un-trusted Network connected to, but separated from, the City's internal network by a firewall, used for external (Internet/partner, etc.) access from within the City, or to provide information to external parties. Only DMZ networks connecting to the Internet fall under the scope of this policy.
Secure Channel	Out-of-band console management or channels using strong encryption according to the *Acceptable Encryption Policy*. Non-encrypted channels must use strong user authentication (one-time passwords).

Un-Trusted Network	Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those resources.

Information Sensitivity Policy
IS-100-11

Purpose:
The Information Sensitivity Policy is intended to help employees outline the Sensitivity levels for the City of Memphis.

The information covered in this policy includes: electronic information, information on paper, and information shared verbally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect City Confidential information (e.g., City Confidential information should not be left unattended in conference rooms).

Scope:
All City of Memphis information is categorized into two main classifications:

- City Public
- City Confidential

City Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the City of Memphis.

City Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as citizens' personal data, development programs, law enforcement information and other information integral to City operation. Also included in City Confidential is information that is less critical, such as telephone directories, general organizational information, personnel information, etc., which does not require as stringent a degree of protection.

Policy:
The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. City Confidential information may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the City Confidential information in question.

- **Minimal Sensitivity:** General internal information; some personnel and technical information

  Marking guidelines for information in hardcopy or electronic form.

  Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

  Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "City Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "City Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, City information is presumed to be "City Confidential" unless expressly determined to be City Public information by a City employee with authority to do so.

  Access: City employees, contractors, people with a business need to know.
  Distribution within City: Standard interoffice mail approved electronic mail and electronic file transmission methods.
  Distribution outside of City internal mail: U.S. mail and other public or private carriers approved electronic mail and electronic file transmission methods.
  Electronic distribution: No restrictions except that it is sent to only approved recipients.

- **More Sensitive:** Financial, technical, and most personnel information

  Marking guidelines for information in hardcopy or electronic form.

  Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "City Confidential" or "City Proprietary", wish to label the information "City Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

  Access: City employees and non-employees with signed non-disclosure agreements who have a business need to know.
  Distribution within City: Standard interoffice mail approved electronic mail and electronic file transmission methods.
  Distribution outside of City internal mail: Sent via U.S. mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within City, but should be encrypted or sent via a private link to approved recipients outside of City premises.

- **Most Sensitive:** Intellectual Property, operational, personnel, financial, source code, & technical information integral to the success of the City.

  Marking guidelines for information in hardcopy or electronic form.

  Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that City Confidential information is very sensitive, you may should label the information "City Internal: Registered and Restricted", "City Eyes Only", "City Confidential" or similar labels at the discretion of your individual business unit or department.

  Access: Only those individuals (City employees and non-employees) designated with approved access and signed non-disclosure agreements.
  Distribution within City: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
  Distribution outside of City internal mail: Delivered direct; signature required; approved private carriers.
  Electronic distribution: No restrictions to approved recipients within the City, but it is highly recommended that all information be strongly encrypted.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
Appropriate measures	To minimize risk to the City from an outside business connection. City computer use by unauthorized personnel must be restricted so that, in the event of an attempt to access City corporate information, the amount of information at risk is minimized.
Configuration of City-to-other Entity Connections	Connections shall be setup to all other entities to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required	Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.
Approved Electronic File Transmission Methods	Includes supported SFTP clients and Web browsers.
Envelopes Stamped Confidential	You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.
Approved Electronic Mail	Includes all mail systems supported by Information Services. These include, but are not necessarily limited to Microsoft Exchange. If you have a business need to use other mailers contact the Service Desk.
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 the City is done via a license. Please contact the Service Desk if you require a license.
City Information System Resources	City Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.
Expunge	To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of a program such PGP or Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten.
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 Macs and PCs, 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 the City.

Encryption

Secure City Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication

One Time Password Authentication on Internet connections is accomplished by using a one-time password token to connect to the City's internal network over the Internet. Contact the Service Desk for more information on how to set this up.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link	A Private Link is an electronic communications path that the City has control over its entire distance. For example, all City networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. The City also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which the City has established private links include some short-term temporary links.

Guest Access Policy
IS-100-12

Purpose:

Typically, only City and/or contract employees have access to the City's network. There are specific circumstances that require others to be eligible for an account as a guest and therefore may be given access to a guest account.

Policy:

- A guest account is to be used as a temporary network account that is available to individuals who are visiting the City for a variety of reasons.
- A guest account is governed by the same computer and network usage policies as any other City account. Without a guest account a visitor to the City of Memphis would not be able to access the network.
- All guest account requests must be approved by the Director of Information Services and/or his/her designee as well as the divison director and/or manager requesting access
- Access will only be granted for the Internet and any other information specifically approved by executive management.
- All guest accounts will be purged from the system by Information Services once the guess access is no longer required.
- At no time will the City have an active guess account on the network that is not used to connect to a specific user.
- Without notifications, the City will conduct periodic reviews of all guest accounts.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, possible civil and/or criminal prosecution to the full extent of the law.

Email Use Policy
IS-100-13

Purpose:
The purpose of this policy is to describe the acceptable use of email by City of Memphis employees, contractors, vendors, and agents operating on behalf of the City.

Scope:
This policy addresses any email sent from a City of Memphis email address and applies to all employees, vendors, and agents operating on behalf of the City.

Policy:

Prohibited Use
City of Memphis email system shall not to be used for the creation or distribution of any libelous, physically threatened, disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. All individuals using a City of Memphis email address are prohibited from sending or forwarding emails, chain mail/letters or joke emails from a City email account. Additionally, all users are prohibited from using email in any way that may disrupt or delay the timely and orderly provision of email services at the City of Memphis or transmitting, displaying, printing, or storing any material prohibited by law or regulations.

Personal Use
The City of Memphis resources are intended to be used for City for City business purposes. Using City of Memphis resources for personal emails is acceptable provided that such use does not interfere with duties or work performance. Employees are expected to exercise good judgment regarding the reasonableness of personal use.

Monitoring
City of Memphis employees shall have no expectation of privacy in anything they store, send or receive on the City's email system. The City may monitor messages without prior notice. The City of Memphis is not obligated to monitor email messages.

Reporting
Employees who receive any emails with this content (described above) from any City employee should report the matter to their supervisor immediately.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, possible criminal and/or civil prosecution to the full extent of the law.

Definitions:

Term:	**Definition:**
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Microsoft Outlook and Entourage.
Forwarded Email	Emails resent from an internal network to an outside point.
Chain Email or Letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

Data Base Password Policy
IS-100-14

Overview:
Computer programs running on City networks often require the use of internal database servers. In order to access a database, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the Credentials are meant to restrict and can be compromised when the Credentials are improperly stored.

Purpose:
This policy identifies the requirements for securely storing and retrieving database usernames and passwords *(i.e.,* database credentials). In order to maintain security of the City's internal databases, access will only be granted after authentication of user credentials.

Scope:
This policy applies to all applications that will access a City-owned multi and single-user Production databases.

Policy:
- The Credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text.
- Database Credentials must not be stored in a location that can be accessed through a web server.

Storage of Data Base User Names and Passwords
- Database user names and passwords must be stored in a file separate from the executing body of the program's code.
- Database Credentials may reside on the database server. A hash number identifying the Credentials may be stored in the executing body of the program's code.
- Database Credentials may not reside in the documents tree of a web server.
- Pass-through authentication (*i.e.,* Oracle OPS$ authentication) must not permit access to the database based solely upon a remote user's authentication on the remote host.
- Passwords used to access a database must adhere to the *Password Policy and Guidelines*.

Retrieval of Database User Names and Passwords
- If database user names and passwords, stored in a file that is not source code, then the database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

- Stored database credentials must be logically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database Credentials. Sharing of Credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the *Password Policy*.
- **Developer groups** must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
Computer language	A language used to generate programs.
Credentials	A combination of password/pass phrase that identifies a user and is unique to a particular individual (e.g., a user name, a fingerprint, voiceprint, retina print). This information should be kept in strict confidence and will be presented for authentication.
Executing Body	The series of computer instructions that the computer executes to run a program.
Hash	An algorithmically generated number that identifies a datum or its location.
Production	Software that is being used for a purpose other than when software is being implemented or tested

DMZ Lab Security Policy
IS-100-15

Purpose:

This policy establishes information security requirements for all networks and equipment deployed in City of Memphis labs located on the "De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to the City from the damage to public image caused by unauthorized use of City resources, and the loss of sensitive/company confidential data and intellectual property.

Scope:

City Lab networks and devices (including but not limited to routers, switches, hosts, etc.) that are Internet facing and located outside the City Internet firewalls are considered part of the DMZ Labs and are subject to this policy. This includes DMZ Labs in primary Internet Service Provider (ISP) locations and remote locations. All existing and future equipment, which falls under the scope of this policy, must be configured according to the referenced documents. This policy does not apply to labs residing inside the City's Internet firewalls. Standards for these labs are defined in the *Internal Lab Security Policy*

Policy:

Ownership and Responsibilities

1. All new DMZ Labs must present a business justification with sign-off at the Division Directory level. Information Services must keep the business justifications on file at all times.
2. Department within the City of Memphis that have DMZ Lab are responsible for assigning lab managers, point of contact (POC), and back up POC, for each lab. The lab owners must notify Information Services of any changes in POC and maintain POC information with Information Services. Lab managers or their backup must be available around-the-clock for emergencies.
3. Changes to the connectivity and/or purpose of existing DMZ Labs and establishment of new DMZ Labs must be requested through the Service Desk and approved by City Management.
4. All ISP connections must be maintained by Information Services.
5. Information Services must maintain a firewall device between the DMZ Lab(s) and the Internet.
6. Information Services reserve the right to interrupt lab connections if a security concern exists.
7. The DMZ Lab will provide and maintain network devices deployed in the DMZ Lab up to the City's point of demarcation.
8. Information Services must record all DMZ Lab addresses spaces and current contact information in the network management system.

9. The DMZ Lab Managers are ultimately responsible for their DMZ Labs complying with this policy.
10. Immediate access to equipment and system logs must be granted to members of Information Services upon request, in accordance with the *Audit Policy*.
11. Individual lab accounts must be deleted within three (3) business days when access is no longer authorized. Group account passwords must comply with the *Password Policy* and must be changed within three (3) business days from a change in the group membership.
12. Information Services will address non-compliance waiver requests on a case-by-case basis.

General Configuration Requirements

1. Production resources must not depend upon resources on the DMZ Lab networks.
2. DMZ Labs must not be connected to the City's corporate internal networks, either directly or via a wireless connection.
3. DMZ Labs should be in a physically separate room from any internal networks. If this is not possible, the equipment must be in a locked rack with limited access. In addition, the Lab Manager must maintain a list of who has access to the equipment.
4. Lab Managers, as well as users and individuals that have access to the DMZ are responsible for complying with the following related policies:
    a. *Password Policy*
    b. *Wireless Communications Policy*
    c. *Lab Anti-Virus Policy*
5. The Information Services maintained firewall devices must be configured in accordance with least-access principles and the DMZ Lab business needs
6. The firewall device must be the only access point between the DMZ Lab and the rest of the City's networks and/or the Internet. Any form of cross-connection which bypasses the firewall device is strictly prohibited.
7. Original firewall configurations and any changes thereto must be reviewed and approved by Information Services (including both general configurations and rule sets). Additional security measures may be required as needed.
8. Traffic from DMZ Labs to the City internal network, including VPN access, falls under the *Remote Access Policy*
9. All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.
10. Operating systems of all hosts internal to the DMZ Lab running Internet Services must be configured to the secure host installation and configuration standards.
11. Current applicable security patches/hot-fixes for any applications that are Internet services must be applied. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
12. All applicable security patches/hot-fixes recommended by the vendor and Information Services must be installed. Administrative owner groups must have processes in place to stay current on appropriate patches/hotfixes.
13. Services and applications not meeting business requirements must be disabled.

14. City of Memphis Confidential information is prohibited on equipment in labs where non-City personnel have physical access (e.g., training labs), in accordance with the *Information Sensitivity Classification Policy.*

15. Remote administration must be performed over secure channels (e.g., encrypted network connections using SSH, SSL or IPSec) or console access independent from the DMZ networks.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment, or possible criminal and/or civil prosecution to the full extent of the law.

Definitions:

Term	Definition
Access Control List (ACL)	Lists kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
DMZ (de-militarized zone)	Networking that exists outside of City of Memphis primary firewalls, but is still under City administrative control.
Least Access Principle	Access to services, hosts, and networks is restricted unless otherwise permitted.
Internet Services	Services running on devices that are reachable from other devices across a network. Major Internet services include DNS, FTP, HTTP, etc.
Point of Demarcation	The point at which the networking responsibility transfers from Information Services to the DMZ Lab. This is usually a router or firewall.
Lab Manager	The individual responsible for all lab activities and personnel.
Lab	A Lab is any non-production environment, intended specifically for developing, demonstrating, training and/or testing of a product.
Firewall	A device that controls access between networks, such as an ASA, a router with access control lists, or a similar security device approved by Information Services.
Internally Connected Lab	A lab within the City's firewall and connected to the internal production network.

Incident Response Policy
IS-100-16

Purpose:
The purpose of the Incident Response Policy is to establish the responsibilities for reporting and responding to security incidents.

Scope:
The Incident Response Policy applies to all City employees (full-time or part-time, temporary and consultants).

Policy:
- All City employees (fulltime, part-time, temporary and consultants) are responsible for reporting known or suspected security incidents promptly, such as theft, loss of equipment or documents, altered data, unauthorized access and/or unauthorized acquisition of confidential information to the Information Services Help Desk.

- Security incident is defined as an adverse event *where restricted or confidential information is revealed or exposed to an unauthorized party* and may include any and all of the following:
  1. The theft or physical loss of City owned computer and/or mobile equipment containing or suspected to contain citizen, local business and/ or employee personal identifiable information.
  2. Printed copies of sensitive City financial information.
  3. Any other unauthorized access to City computer systems.

- Information Services has created a *Security Incident Report Form* to accurately record all security incidents for future reference. In addition to completing and submitting the form, please be sure to:
  1. Prevent further data exposure. For Information Services staff: if you are in a position to stop the unauthorized activity and prevent any further data loss, then do so. This may involve shutting down systems, terminating access, or disabling applications.
  2. Immediately notify your immediate supervisor and/or Director of the issue and any action taken.
  3. Gather the facts and record what you know. Immediately begin to keep a log of information and action taken along with the time and date stamp of those occurrences. For Information Services staff: preserve any and all records/logs of access, names of people involved (if known), the data itself, any information used to generate the data at issue and any other evidence that may be needed for a forensic evaluation of the issue.
  4. Provide contact information and be available for interaction with the IS Security Administrator and law enforcement if needed.

Other Recommendations:

1. Quickly work with other staff to determine if the activity is still in progress. If so, stop the unauthorized activity to prevent any further data loss. Begin to ascertain the extent of the breach and determine the source and type of data, amount of data, affected persons and to the degree possible, the exact data involved.
2. Appoint an incident response team. The composition and charge of the team will depend upon the type of breach and resulting data exposure. The team will conduct a preliminary assessment and risk assessment and help develop a tailored incident response plan. Once the incident is contained, this team will also evaluate changes in processes, systems and/or policies to prevent a repeat event.
3. Alert the appropriate departments and individuals *(i.e.,* Legal, Information Services, and others as the situation warrants).
4. Work with IS, the incident response team, and other internal or external parties to determine the identities of affected individuals and determine exactly how they are affected.
5. Review and refine the incident response plan as appropriate. Help ensure that appropriate resources are available.
6. Develop a separate data exposure notification plan. Provide accurate and timely notification that meets or exceeds all legal requirements. Develop remediation strategies as appropriate to the situation.
7. Communicate status as appropriate, determine next steps, and develop a final report to include lessons learned and action taken.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including, termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Confidential & Sensitive Data Transmission Policy IS-100-17

Purpose:

The Confidential and Sensitive Data Transmission Policy is intended to identify what information can be transmitted electronically.

Scope:

The information covered in this policy includes, but is not limited to, information that is either stored or shared via any means. This includes: 1) electronic information, 2) information that is on paper and 3) information shared verbally or visually (such as receiving/forwarding encrypted emails, telephone and video conferencing.
All City of Memphis' information is categorized into two main classifications:

- City Public
- City Confidential

City Public information is information that has been declared public knowledge by someone with the authority to do so, and can be given to anyone.

City Confidential is information that should be protected very closely, such as, personal identifiable information (PII), personal credit information (PCI), development programs, and other informational integral to the success of the City.

A subset of City confidential information is third party confidential information and open records requests.
Questions about the proper classification of a specific piece of information should be addressed to your manager/supervisor.

Policy:

City personnel will secure confidential information. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager.

The sensitivity policy below provides details on how to protect information at varying sensitivity levels. Use this Policy as a reference only, as City Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the City Confidential information in question.

Minimal Sensitivity: General City information; limited personnel and technical information

- **Access:** City employees, contractors, people with a business need to know.
- **Transmission/Distribution within the City:** Standard interoffice mail, and approved electronic mail and electronic file transmission methods. If marked CONFIDENTIAL, then the information should only be view by the individual to whom the transmission or distribution is addressed.

- **Transmission/Distribution outside of the City internal mail**: U.S. mail and other public or private carriers, and approved electronic mail and electronic file transmission methods.

- **Electronic distribution:** No restrictions except that it is sent encrypted to only approved recipients to prevent unauthorized disclosure of sensitive information.

More Sensitive: Business, financial, technical, and most personnel information

- **Access:** City employees and non-employees with signed non-disclosure agreements who have a business need to know.

- **Distribution within the City:** Standard interoffice mail approved electronic mail and electronic file transmission methods.

- **Distribution outside of the City's internal mail:** Must be sent via U.S. mail or approved private carriers.

- **Electronic distribution:** No restrictions to approved recipients within the City but must be encrypted or sent via a private link to approved recipients outside of City premises/infrastructure.

Most Sensitive: Intellectual Property information, operational information, personnel data, financial data, source code, & technical information integral to the success of the City.

- **Access:** Only those individuals City employees and non-employees) designated with approved access and signed non-disclosure agreements.

- **Distribution within the City:** Must be delivered direct, signature required, envelopes stamped confidential or approved electronic file transmission methods.

- **Distribution outside of the City internal mail:** Must be delivered direct; signature required; approved private carriers.

- **Electronic distribution:** No restriction to approved recipients within the City, but it is mandatory that all information be encrypted.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
Delivered Direct; Signature Required	Do not leave in interoffice mail slot; call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods	Includes supported FTP clients and Web browsers
Envelopes Stamped Confidential	You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.
Approved Electronic Mail	Includes email systems supported by the City IT Support Staff.
Approved Encrypted Email and Files	Must utilize encryption application and file structure approve by City Information Services.
City Information System Resources	City Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the internal use only level and above.
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.
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 the City.
Encryption	Secure City Sensitive information in accordance with the *Encryption Policy*.
One Time Password Authentication	One Time Password Authentication on Internet connections is accomplished by using a one-time password token to connect to City's internal network over the Internet. Contact City Information Services support staff for more information on how to set this up.

Physical Security	Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. If you are in the office, then always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.
Private Link	A Private Link is an electronic communications path that the City has control over its entire distance.

Extranet Use Policy
IS-100-18

Purpose:
This policy describes the policy under which third party organizations connect to the City of Memphis networks. Such third organizations may only connect to the network for the purpose of transacting business related to the City.

Scope:
Connections between third parties that require access to non-public City of Memphis resources fall under this policy, regardless of whether a telecommunications circuit (such as frame relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for the City or to the Public Switched Telephone Network does NOT fall under this policy.

Policy:

Security Review
All new extranet connectivity will go through a security review with the Information Services department. The reviews are to ensure all access requests match the business requirements and that the principle of least access is followed.

Third Party Connection Agreement
All new connection requests between third parties and the City of Memphis require that the third party and City representatives agree to and sign the *Third Party Agreement (or a Memorandum of Understandng (MoU))*. This agreement must be signed by the Director of the Sponsoring Division as well as a representative from the third party who is legally empowered to sign on behalf of the third party. The agreement must also be signed by the Director/CIO of Information Services and the Chief Information Security Officer. The signed document is to be kept on file with the relevant extranet group.

Business Case
All production extranet connections must be accompanied by a valid written business justification, that is approved the department Director.

Point of Contact
The Sponsoring Division must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the Sponsoring Division, and is responsible for those portions of this policy and the *Third Party Agreement (or a Memorandum of Understanding (MoU))* that pertain to it. In the event that the POC changes, Information Services must be informed as soon as the change is made.

Establishing Connectivity
The Sponsoring Division must provide full and complete information as to the nature of the proposed connection. All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will the City of Memphis rely upon the third party to protect the City's network or resources.

Modifying or Changing Connectivity and Access
All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate change management process. The Sponsoring Division is responsible for notifying Information Services when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

Terminating Access
When access is no longer required, the Sponsoring Division within the City must notify Information Services as soon as it is determined that the connection is no longer needed, which will then terminate the access. This may mean a modification of existing permissions up to terminating the Circuit, as appropriate.

Reporting an Incident
If a security incident occurs or it is discovered that a Circuit has been deprecated and is no longer being used to conduct City business, then it may be necessary to modify existing permissions, or terminate connectivity. Information Services will notify the POC of the Sponsoring Division of the change prior to taking any action.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
Circuit	For the purposes of this policy, circuit refers to the method of network access, whether it is through traditional ISDN, Frame Relay etc., or via VPN/Encryption technologies.
Sponsoring Division	The City of Memphis Division making the request that the third party have access into the City network.
Third Party	A business or organization that is not a formal or subsidiary part of the City of Memphis

Password Policy
IS-100-19

Overview:
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. As such, all City employees (including contractors and vendors with access to City systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose:
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope:
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any City facility, has access to the City network, or stores any non-public City information.

Policy:
- All system-level passwords (e.g., root, enable, Administrator, Application Administration Accounts, etc.) must be changed quarterly or as required by authorized personnel such as the database administrator, application administrator, etc.
- All production system-level passwords must be secured and maintained by Information Services.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every three months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the following:
    - At least 10 characters in length
    - Contain at least one upper case
    - Contain at least one lower case
    - Contain at least one number
    - Contain a special character (i.e., #, *, !, @)
    - Single user to access account

Application Development Requirements

Application developers must ensure their applications contain the following security measures:

- Require authentication of individual users, not groups
- Passwords must not be in clear text or in any easily reversible form
- Provide for some type/form of role management, such that one user can take over the functions of another without having to know the other's password.
- Must support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, SQL database administrator).

Virtual Private Network (VPN) Policy
IS-100-20

Purpose
The purpose of this policy is to protect the City's electronic information from being inadvertently compromised by authorized personnel utilizing an Internet or dial-in connection.

Scope
This policy applies to all City employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing Virtual Private Networks (VPNs) to access the City's network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

Policy
- Approved City employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.
- It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to City internal networks.
- VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
- When actively connected to the City's network, VPNs will force all traffic to and from the PC over the VPN tunnel. All other traffic will be dropped.
- Dual (split) tunneling is NOT permitted; only one network connection is allowed.
- VPN gateways will be set-up and managed by City Information Services.
- All city issued computers connected to City internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is equivalent to the standards required by the City.
- VPN users will be automatically disconnected from the City's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
- The VPN concentrator is limited to an absolute connection time of 24 consecutive hours.
- Only those VPN clients provided by Information Services may be used.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
IPSec Concentrator	A device in which VPN connections are terminated.

Personal Communications Devices and Voicemail Policy
IS-100-21

Purpose:
This policy describes Information Security Department's requirements for Personal Communication Devices and Voicemail for the City of Memphis.

Scope:
This policy applies to any use of personal communication devices (PCDs) or Voicemail issued by the City of Memphis and/or used for City business. This policy does not include and/or apply to PCDs which are not used for City business.

PCDs will be issued only to City personnel with duties that require them to be in immediate and frequent contact when they are away from their normal work locations. For the purpose of this policy, PCDs are defined to include handheld wireless devices, cellular telephones, laptop wireless cards and pagers. Effective distribution of the various technological devices must be limited to persons for whom the productivity gained is appropriate in relation to the costs incurred.

Handheld wireless devices may be issued, for operational efficiency, to City personnel who need to conduct immediate, critical City business. These individuals generally are at the executive and management level. In addition to verbal contact, it is necessary that they have the capability to review and have documented responses to critical issues.

Policy:

Bluetooth
Hands-free enabling devices, such as Bluetooth, may be issued to authorized City personnel who have received approval. Care must be taken to avoid being recorded when peering Bluetooth adapters, as Bluetooth 2.0 Class 1 devices have a range of 330 feet.

Voicemail
Voicemail boxes may be issued to City personnel who require a method for others to leave messages when they are not available. Voicemail boxes must be protected by a PIN which must never be the same as the last four digits of the telephone number of the voicemail box.

Loss and Theft
Files containing confidential or sensitive data may not be stored in PCDs unless protected by approved encryption. Confidential or sensitive data shall never be stored on a personal PCD. Charges for repair due to misuse of equipment or misuse of services may be the responsibility of the employee, as determined on a case-by-case basis. The cost of any item beyond the standard authorized equipment is also the responsibility of the employee. Lost or stolen equipment must immediately be reported and the data stored on that device will be wiped.

Personal Use
PCDs and voicemail are issued for City of Memphis business. Personal use should be limited to minimal and incidental use.

PCD Safety
Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
Bluetooth	Bluetooth is an industrial specification for wireless personal area networks (PANs), also known as IEEE 802.15.1. Bluetooth provides a way to connect and exchange information between devices such as personal digital assistants (PDAs), and mobile phones via a secure, globally unlicensed short-range radio frequency. Source: Wikipedia
Confidential/Sensitive Data	All data that is not approved for public release shall be considered confidential or sensitive.

Removable Media Disposal Policy
IS-100-22

Purpose:
The purpose of this policy is to define the process and procedures for proper disposal of City-owned removable media devices in order to ensure that confidential and/or sensitive information cannot be recovered by unauthorized individuals.

Scope:
This policy applies to all City-owned removable media (*i.e.*, CD-ROMS, DVDs, USB thumb drives, external hard drives, optical drives, magnetic tapes, etc.).

Policy:
- All City-owned removal media must be reformatted before disposal. This will ensure removal of sensitive and/or confidential City data. If an employee is not sure how the properly reformat the removal media, contact the Information Services' Help Desk (9010636-6100) for instructions. In general, it is insufficient to delete the information, as it may remain in a recoverable state on the media.
- Information Services will be responsible for reformatting and/or disposal of all hard drives. Before any disposal takes place, Information Services should receive confirmation that destruction has been approved by management (if applicable) and information found on the media has expired (i.e., media does not need to be archived for business or legal reasons). The disposal procedures used will depend upon the type and intended disposition of the media.

Note:
Disposal is the act of discarding media. All assets marked for disposal must never be thrown in the trash. They must be disposed of securely and safely, e.g. by incinerator or shredding. If no longer required, then the contents of any re-useable media that are to be repurposed or removed should be made unrecoverable. Physical destruction can be accomplished using a variety of methods, including incineration, pulverizing, shredding, melting and disintegration.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action which may include losing the privilege of utilizing personal computers or other data devices on the City's network, up to and including termination of employment, with possible civil and/or criminal prosecution to the full extent of the law.

Router Security Policy
IS-100-23

Purpose:
This policy describes the required security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of the City of Memphis.

Scope:
All routers and switches connected to City production networks are affected. Routers and switches within internal, secured lab networks are not affected. Routers and switches within DMZ areas fall under the *Internet DMZ Equipment Policy*.

Policy:
Every router must meet the following configuration standards:

- No local user accounts are configured on the router.
- Routers must use TACACS+ or RADIUS for all user authentication
- The enabled password on the router must be kept in a secure encrypted form usually controlled by the CIO and/or Deputy CIO.
- The router must have the enable password set to the current production router password from Information Services.
- The following are not allowed:
  1. IP directed broadcasts
  2. Incoming packets at the router sourced with invalid addresses such as RFC1918 address. The exception is for any such addresses that are in use within the internal network.
  3. TCP small services
  4. UDP small services
  5. All source routing
  6. All web services running on router
- Standardized SNMP community strings must be read.
- Access rules are to be added as business needs arise.
- The router must be included in the corporate enterprise management system with a designated point of contact.
- Each router must have the following statement posted in clear view:
  "*UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device*."
- Telnet will only be used with secure tunnel. SSH, specifically SSH v2, is the preferred management protocol.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law

Definitions:

Term	**Definition**
Production Network	The "production network" is the network used in the daily business of the City and includes: (i) Any network connected to the network backbone, either directly or indirectly, which lacks an intervening firewall device, and (ii). Any network whose impairment would result in direct loss of functionality to City employees or impact their ability to do work.
Lab Network	A "lab network" is defined as any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to the City nor affect the production network.

Server Security Policy
IS-100-24

Purpose:
The purpose of this policy is to establish requirements for the base configuration of internal server equipment that is owned and/or operated by the City of Memphis. Effective implementation of this policy will minimize unauthorized access to City proprietary information and technology.

Scope:
This policy applies to server equipment owned and/or operated by the City, and to servers registered under any City-owned internal network domain.

This policy is specifically for equipment on the internal City network. For secure configuration of equipment external to City on the DMZ, refer to the *Internet DMZ Equipment Policy*. Desktop machines and Lab equipment are not relevant to the scope of this policy.

Policy:

Ownership and Responsibilities
All internal servers deployed at the City must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Information Services. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Information Services.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

General Configuration

- Operating System configuration should be in accordance with approved Information Services guidelines.
- Services and applications that will not be used must be disabled, where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most current security patches must be installed on the system as soon as it becomes available the only exception is when said application would interfere with business requirements.
- Trust relationships between systems are a security risk and their use should be avoided. Do not use a trust relationship when some other method of communication is available.
- Always use standard security principles of least required access to perform a function.
- Do not use the root or Administrator account when a non-privileged account is available.
- If a methodology for a secure connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH, SSL, or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental backups will be retained for at least 1 month.
    - Weekly full backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to Information Services, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

Compliance

- Audits will be performed on a regular basis by authorized organizations within the City.
- Audits will be managed by the internal audit group or Information Services, in accordance with the *Audit Policy*. Information Services will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	**Definition**
DMZ De-militarized Zone.	A network segment external to the corporate production network.
Server	For purposes of this policy, a Server is defined as an internal City Server.

USER ACCOUNT, NETWORK SHARE AND EMAIL ACCOUNT DISABLING POLICY IS-100-25

Purpose:

The purpose of this policy is to describe the user account, network share and e-mail retention policy for City of Memphis employees, contractors, vendors, and agents operating on behalf of the City.

Scope:

This policy addresses the user account, network share and e-mail information contained within City of Memphis resources, such as e-mail, and network file shares.

Policy:

User access account:

The City will immediately, upon notification of a retirement, resignation or termination of any employee, contractor, vendor, and or agent, operating on behalf of the City, will disable the user access account. 30 days after disabling the account, the user access account will be deleted.

Network shared files:

30 days after disabling a user account, the City will delete any shared network data, with the exception of electronic information retained per the City's Electronic Data Retention policy or electronic information held within the confines of a legal hold, as directed by the City Attorney's office.

Email account data:

The City will immediately, upon notification of a retirement, resignation or termination of any employee, contractor, vendor, and or agent, operating on behalf of the City, retain online for a period of 30 days the e-mail account of any employee, contractors, vendors, and agents operating on behalf of the City. After the 30 day period has expired, the City will delete the e-mail account with the exception of electronic information retained per the City's Electronic Data Retention policy or electronic information held within the confines of a legal hold, as directed by the City Attorney's office.

Definitions:

Term:	**Definition:**
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP.
Network Files	Electronic data stored in a network directory.
User access Account	Used to grant someone access to electronic resources.
Disabling Account	Removing login access to an account by the resigned, retired, or terminated personnel.
Deleting Account	The electronic removal of the user access account.

Server Malware Protection Policy
IS 100-26

Overview:
The City of Memphis is entrusted with the responsibility to provide professional management of clients and servers as outlined in its legal responsibilities to the citizens and in each of the contracts with its customers. Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

Purpose:
The purpose of this policy is to outline which server systems are required to have anti-virus and/or anti-spyware applications.

Scope:
This policy applies to all servers that the City of Memphis is responsible to manage. This explicitly includes any system for which the City has a contractual obligation to administer. This also includes all server systems setup for internal use by the City, regardless of whether City retains administrative obligations or not.

Policy:
City operations staff will adhere to this policy to ensure that servers have anti-virus and/or anti-spyware applications installed on them and to deploy such applications as appropriate.

Anti-Virus
All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- Non-administrative users have remote access capability
- The system is a file server
- NBT/Microsoft Share access is open to the server from systems used by non-administrative users
- HTTP/FTP access is open from the Internet
- Other “risky” protocols/applications are available to this system from the Internet at the discretion of the City Information Services Management.
- Outbound web access is available from the system.

Mail Server Anti-Virus
If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.

Anti-Spyware
All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:

- Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet
- Any system where non-technical or non-administrative users have the ability to install software on their own

Notable Exceptions
An exception to the above standards may be granted with approval from Information Services if one of the following notable conditions applies to the system:

- The system is a SQL server
- The system is used as a dedicated mail server
- The system is not a Microsoft Windows-based platform

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
Server	For purposes of this policy, a server is any computer system residing in the physically secured data center owned and operated by the City of Memphis. In addition, this includes any system running an operating system specifically intended for server usage as defined by City Information Services Management that has access to internal secure networks. This includes, but is not limited to, Microsoft Server 2003 and all permutations, Microsoft Server 2008 and all permutations, any Linux/Unix based operating systems that external users are expected to regularly connect to and VMS.
Malware	Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a blend of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Spyware	Broad category of software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has also come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.
Anti-Virus Software	Consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).

Removable Media Policy
IS 100-27

Overview:
In today's work environment it is not uncommon for employees as well as management, to utilize removable media such as thumb or pin drive to store and transfer information form one device to another. As such, removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations.

Purpose:
To minimize the risk of loss or exposure of sensitive information maintained by the City of Memphis and to reduce the risk of acquiring malware infections on computers operated by the City.

Scope:
This policy covers all computers and servers owned and/or operated by the City of Memphis.

Policy:
City employees (full-time, part-time, vendors, contractors and agents) may only use City-owned removable media in their work computers. City-owned removable media may not be connected to or used in computers that are not owned or leased by the City without explicit permission of Information Service.

When sensitive information is stored on removable media, it must be encrypted in accordance with the City of Memphis *Encryption Policy* and the *Confidential and Sensitive Data Transmission Policy.* Exceptions to these policies may be requested on a case-by-case basis by Information Services.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Definitions

Term	Definition
Removable Media	Device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks not provided by the City.
Encryption	A procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.
Sensitive Information	Information which, if made available to unauthorized persons, may adversely affect the City of Memphis, its programs, or participants served by its programs. Examples include, but are not limited to, personal identifiers, social security numbers, credit card numbers, and financial information.
Malware	Software of malicious intent/impact such as viruses, worms, and Spyware.

Risk Assessment Policy
IS 100-28

Purpose:
To empower the Information Services Department to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Scope:
Risk assessments (RA) can be conducted on any entity within the City of Memphis or any outside entity that has signed a *Third Party Agreement (or Memorandum of Understanding (MoU))* with the City. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Policy:
- The execution, development and implementation of remediation programs are the responsibility of Information Services.
- Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable.
- Employees are further expected to work with the Information Services in the development of a remediation plan.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
Entity	Any business unit, department, group, or third party, internal or external to the City, responsible for maintaining City assets.
Risk	Those factors that could affect confidentiality, availability, and integrity of the City's key information assets and systems. Information Services is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

Remote Access Policy
IS 100-29

Purpose:
The purpose of this policy is to define requirements for connecting to the City of Memphis' network remotely. These requirements are designed to minimize the potential exposure to the City from damages which may result from unauthorized use of City resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical City internal systems, etc.

Scope:
This policy applies to all City employees, contractors, vendors and agents with a City-owned computer that connects to the City network. This policy applies to remote access connections used to do work on behalf of the City.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

Policy:
- General access to the Internet by employees, contractors, vendors, and agents that go through the City Network on personal computers is prohibited.
- Please review the following policies for details of protecting information when accessing the City's network via remote access methods, and acceptable use of City's network:
    1. *Encryption Policy*
    2. *Virtual Private Network (VPN) Policy*
    3. *Wireless Communications Policy*
    4. *Acceptable Use Policy*
- Secure remote access must be controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the *Password Policy and Guidelines*.
- At no time should any City employee, contractor, vendor or agent provide their login or email password to anyone, not even family members.
- City employees, contractors, vendors or agents with remote access privileges to the City's network must not use non-City email accounts (*i.e.*, Hotmail, Yahoo, AOL, Google), or other external resources to conduct City business, thereby ensuring that official business is never confused with personal business.
- Routers for dedicated ISDN lines configured for access to the City network must meet minimum authentication requirements of CHAP.
- Reconfiguration of a user's personal equipment for the purpose of split-tunneling or dual homing is not permitted.

- Frame Relay must meet minimum authentication requirements of DLCI standards.
- Non-standard hardware configurations must be approved by Information Services, including approval of the security configurations for access to hardware.
- All hosts connected to City internal networks via remote access technologies must use up-to-date anti-virus software. This requirement includes personal computers.
- Personal equipment that is used to connect to the City's networks must meet the requirements of City-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the City production network must obtain prior approval from Information Services.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	**Definition**
Cable Modem	Cable companies such as Comcast provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function.
DLCI	Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the City’s network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a City-

provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into City and an ISP, depending on packet destination.

DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to the City's internal network through a non-City controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-City network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into City's internal network via a VPN tunnel.
VPN	Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

Stolen/Loss Computer Equipment Policy
IS-100-30

Purpose:
The purpose of this policy is to define the procedure to follow in the event of stolen and/or lost City-owned computer or mobile data device.

Scope:
This policy applies to all City-owned computers and mobile devices to include:

- Laptops,
- Netbooks,
- iPads, Tablets,
- Other data devices such as iPhones

Policy:

- Employees must contact their area supervisor immediately after they become aware that their City-owned desktop/workstation and/or mobile data device is missing from their assigned work area or their possession.
- Once it has been determined that the equipment has been stolen or is missing, the department must file a police report and then notify Information Systems.
- The department must complete a *Stolen or Missing Computer Equipment Form*. Please provide details relating to the loss of theft, including:
    - Whether or not the device was logged into the City's network when stolen,
    - If it contained files with sensitive or confidential data, and
    - If those files were encrypted and password protected.
- Information Services or Legal may contact you in order to obtain additional details to determine the nature and scope of any compromised data.
- One copy of the form is to be given to Information Services and the second copy is to remain with the department for future records.
- Upon notification of theft or loss of computer equipment, Information Services will reset your password and block all access to network resources, including e-mail if necessary, until you can change your password. Other security measures may be taken depending on the level of access the individual(s) involved and the scope of the loo or theft
- If there is a potential compromise of sensitive information or exposure of network resources, the Legal department will coordinate notification to affected individuals, and report the incident to state or federal agencies and the media, as required.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action which may include losing the privilege of utilizing personal computers or other data devices on the City's network, up to and including termination of employment, with possible civil and/or criminal prosecution to the full extent of the law.

Personal Device Usage Policy
IS-100-31

Purpose:
This policy defines the use of employee personal device(s) within the City's network infrastructure.

Scope:
This policy applies to all full/part-time employees, contractors/sub-contractors, and vendors, who want to utilize a personal device/s such as laptops, netbooks, iPads, tablets, smart phones, etc… within the City's network.

Policy:
- Personal devices (as stated above) will not be authorized for connection into the city's secure network, wireless and or wired.
- Employee personal devices will only be allowed to connect to the city's 'guest' wireless network.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action and or including termination of employment, with possible civil and/or criminal prosecution to the full extent of the law.

Wireless Communication Policy (Wi-Fi)
IS-100-32

Purpose:
This purpose of this policy is to identify the requirements that wireless infrastructure devices must satisfy to connect to the City's network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Services Department are approved for connectivity to a City network.

Scope:
This policy applies to all employees, contractors, consultants, and temporary employees at the City of Memphis. This policy applies to all wireless infrastructure devices that are authorized to connect to a City of Memphis network or reside on a City site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data. The Information Services Department must approve exceptions to this policy in advance.

Policy:

General Network Access Requirements
All wireless infrastructure devices that reside at a City of Memphis site and connect to a City network, or provide access to information classified as City Confidential, City Highly Confidential, or City Restricted must:

- Abide by the standards specified in the *Wireless Communication Standard.*
- Must be installed, supported, and maintained by an approved support team.
- Use City-approved authentication protocols and infrastructure.
- Use City-approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.
- Information Services shall conduct regular site reviews to detect unauthorized wireless access points and report and/or remove them as appropriate.

Lab and Isolated Wireless Device Requirements
All lab wireless infrastructure devices that provide access to City Confidential, City Highly Confidential, or City Restricted information must adhere to the general network requirements. Lab and isolated wireless devices that do not provide general network connectivity to the City network must:

- Be isolated from the internal network (that is it must not provide any internal connectivity) and comply with the *DMZ Lab Security Policy* .
- Not interfere with wireless access deployments maintained by other support organizations.

Home Wireless Device Requirements

- Wireless infrastructure devices that provide direct access to the City network must conform to the Home Wireless Device Requirements as detailed in the *Wireless Communication Standard*.
- Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the City internal network. Access to the City network through this device must use standard remote access authentication.

Enforcement:

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	**Definition**
City Network	A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to City services.
MAC Address	The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.

Physical Access Policy
IS-100-33

Overview:
Physical security means providing the following: 1) environmental safeguards for, the data centers and equipment (servers, network, storage, printers, etc.,) and 2) controlling physical access to equipment and data on the City of Memphis network infrastructure in order to protect information technology resources from unauthorized use, in terms of both physical hardware and data perspectives.

Purpose:
The purpose of this policy is to establish standards for granting, monitoring, and terminating physical access to the City of Memphis network infrastructure and to protect equipment within the City of Memphis environment

Scope:
This policy applies to the City of Memphis data centers and network infrastructures including those located at City Hall, the main library, and the backup data center located in Smyrna, TN.

Policy:

Environmental Safeguards

- Air conditioning must be operational in City data center facilities that house information technology resources in order to prevent long-term heat damage and equipment failure.
- City data center facilities must have fire extinguishing devices present in the office area.
- City data center facilities equipment must be fitted with Surge Protectors to prevent power spikes and subsequent damage to data and hardware.
- Critical City data center equipment must each be connected to an Uninterrupted Power Supply (UPS) in order to prevent power spikes, brownouts, and subsequent damage to data and hardware.
- Electrical outlets must not be overloaded. Proper and practical usage of extension cords are to be reviewed annually.
- Water sensors must be placed under any raised floor.

Physical Access

- Physical access privileges to City data center facilities must be documented and managed by the Information Services Division.

- Access to City Information Technology network restricted facilities will be granted only to data center staff and affiliates whose job responsibilities require access to that facility.
- The process for granting card or key access to City data center facilities must include approval from the Director of Information Services Division.
- Secured access devices (e.g. access cards, keys, combinations, etc.) must not be shared with or disclosed to others by authorized users.
- Secured access devices that are no longer needed or in use, must be returned to Information Services Division where they will be logged appropriately before they are re-allocated to another authorized user.
- Lost or stolen City secured access devices must be reported to Information Security personnel immediately.
- Information Services is responsible for the removal of the secured access device rights of individuals that no longer requires access.
- Visitors and other invitees must be escorted and monitored while in restricted City data centers facilities.
- Information Services must review access records and visitor logs for each data center facility on a periodic basis, and investigate any unusual access. Visitor logs should include time in, time out, as well as the reason for visit and the City of Memphis personnel that will escort the visitor.
- All areas housing employees and other technology resources must be kept locked when not occupied by a City employee, in order to reduce the occurrence of unauthorized entry and access.
- Any piece of City equipment which resides in a public access area must be secured to a piece of furniture, counter-top, or other suitably deterrent object with a theft-inhibiting device. Portable computers must also be secured with theft-inhibiting devices.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, possible civil and/or criminal prosecution to the full extent of the law.

Geographic Information Systems Data Dissemination Policy
IS-100-34

Purpose:
The Geographic Information Systems (GIS) Policy is intended to outline the rules and procedures for the dissemination of GIS created and/or managed by the City of Memphis.

The information covered in this policy includes, but is not limited to, the GIS spatial data and intellectual property relating to or derived from GIS data that is owned and managed by the City of Memphis.

Scope:
All City of Memphis GIS data in all formats including:

- Shape files
- File Geodatabases
- Geodatabases
- Aerial Photography
- Tabular Data with Spatial Attributes (Addresses, Parcel ID, X,Y coordinates)

Policy:
City Personnel with access to GIS data will secure the data at all times by maintaining the data on their password protected City computer, their City network drive or within the Enterprise GIS geodatabase system.

Data request from external entities: The City Personnel must forward the request to the City's Legal Division for review and approval. If approval is given by Legal then the personnel will follow the guidelines provided by the City's Legal Division for the delivery of the requested data to the external entity. The details of the guidelines are dependent upon the nature of the data being requested.

Dissemination of GIS data via external online publically accessible mapping application or systems: City personnel must first obtain written approval via email from their supervisor stating that the data is permitted to be shared in a public forum. Then the personnel must contact the City's Enterprise GIS (EGIS) department, forward the approval email and allow the EGIS to evaluate the data in order to ensure the accuracy of the data and to check for topology and metadata errors. If the data does not meet the data integrity standards then corrections must be made by the City personnel requesting the dissemination. Upon approval of the data integrity it can be disseminated to the publicly accessible online applications or systems such as the ESRI ArcGIS Online.

Enforcement: Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, possible civil and/or criminal prosecution to the full extent of the law.

Intrusion Detection Policy
IS-100-35

Purpose:
The purpose of this policy is to establish and maintain electronic intrusion detection services (IDS) for the City of Memphis network.

Scope:
This policy applies to all City of Memphis Information Services employees, Information Services contractors, and Information Services related vendors and agents that are responsible for the design, deployment, and day-to-day operation of intrusion detection services. This policy applies to all external public and internal private sourced communications that access the City of Memphis infrastructure and production servers.

Policy:
Electronic Intrusion Detection
The Information Services Department will design, implement and maintain an electronic intrusion detection system to increase the security of our critical infrastructure and key business systems and data, such as Finance, Human Resources, Audit, and Mortgage Services. All traffic will be evaluated based on signature and behavior analysis and then dropped or passed accordingly. Suspicious traffic will be compiled into reports and then investigated and remediated appropriately by Information Services personnel, such as data center, network and information security.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

Definitions:

Term	Definition
Intrusion Detection System (IDS):	Hardware and/or software that that is used to detect the presence of malicious or suspicious network traffic.

Mobile Device Management
Policy IS-100-036

Purpose:
Mobile devices can hold and carry a great deal of information, both personal and work related. Mobile devices are issued by the City Of Memphis to employees on as needed basis. These devices are City Of Memphis owned and require monitoring.

Scope:
This policy applies to all City of Memphis employees and contractors who are issued mobile devices by the city.

Policy:
- The City Of Memphis provides the following type of mobile devices:
    - Air card (embedded and external)
    - Basic Phones
    - iPads
    - iPhones
    - Android Phones
    - Android Tablets
    - BlackBerrys__

- Information Services Division (ISD) will issue the approved mobile device with the required security solution installed.

- Each of the following will be enabled on City of Memphis issued mobile devices:
    - Enrollment in the ISD supported mobile tracking application
    - Remote lock and or unlock mobile devices
    - Remote wipe when the mobile device is stolen or lost
    - GPS – Location information

- The mobile security solution and its application must remain on the mobile device at all times.

- All City Of Memphis mobile devices will utilize the '**COM-Secure'** network only, designed specifically for the City Of Memphis mobile end users.

- Each approved user will sign a custody log, maintained by ISD.

- When a City Of Memphis mobile device end user becomes aware their mobile device is missing; they are required to contact the City Of Memphis Service Desk to report the device lost or stolen. ISD will remote wipe the asset, thus ensuring all data is no longer retrievable.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, or possible civil and/or criminal prosecution to the full extent of the law.

PCI Compliance Policy
IS-100-37

Overview:

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council (PCI SSC). The PCI SSC is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

Purpose:

The purpose of this policy is to establish a standard to protect cardholder data that is processed, or transmitted by the City of Memphis to credit card merchants.

Scope:

The scope of this policy includes all credit card process entities with City of Memphis (CoM) (such as Permits, Golf, Pink Palace, etc…).

Policy:

City of Memphis Information Services policy prohibits the storing and emailing of any credit card information in on any computer, server or database including Excel spreadsheets.
Compliance requirements are:

- Each Division utilizing credit card processing will be annually required, to attend PCI Compliance training provided by the CoM ISD – Information Security Officer.

- Credit card information must not be stored on City of Memphis network servers, workstations, or laptops.

- Credit card information must not be transmitted via email.

- Perform no less than a quarterly Network scan to include the credit card processing sites.

- Divisions accepting credit cards payments on behalf of the City will:
    1. Allow an annual self-assessment against the requirements to be conducted by ISD.
    2. All employees involved in processing credit card payments sign a statement that they have read, understood, and agree to adhere to Information Services policies of City of Memphis and this policy.
    3. Documented procedures for processing manual credit card transactions, in the event of a failure of the electronic system.

- All CoM provided computers using Encrypted Credit Card Swipe Devices, will be required to meet the following PCI DSSv3 requirements,:
    1. Anti-Virus installed and up to date
    2. Patches up to date
    3. Authentication – access (Logon and PW)
    4. Screen saver enabled

5. File Integrity Monitoring – must be able to monitor Windows System folder and the vendor card swipe software folder (if required) count

- Any proposal for a new process (electronic or paper) related to the storage, transmission or processing of credit card data must be brought to the attention of the Information Services Division and be approved by the CIO.

Enforcement:

The Information Security Officer will oversee enforcement of the policy. Additionally this individual will investigate any reported violations of this policy, lead investigations about credit card security breaches and may terminate access to protected information of any users who fail to comply with the policy. S/he will be assisted by the CIO, DCIO, Legal, and other City Officers as needed.
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and possible civil and/or criminal prosecution to the full extent of the law.

Patch Management Policy
IS-100-38

1.0 Overview
City of Memphis Information Services Division (ISD) is responsible for ensuring the confidentiality, integrity, and availability its data and that of customer data stored on its systems. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

2.0 Purpose
This document outlines the ISD's requirements for maintaining security and application patches and on all City of Memphis Information Services Division (ISD) owned and managed workstations and servers.

3.0 Scope
This policy applies to workstations and servers owned or managed by City of Memphis Information Services Division (ISD). This includes city systems that contain data owned or managed by City of Memphis Information Services Division (ISD) regardless of location.

The following ISD team members will be informed and kept up to date regarding the patch management process via email notification:

Deputy Chief Information Officer
Information Security Officer
GIS Program Manager
Data Center Team
Application Team Lead
Information Technology Officer
CAD Coordinator
End User Services Manager
GIS Technical Coordinator
MPD IT Liaison
Oracle Team Lead
Manager of Fire Communication

4.0 Policy
Workstations and servers owned by City of Memphis Information Services Division (ISD) will have up-to-date security & application patches for all software on the assets (to include Operating System, Vendor software) installed including all laptops, desktops, and servers owned and managed by City of Memphis Information Services Division (ISD).

The patches with a qualification level of 'Important' and higher (to include critical as well) will be applied to the City of Memphis Information Services Division (ISD) laptops, desktops, and servers, no less than once a month. On the third Tuesday (after working hours 6 to 11pm) of each month the Data Center will begin the server monthly patch process by utilizing the city approved Patch Management Tool. The Desktop Engineering Team will begin the laptop and desktop monthly patch process by utilizing the approved – software distribution tool.

The Fire Department CAD environment allows for Quarterly patching only, per their vendor requirement.

4.1 Workstations

Desktops and laptops must have automatic updates disabled. This is the default configuration for all workstations built by City of Memphis Information Services Division (ISD). Any exception to the policy must be documented and forwarded to the ISO for review. *See Section 8.0 on Exceptions.*

4.2 Servers

Servers will comply with the minimum baseline requirements approved by the City. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the City of Memphis asset and the data that resides on the system. Any exception to the policy must be documented and forwarded to the ISO for review. *See Section 8.0 on Exceptions.*

5.0 Roles and Responsibilities

- **Data Center** will manage the patching needs for the Linux and Microsoft Windows servers on the network (to include all software vendor patch releases)**.**
    - Subscribing to the various vendor newsletters on patching
    - Identify which patches can or cannot be removed after implementation
    - Communicate patch information to others
    - Create & update RFCs when appropriate

- **Desktop Engineering** (Workstations (desktops and laptops)) will manage the patching needs of all workstations on the network.
    - Subscribing to the various vendor newsletters on patching
    - Identify which patches can or cannot be removed after implementation
    - Communicate patch information to others
    - Create & update RFCs when appropriate

- **Information Security Officer** is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.
    - Run Monthly Audit Scans on server assets
    - Review Monthly LANDesk patch report for Workstations

- **The Change Control Board** is responsible for approving the monthly and emergency patch management deployment requests.

Other Administrators:

Administrators of systems (servers) not managed by the ISD (e.g., Memphis Police Department (MPD) Real Time Crime Center (RTCC)) are responsible for ensuring their servers are maintained in compliance with the CoM ISD Patch Management Policy or their own Patch Management Policy, which needs to be provided to the CoM ISD - ISO.

6.0 Monitoring and Reporting

Active patching teams noted in the Roles and Responsibility section (5.0) are required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Information Security and Internal Audit upon request.

7.0 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all employees within the ISD. Information Security and Internal Audit may conduct random assessments to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Repeated failures to follow policy may lead to disciplinary action.

8.0 Exceptions

Exceptions to the patch management policy require formal documented and approval from the Deputy CIO and or the CIO. Any servers or workstations that do not comply with policy must have an approved exception on file with the ISO. All exceptions will first be submitted through the ISD Remedy ticket process and a Request for Change (RFC) will be created to provide details as the requirement/need for exception as it relates to the Patch. The Change management Board has final approval regarding exceptions.

Electronic Data Retention Policy
IS-100-39

Purpose:
The purpose of this policy is to describe the electronic data retention of email, voicemail, and instant messages used by City of Memphis (CoM) employees, contractors, vendors, and agents operating on behalf of the City within the CoM network environment.

Scope:
This policy addresses the electronic data retention requirements for all email, instant messaging, & voicemail (converted to email), systems that are provided by the City for the purpose of conducting and supporting official City business activity through the City's network infrastructure.

Policy:

Email Retention
Email is retained (barring unanticipated database corruption) for the duration of employment with the City. Upon termination, resignation, and or loss of employment, an employee's email box will be purged after one year.

The only exception is when a litigation hold is placed on specific email account.

Voicemail sent to email
Voice mail is a resource provided by the City and is the property of the City. It is provided solely for business purposes. The City of Memphis email system has the capability to receive voicemail as an attachment in an email. These voicemails are a part of the electronic data retention policy and will be retained for no less than **30 days** after receipt.

Instant messaging (IM)
Instant Messaging is not a part of the electronic data retention policy and will not be retained.

Enforcement:
The retention of email, voicemail sent to email, & IM will be imposed by the Information Services Division (ISD) as noted above.

Annual Approvals:

Brent Nair – Chief Information Officer, City of Memphis

_____ Date: 12/3/15

Jack Sammons – Chief Administration Officer, City of Memphis

_____ Date: 12/3/15

Revision History:

Changed by:	**Date:**	**Ver:**	**Change:**
Brent Nair	April 19, 2013	1.0	Created policy
Susan Alders	December 10, 2015	2.0	Updated policies

Appendix

Anti-Virus Guidelines
IS-101-01

The following processes are required to prevent virus problems:

- Always run the City standard, supported anti-virus software that is available from the Information Services. Download and run the current version; download and install anti-virus software updates as they become available.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in accordance with the City's *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette or USB storage device from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. Periodically check the *Lab Anti-Virus Policy* and this Recommended Processes list for updates.

Bluetooth Setup Guidelines
IS-101-02

The following are setup guidelines for City-owned Bluetooth Devices:

Pins and Pairing

- When pairing your Bluetooth unit to your Bluetooth enabled equipment *(i.e.* phone, laptop, etc.), ensure that you are not in a public area.

Device Security Settings

All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.

- If your device allows the usage of long PINs, you must use either a 13 alphabetic PIN or a 19 digit PIN (or longer).
- Switch the Bluetooth device to use the hidden mode, and activate Bluetooth only when it is needed.
- Update the device's firmware when a new version is available.

Data Line Usage Guidelines
IS-101-03

Requesting an Analog/ISDN Line

All requests **MUST BE** approved by a manager. Once approved by a manager, the individual requesting an analog/ISDN line must provide the following information to Information Services:

- A clearly detailed business case of why other secure connections available at the City of Memphis cannot be used,
- The business purpose for which the analog line is to be used,
- The software and hardware to be connected to the line and used across the line,
- What external connections the requester is seeking to access

The business case must answer, at a minimum, the following questions:

- What business needs to be conducted over the line?
- Why is a City-equipped desktop computer with Internet capability unable to accomplish the same tasks as the proposed analog line?
- Why is the City's current dial-out access pool unable to accomplish the same tasks as an analog line?

In addition, the requester must be prepared to answer the following supplemental questions related to the security profile of the request:

- Will the machines that are using the analog lines be physically disconnected from the City's internal network?
- Where will the analog line be placed? A cubicle or lab?
- Is dial-in from outside of the City of Memphis needed?
- How many lines are being requested, and how many people will use the line?
- How often will the line be used? Once a week, 2 hours per day...?
- What is the earliest date the line can be terminated from service?
- The line must be terminated as soon as it is no longer in use.
- What other means will be used to secure the line from unauthorized use?
- Is this a replacement line from an old location? What was the purpose of the original line?
- What types of protocols will be run over the line?
- Will a City-authorized anti-virus scanner be installed on the machine(s) using the analog lines?
- The requester should use the Analog/ISDN Line Request Form to address these issues and submit a request.

Password Guidelines
IS-101-04

General Password Construction Guidelines

Passwords are used for various purposes at the City of Memphis. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords:

Poor, weak passwords have the following characteristics:

- The password contains less than ten (10) characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "City", "Memphis," or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Repetitive characters such as, “mmmmmmmmm”
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

Password Protection Standards

- Do not use the same password for City accounts as for other non-City access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, **do not** use the same password for various City access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for a Windows account and a UNIX account.

- Do not share City passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential City information.

- If someone demands a password, refer them to the **Password Guidelines** or have them call someone in the Information Services Department.

- Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook).

- Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including iPhones or similar devices) without encryption.

- Change passwords at least once every three months (except system-level passwords which must be changed quarterly).

- If an account or password is suspected to have been compromised, report the incident to Information Services and **immediately** change all passwords.

Recommendation:
If a user makes a certain number of unsuccessful login attempts, then the system will automatically disable the user ID.

Virtual Private Network (VPN) Guidelines
IS-101-05

The following guidelines must be followed in order to access the City of Memphis' internal network via its virtual private network (VPN) gateway:

- VPN access to the City of Memphis network will only be granted to users who have a valid requirement for such access as part of their duties performed for the City. A *Information Services Access Request Form* must be completed, reviewed, approved, and signed by the Deputy CIO prior to granting VPN access.
- The City of Memphis, Information Services will **NEVER** employ generic VPN accounts. For security reasons, **ALL** VPN accounts will be established for specific named users only.
- Information Services will be responsible for maintaining a list of active VPN user accounts. It is the responsibility of the vendor to inform the City when users leave the company or change to a role which does not require VPN access.
- VPN accounts must **NEVER** to be shared within the vendor environment or between City employees who have VPN account access.
- Once VPN accounts have been established for vendor personnel, they will only be enabled when work is to be done:
    - To activate a VPN account, the vendor must contact the Information Services Service Desk to place a request to have the account enabled.
    - Once the vendor has completed its use of the VPN account for the work being done, they will call the Information Services Help Desk to have the account disabled until needed again.
    - If the vendor does not contact the Information Services Help Desk when work is complete, Information Services will automatically disable account access twenty-four (24) hours after enablement without vendor notification.
    - If a vendor requires VPN access for more than a 24-hour period, an official request with justification must be made to Information Services for a longer enablement period.
- Information Services reserves the right to disable any VPN account if the City believes the access is being abused in any way. It is the responsibility of the VPN account holder to ensure that the VPN access policy is adhered to in its entirety.

Wireless Communication Standards
IS-101-06

Overview:

The purpose of this standard is to secure and protect the information assets owned by the City of Memphis. The City provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. The City grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a City network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by Information Services are approved for connectivity to a City network.

Scope:

All employees, contractors, consultants, temporary and other workers at the City, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of the City, must adhere to this standard. This standard applies to all wireless infrastructure devices that connect to a City network or reside on a City site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data. City Information Services must approve exceptions to these standards in advance.

Policy:

General Requirements

All wireless infrastructure devices that connect to a City network or provide access to City Confidential, City Highly Confidential, or City Restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.

- Use Temporal Key Integrity Protocol (TKIP) or (preferably) Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.

Lab and Isolated Wireless Device Requirements

- Lab device Service Set Identifier (SSID) must be different from City production device SSID.
- Broadcast of lab device SSID must be disabled.

Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a City network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Enable Wi-Fi Protected Access 2 Pre-shared Key (WPA2-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA2-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

References

In support of this standard, the following policies, guidelines, and resources are included:

- *Information Sensitivity Policy*
- *Wireless Communication Policy*

Enforcement:

This standard is part of the *Wireless Communication Policy* and failure to conform to the standard is a violation of the policy. Any employee found to have violated the policy may be subject to disciplinary action, up to and including termination of employment. Any violation of the policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the City.

Definitions:

Term	Definition
AES	Advanced Encryption System

City network	A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to City services.
Corporate connectivity	A connection that provides access to a City network.
EAP-FAST	Extensible Authentication Protocol-Fast Authentication via Secure Tunneling: authentication protocol for wireless networks.
EAP-TLS	Extensible Authentication Protocol-Translation Layer Security, used to create a secured connection for 802.1X by pre-installing a digital certificate on the client computer.
Enterprise Class Teleworker	An end-to-end hardware VPN solution for teleworker access to the City network.
Information assets	Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.
PEAP	Protected Extensible Authentication Protocol, a protocol used for transmitting authentication data, including passwords, over 802.11 wireless networks.
Service Set Identifier (SSID)	A set of characters that give a unique name to a wireless local area network.
TKIP	Temporal Key Integrity Protocol, an encryption key that's part of WPA.
WPA2-PSK	Wi-Fi Protected Access 2 pre-shared key

Patch Management Process
IS-101-07

Patch Management Process (Servers)

Purpose:
To ensure all servers, maintained by the City of Memphis Data Center, have the most current (latest) vendor released patches applied within the month of their release.

- Data Center will manage the patching needs for the Linux and Microsoft Windows servers on the network (to include all software vendor patch releases).
- Workstations (desktops and laptops) managed by Desktop (Workstations) Engineering Team

Pre-Patch Management:
All communications will be provided to the following City Of Memphis Information Services Division Management as it pertains to the Patch Management process via Change Management Board meetings (Request For Change (RFC) submitted for server sets to be patched) and email notification when completed:

Deputy Chief Information Officer
Information Security Officer
GIS Program Manager
Data Center Team
Application Team Lead
Information Technology Officer
CAD Coordinator
End User Services Manager
GIS Technical Coordinator
MPD IT Liaison
Oracle Team Lead
Manager of Fire Communication

Pre-Patching Scans:
The Information Security Officer will perform and provide 'pre-patching' scans to the Data Center team by the end of the second week of each month, and provide a list of outstanding patches needed for the servers.

Exception List:
The Data Center Team Lead will note which patches can be removed versus which ones cannot due to noted/documented exceptions.

Test/No Test:
Data Owners are key players as it relates to patch management. They will provide the following information to the Data Center prior to patching:

- Provide information related to any type of possible 'Risk' to their data
- Call out an "Test/No Test' email to the Change Control Board members to include the Data Center Team, prior to the Test environment being patched
- Provide a detail description of the reason/s for 'Not' patching a specific asset.

After the "Test' result, the Data Center will use LANDesk, where available, to create a list of all currently installed patches on the server/s. A manual audit will be conducted on any server which LANDesk will not work.

Prior to the third Tuesday of each month the Data Center will conduct an internet search looking for known issues to the latest patch release. With a positive report from the Internet search the Data Center will create 'RFCs' to use LANDesk to push the accepted patches, which are from the 'Important' and higher level, to all applicable servers as identified on the 'Server Sharepoint site': http://memsharepoint1/DataCenter/Lists/Servers/AllItems.aspx which is broken down into days for each set of servers in order to avoid to many patches on to many servers at once. This process will help troubleshoot if the server responds poorly to an applied patch.

Patch Management:
Once the created RFCs have been approved by the Change Control Board, the Data Center team will start the Patch Process.

Patching will start after normal working hours; the 6pm to 11pm time frame has been designated as the 'Patch Window' for the third week of the month. Starting on Tuesday (Test 1), Wednesday (day 1), Thursday (day 2), Friday)day 4 and Sunday (day 5), as indicated on the ISD SharePoint site: http://memsharepoint1/DataCenter/Lists/Servers/AllItems.aspx for each server. If and or when there has been a delay in the patching process Saturday can be used as a catch up day if approved by management.

When all the patches for the patch day have been applied an email to MEM Change Control Board mail address will be provided reporting the patch status for that day (which includes the ISD management team – noted earlier). If there is any issue that comes from patching a server the RFC will be documented with the effects and resolve.

Back Out Plan:
The Request For Change (RFC) for each set of servers will have a documented 'Back Out Plan'. The first step in the 'Back Out Plan' will be to analyze the symptoms and research/discover the core cause of the issue noted after patching. ***Important***The first step is NOT to remove the patch.

> *Ex: When a server has an issue within a two day time frame of being patched the data owner must also troubleshoot the issue and assist in identifying whether it is truly the patch that has caused an issue or something else has occurred. If there is a group of server/s that have the same patch applied and only one of those is having an issue, removing the patch should be the last recourse prior to detailed troubleshooting.*

The Change Approval Board (CAB) will determine when and if an applied patch should be removed. In the event that a patch must be removed and the patch can be removed, the Data center will use the Vendor approved method of patch removal for the appropriate server.
Once approved the details are documented within the RFC relative to the day it was patched, and documented in the 'Master Exception' list for patches that cannot be applied to a specific asset.

Post Patching Scans:
Post patching scans will occur after the data Center team has informed the ISO all assets have

been successfully patched. The scans will start no later than the end of the third week of the month. These scans will be provided to the Data Center for review and resolve as required to ensure current patching has been applied to all ISD servers.

The Fire CAD Patching Process:
Due to the nature of the FireCAD system it was agreed that all patching would be done on a quarterly basis. The Patching process will be coordinated between the two divisions (ISD and Memphis Fire Department (MFD)). This process has been approved by both divisions.

Pre-patching Scanning will be completed by the ISO. The Only server NOT to be scanned will be the 'CAD' server, this is a noted exception.

2 weeks prior to implementation date:
The Data Center personnel will send a list of the servers to be patched to the Information Technical Officer (ITO), CAD coordinator, Fire Communications Coordinator and the CAD system vendors for the MFD.
The Data Center personnel will coordinate a meeting between MFD and the vendors to discuss which 2 days are best for patching and inquire about any known patching issues.

The Data Center Team Lead (Manager) will create an RFC for each patch day. Data Center Manager will send a notification to the ITOs, the CAD coordinator and the Fire Communications Coordinator of the RFCs approval.

1 week prior to implementation date
Data Center Manager will send a reminder to the ITOs, the CAD coordinator and the Fire Communications Coordinator of the patch days and confirm the approved date of patching.

****NOTE**** Prior to beginning the patch process the Data Center personnel will confirm with the 'Backup' vendor that they have a valid backup of each server to be patched. Using LANDesk, the Data Center personnel will select the patches to be applied to each server.

Data Center personnel will monitor the patching of the servers via LANDesk. At the completion of the patching process, Data Center personnel will print a report from LANDesk on the success or failures of the patching and attempt to resolve any failure issues provided there is remaining time in the outage window.

Expected duration of time for patching is two days.

Post-Patching Scanning will be completed by the ISO after notification from the Data Center lead. The Only server NOT to be scanned will be the 'CAD' server, this is a noted Exception.

City of Memphis ISD Patch Management Process (Workstations)

Purpose:
To ensure all workstations (desktops & laptops), maintained by the City of Memphis ISD, have the most current (latest) vendor released patches applied within the month of their release.

Software Patch list:
ISD is responsible for the approved software list imaged on the workstations within the City of Memphis Information Technology environment. The below list of software is purchased, licensed and maintained by the ISD:

Microsoft Windows 7
Microsoft Windows XP
Microsoft Office (all versions)
Microsoft Project, Visio, Visual Studio, etc… (all versions)
Internet Explorer (all authorized versions)
Microsoft Silverlight
Microsoft .NET Framework (all versions)
Windows Media Player
Adobe Reader
Adobe Flash Player
Adobe Shockwave
Java Runtime Environment
Java SDK
LANDesk

Pre-Patch Management:
During the first week of each month the DET will research all new patches since the last deployment and apply them to the desktop test environment. The research will be to determine which patches are applicable within the City environment and the technical requirements for deployment. Download all applicable patch content. This will normally be done once per day by an automated task in LANDesk.

Start by verifying the most recent definitions have been downloaded in LANDesk. Patch content is scheduled for daily downloaded. The Desktop Engineering Team (DET) will analyze the definitions downloaded since the last patch cycle and identify which ones apply to the COM environment. Patch content will be downloaded for patches affecting the software listed.

All necessary RFCs for the patch process will be submitted on the first day of the first week of the month. Patch testing will follow the steps outlined in the Patch and Software Testing Standard Operating procedure. A full test run will be performed on all test environment machines.

After the testing process has been completed the patches will be deployed to the production environment via LANDesk.

Previously approved exceptions to the deployment of patches for specific software will be documented within the 'Master Exception' list. Exceptions will be made if the patch cannot be applied to all computers in the environment (e.g. Library workstations cannot have .NET Framework 4.5). The exceptions will adhere to the Patch Management Policy applies

Patch Management:
The tested patches will be pushed out to all desktop computers listed in LANDesk at the time of scheduling the tasks in the LANDesk system. Computers will be evenly divided across the five days of the work week. Each day will have four separate pushes scheduled for 9:00 AM, 11:00 AM, 1:00 PM, and 3:00 PM. Computers will be sorted by IP address before being assigned to a specific task. This process will occur during the second week of the month.

At the beginning of the third week, all tasks will be reset to a policy mode. This will allow computers that were not turned on during their scheduled task time to apply the patches during the next security check. Policy mode will be left in place for the last two weeks of the month. At the end of the Policy Phase, all tasks related to the patches will be deleted from the LANDesk environment.

After the initial deployment, patches will be moved into a policy group to be applied to all computers. Any deployed patch will also be added to the list of updates for the relevant images in the image update cycle, no less than quarterly.

The next step will be to set the 'Autofix' function within the LANDesk environment for City assets (not including servers) for all deployed patches. From this time forward any computer with the LANDesk agent correctly installed will attempt to pull down the listed patches and install them during the weekly security scan.

Back out Plan:
In the event that a patch must be removed and the patch can be removed, the DET will use the Vendor approved method of patch removal for the appropriate workstation, only after the Change Control Board has approved such a requirement. Once approved the details are documented within the RFC relative to the day it was patched, and documented in the 'Master Exception' list for patches that cannot be applied to a specific asset.

LANDesk Patch 'Success' Reporting:
The LANDesk Admin/Desktop Engineer will provide, no less than weekly, a sample (between 20 to 30 assets in a particular subnet) report of the various subnets for which the Workstations connect, in order to evaluate and provide quality assurance that the asset patch management process has lowered the overall risk from known patch vulnerabilities. This report will be provided to the CIO, DCIO, and ISO, weekly.

Incident Response Policy IS-100-16
Security Incident Report Form

(as it pertains to 'Sensitive' or 'Confidential' information)

Instructions: This form is to be completed by the employee and or the ISD service desk as soon as possible following the detection or reporting of an Information Technology (IT) security incident; as defined by the Incident Reponses Policy IS-100-16.
All items completed should be based on information that is currently available.

1. Contact Information for this Incident	
Name:	
Title:	
Service Center/Division	
Work Phone:	
Mobile Phone:	
Email address:	

2. Incident Description.

Provide a brief description:

3. Impact / Potential Impact Check all of the following that apply to this incident.

- ☐ Loss / Compromise of Data
- ☐ Financial Data Loss
- ☐ Other Organizations' Data Affected
- ☐ Damage to the Integrity or Delivery of Information
- ☐ Violation of legislation / regulation
- ☐ Unknown at this time

Provide a brief description:

4. Sensitivity of Data/Information Involved Check all of the following that apply to this incident.

Sensitivity of Data	
Category	**Example**
Confidential Data	Confidential Data: All data that is not approved for public release.
Sensitive Data (Privacy Violation/Data Breach)	Sensitive Information: Information which, if made available to unauthorized persons, may adversely affect the City of Memphis, its programs, or participants served by its programs. Examples include, but are not limited to, personal identifiers (Data Of Birth (DOB), social security numbers, credit card numbers, and financial information.

☐ Confidential Data	☐ Sensitive Data (Privacy violation)

Provide a brief description of data that was compromised:

5. Who Else Has Been Notified?

Provide Person and Title:

6. What Steps Have Been Taken So Far? Check all of the following that apply to this incident.

☐ No action taken	☐ Restored backup from tape
☐ System Disconnected from network	☐ Log files examined (saved & secured)
☐ Updated virus definitions & scanned system	☐ Other – please describe:

Provide a brief description:

7. Incident Details	
Date and Time the Incident was discovered:	
How the incident was established?	
Physical location of affected system(s):	
Number of sites affected by the incident:	
Approximate number of systems affected by the incident:	
Approximate number of users affected by the incident:	
Are business partners, affected by the incident? (Y or N – if Yes, please describe)	
Please provide any additional information that you feel is important but has not been provided elsewhere on this form.	

Please submit this completed form to:

Service.Desk@memphistn.gov

901-636-6100

Stolen/Loss Computer Equipment Report Form

DIVISION _____

PLEASE ANSWER THE FOLLOWING QUESTIONS IN DETAIL

1) What was the last known location of the missing equipment? _____

2) When was the missing equipment last seen? _____

3) Was the missing equipment vital to the operation of your Division/City? YES____ NO_____

4) When was the equipment last used? _____

_____

5) If equipment was not in use and not vital to the Division and or City, please explain why it had not been declared surplus: _____

_____

6) Please describe what steps have been taken to locate the missing equipment: _____

_____

7) Has a Police Report been filed? YES___ or NO___: Provide Police Report #:_____

8) Will the missing equipment need to be replaced? YES____ (go to #8) NO____ (go to #9)

9) What account number /City-Division Code will be used to pay for the replacement equipment? _____

10) Please describe steps that have been taken to prevent equipment loss from occurring in the future:

_____

_____

DESCRIPTION	MODEL#	SERIAL#	DATE MISSING

PLEASE OBTAIN THE FOLLOWING SIGNATURES UPON COMPLETION, PLEASE RETURN TO CITY ISD SERVICE DESK via EMAIL – Subject 'Stolen/Loss Computer Equipment Report Form'.

Division Director	Date	Deputy Director	Date	Immediate Supervisor	Date
_____		_____		_____	

City of Memphis
Information Services Division

Policy & Procedures Approval

IS-100-01 Encryption Policy
Last Updated: 02/08/2013

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. The City of Memphis will utilize encryption to protect confidential and personal identifiable information that pertains to individual citizens, employees and businesses.

IS-100-02 Acceptable Use Policy
Last Updated: 02/08/2013

Inappropriate use exposes the City of Memphis to risks including virus attacks, compromise of network systems and services, and legal issues. Information Services is committed to protecting the City's employees, partners, assets and the organization itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

IS-100-03 Bluetooth Security Policy
Last Updated: 02/08/2013

The purpose of this policy is to outline the requirements for secure Bluetooth operations.

IS-100-04 Backup and Restoration Policy
Last Updated: 02/08/2013

The purpose of this policy is as follows:

- To safeguard the information assets of the City of Memphis
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the media employed in the process.

IS-100-05 Audit Policy
Last Updated: 02/08/2013

The purpose of this policy is to set forth the City of Memphis policy regarding network security scanning offered by the City. Information Services-approved software will be utilized to perform electronic scans of networks and/or firewalls or on any system used by the City.

IS-100-06 Anti Virus Policy
Last Updated: 02/08/2013

The purpose of the Anti-Virus Policy is to establish the requirements for protection from malware infection, prevention, detection and cleanup. A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, CDs, or thumb/pin drives. A virus infection can be very costly to the City in terms of lost/corrupted data, lost staff productivity, lost reputation and citizen's confidence.

IS-100-07 Data Line Usage Policy
Last Updated: 02/08/2013

This policy explains the City of Memphis analog and data line acceptable use and approval policies and procedures. This policy covers two distinct uses of analog/data lines: (i) lines connected for the sole purpose of fax sending and receiving, and (ii) lines connected to computers.

IS-100-08 Computer & Mobile Device Disposal Policy
Last Updated: 02/08/2013

The purpose of this policy is to define the process and procedures for proper disposal of City• owned computers and mobile devices.

IS-100-09 Internet Use Monitoring and Filtering Policy
Last Updated: 02/08/2013

The purpose of this policy is to define standards for systems that monitor and limit web use from any host within the City's network. These standards are designed to ensure employees use the Internet in a safe and responsible manner, and ensure that employee web use can be monitored or researched during an incident.

IS-100-10 Internet DMZ Equipment Policy
Last Updated: 02/08/2013

The purpose of this policy is to define the requirements for all equipment owned and/or operated by the City of Memphis and located outside the City's Internet firewalls. Devices that are Internet facing and outside the City firewall are considered part of the "de-militarized zone" (DMZ) and subject to this policy. These devices (network and host) are particularly vulnerable to attack from the Internet.

IS-100-11 Information Sensitivity Policy
Last Updated: 02/08/2013

The Information Sensitivity Policy is intended to help employees outline the Sensitivity levels for the City of Memphis. The information covered in this policy includes: electronic information, information on paper, and information shared verbally or visually (such as telephone and video conferencing).

IS-100-12 Guest Access Policy
Last Updated: 02/08/2013

Typically, only City and/or contract employees have access to the City's network. There are specific circumstances that require others to be eligible for an account as a guest and therefore may be given access to a guest account.

IS-100-13 Email Use Policy
Last Updated: 02/08/2013

The purpose of this policy is to describe the acceptable use of email by City of Memphis employees, contractors, vendors, and agents operating on behalf of the City.

IS-100-14 DB Credentials Policy
Last Updated: 02/08/2013

This policy identifies the requirements for securely storing and retrieving database usernames and passwords *(i.e.,* database credentials). In order to maintain security of the City's internal databases, access will only be granted after authentication of user credentials.

IS-100-15 DMZ Lab Security Policy
Last Updated: 02/08/2013
This policy establishes information security requirements for all networks and equipment deployed in City of Memphis labs located on the "De-Militarized Zone" (DMZ). Adherence to these requirements will minimize the potential risk to the City from the damage to public image caused by unauthorized use of City resources, and the loss of sensitive/company confidential data and intellectual property.

IS-100-16 Incident Response Policy
Last Updated: 02/08/2013
The purpose of the Incident Response Policy is to establish the responsibilities for reporting and responding to security incidents.

IS-100-17 Confidential and Sensitive Data Transmission Policy
Last Updated: 02/08/2013
The Confidential and Sensitive Data Transmission Policy is intended to identify what information can be transmitted electronically.

IS-100-18 Extranet Use Policy
Last Updated:12/10/2015
This policy describes the policy under which third party organizations connect to the City of Memphis networks. Such third organizations may only connect to the network for the purpose of transacting business related to the City.

IS-100-19 PasswordPolicy
Last Updated: 12/10/2015
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords; and the frequency of change.

IS-100-20 Virtual PrivateNetwork Policy
Last Updated: 12/10/2015
The purpose of this policy is to protect the City's electronic information from being inadvertently compromised by authorized personnel utilizing an Internet.

IS-100-21 Personal Communication Device and Voicemail Policy
Last Updated: 02/08/2013
This policy describes Information Security Department's requirements for Personal Communication Devices and Voicemail for the City of Memphis.

IS-100-22 Removable Media Disposal Policy
Last Updated: 02/08/2013
The purpose of this policy is to define the process and procedures for proper disposal of City• owned removable media devices in order to ensure that confidential and/or sensitive information cannot be recovered by unauthorized individuals.

IS-100-23 Router Security Policy
Last Updated: 02/08/2013
This policy describes the required security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of the City of Memphis.

IS-100-24 Server Security Policy
Last Updated: 02/08/2013

The purpose of this policy is to establish requirements for the base configuration of internal server equipment that is owned and/or operated by the City of Memphis. Effective implementation of this policy will minimize unauthorized access to City proprietary information and technology.

IS-100-25 User Account Deletion Policy
Last Updated: 12/10/2015

The purpose of this policy is to describe the user account, network share and e-mail retention policy for City of Memphis employees, contractors, vendors, and agents operating on behalf of the City.

IS-100-26 Server Malware Protection Policy
Last Updated: 02/08/2013

The purpose of this policy is to outline which server systems are required to have anti-virus and/or anti-spyware applications.

IS-100-27 Removable Media Policy
Last Updated: 02/08/2013

To minimize the risk of loss or exposure of sensitive information maintained by the City of Memphis and to reduce the risk of acquiring malware infections on computers operated by the City.

IS-100-28 Risk Assessment Policy
Last Updated: 02/08/2013

To empower the Information Services Department to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

IS-100-29 Remote Access Policy
Last Updated: 12/10/2015

The purpose of this policy is to define requirements for connecting to the City of Memphis' network from any host. These requirements are designed to minimize the potential exposure to the City from damages which may result from unauthorized use of City resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical City internal systems, etc.

IS-100-30 Stolen Computer Equipment Policy
Last Updated: 12/10/2015

The purpose of this policy is to define the procedure to follow in the event of stolen and/or lost City-owned computer or mobile data device.

IS-100-31 Personal Computer Device Usage Policy
Last Updated: 12/10/2015

The purpose of this policy is to define the use of personally-owned devices within the city's network.

IS-100-32 Wireless Communication Policy
Last Updated: 02/08/2013

This purpose of this policy is to identify the requirements that wireless infrastructure devices must satisfy to connect to the City's network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Services Department are approved for connectivity to a City network.

IS-100-33 Physical Access Policy
Last Updated: 12/10/2015

The purpose of this policy is to establish standards for granting, monitoring, and terminating physical access to the City of Memphis network infrastructure and to protect equipment within the City of Memphis environment

IS-100-34 Geographic Information Data Dissemination Policy
Last Updated: 02/08/2013

The Geographic Information Systems (GIS) Policy is intended to outline the rules and procedures for the dissemination of GIS created and/or managed by the City of Memphis. The information covered in this policy includes, but is not limited to, the GIS spatial data and intellectual property relating to or derived from GIS data that is owned and managed by the City of Memphis.

IS-100-35 Incident Response Policy
Last Updated: 12/10/2015

The purpose of the Incident Response Policy is to establish the responsibilities for reporting and responding to security incidents.

IS-100-36 Mobile Device Monitoring Policy
Last Updated: 12/10/2015

The purpose of the Mobile Device Monitoring Policy is to establish the monitoring tool within the city's mobile devices provided to city employees.

IS-100-37 PCI Compliance Policy
Last Updated: 12/10/2015

The purpose of the PCI Compliance Policy is to establish a standard to protect cardholder data that is processed, or transmitted by the City of Memphis to credit card merchants..

IS-100-38 Patch Management Policy
Last Updated: 12/10/2015

The purpose of this document is to outline the ISD's requirements for maintaining security and application patches and on all City of Memphis Information Services Division (ISD) owned and managed workstations and servers.

IS-100-39 Electronic Data Retention Policy
Last Updated: 12/10/2015

The purpose of this policy is to describe the electronic data retention of email, voicemail, and instant messages used by City of Memphis (CoM) employees, contractors, vendors, and agents operating on behalf of the City within the CoM network environment.

Brent Nair, Chief
City of Memphis