Procedure Guideline

Index No: 8040
Date: 3/28/19
Revised: 1/17/20
Revised: 10/1/20

NETWORK SECURITY

I. PURPOSE:

The following guideline establishes guidelines which will assist in protecting City assets and safeguard against cyber, physical and environmental threat while ensuring the confidentiality, integrity and availability of information and data needed by all employees to support our mission. The protection of all data and information shall be in accordance with the City's policies, rules and regulations, best practices, accreditation standards (Little Rock Police, Little Rock Fire, Little Rock Zoo and Parks & Recreation Departments), financial audit requirements, and local, State and Federal Laws, to include the Criminal Justice Information Services Guidelines.

II. PROCEDURE:

A. Anti-Virus: A software utilized to scan the system and remove viruses.
B. App: The term is short for "application" which is the same as a software program, typically downloaded onto a device.
C. ATF: Bureau of Alcohol, Tobacco, Firearms and Explosives.
D. Availability: Data must be available to those who are authorized to use it. Denial-of-Service Attacks are becoming common, and the goal is to ensure that users can access the data they need in a secure and timely manner.
E. Breach: A breach is the actual or suspected compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, and/or any similar occurrence where:
    1. A person other than an authorized user accesses or potentially accesses PII; or,
    2. An authorized user accesses or potentially accesses PII for other than an authorized purpose.
F. CJIS: Criminal Justice Information Services.
G. Confidentiality: Ensuring that only authorized users can access confidential or sensitive information. By precisely defining groups of users, logging all access and regularly auditing the accuracy and consistency of those groups, limits and controls can be placed on who has access to which data. Through a variety of policies, practices and

systems, staff works to ensure that only those who are authorized will access any given data resource.

H. Departmental Admin: Employee designated by the Department Director to enter HelpDesk Tickets.
I. DOJ: Department of Justice.
J. Employee: Any individual employed by the City of Little Rock, affiliated agencies or Departments in any capacity, whether full or part-time, active or inactive, including interns, contractors, consultants and vendors.
K. Encryption: The translation of data into a secret code to achieve security.
L. Firewall: A Network Security System designed to prevent unauthorized access to or from a private network; firewalls can be implemented in both hardware and software, or a combination of both.
M. Hacker: A skilled or unskilled individual who gains unauthorized access into a secure system.
N. Hardware: The physical components of the computer such as the machine, wiring, monitor, keyboard, etc.
O. Hub/Switch: Basic networking device that connects multiple computers or other network devices together.
P. Integrity: Ensuring that data has not been tampered with, either on the network or in storage. The goal is to ensure that data integrity is maintained at all levels with added safeguards.
Q. Availability: Data must be available to those who are authorized to use it. Denial-of-Service Attacks are becoming common, and the goal is to ensure that users can access the data they need in a secure and timely manner.
R. LRIT: Little Rock Information Technology.
S. NIBIN: National Integrated Ballistic Information Network.
T. Personally Identifiable Information (PII): PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. 2 C.F.R. § 200.79. Public PII is information that is considered to be PII and is available in public sources such as telephone books, public web sites, and university listings. *Id.* Public PII includes, but is not limited to, first and last name, address, work telephone number, work e-mail address, home telephone number, photos, and videos. Non-public PII includes, but is not limited to, social security number, usernames and passwords, passport number, credit card numbers, banking information, date and place of birth, medical and financial records, and educational transcripts. This Policy addresses breaches or imminent breaches of non-public PII.
U. Server: A centralized component to which other computers in a network are connected, allowing all computers in the network to share applications and communicate with each other.
V. Software: Programs or applications that direct a computer's processor to perform specific operations.

W. Wireless Access Point (WAP): A network hardware device that allows a Wi-Fi device to connect to a wired network.

X. Wi-Fi: Wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connection.

III. PRIVACY:

A. All electronic data, communications and information, including information transmitted or stored on the electronic systems of the City, remain the property of the City. The City retains the right to access, inspect, monitor or disclose any material transmitted or received on its electronic systems, including information downloaded from the Internet, or received or sent via e-mail.

B. Employees shall have no expectation of privacy in regard to electronic or physical records including email, personal files or official work documents, either received or generated by them, while using Department-owned information technology equipment, or while connected to the City network. The City reserves the right to access, without prior notice, any information from any technology resources and may require employees to provide passwords to files that are encrypted or password protected, upon request. The request will be made by the employee's Department Director or his/her designee. The Information Technology Director and the City Manager shall be notified in writing of the request, prior to accessing any device. Any access shall be documented and forwarded to both the City Manager and the Information Technology Director.

IV. ACCESS TO DATA CENTER, SOFTWARE AND DATA CLOSETS:

A. The City of Little Rock has three (3) Data Centers, and access to these centers shall be limited to authorized personnel only and individuals with a valid reason for entry. Entry to these facilities will be gained through use of an Electronic Access Card System. Anyone not a member of the Information Technology Staff will be required to sign in and out of the facility. Visitors shall be accompanied at all times by a member of the Information Technology Staff while on the premises, and all areas will be monitored by security cameras.

B. In accordance with the Criminal Justice Information Services (CJIS), all vendors, contractors, service providers who have access to the City of Little Rock Network shall have passed a background investigation and successfully completed the CJIS Vendor Course. This requirement applies to the actual employee of the vendor, contractor or service provider who is physically accessing the system. Those who have not successful completed a background check will be accompanied at all times, no exceptions.

C. In accordance with ATF standards for the NIBIN System, all NIBIN System users, whether City employees or otherwise, shall complete ATF approved

training. The City may provide access to the NIBIN System to other law enforcement agencies.

D. Data Closets shall be secure at all times and access limited to only Information Technology Department Staff or individuals authorized by the Information Technology Director or their designee. Access will be determined on a case-by-case basis.

V. EQUIPMENT CONNECTED TO THE CITY'S NETWORK:

A. The Information Technology Department will assist other Departments in identifying specialized software to facilitate new programs, enhance current programs or increase efficiency of daily operations.

B. The Information Technology Department shall be included in computer network planning, design and will assist with the preparation of bid specifications involving technology hardware and software that will be connected to the City's Network.

C. Under no circumstances shall any desktop, laptop, mobile device, printer, camera system, digital video recorder, switch, server, firewall, hub, modem, wireless access point, IP-connected external hard drive or other device be attached to the network by anyone other than the Information Technology Department's Staff without written authorization. The authorization will be retained in a file on the Information Technology Fileshare.

D. No personal devices (laptops, mobile devices, etc.) will be connected to the City of Little Rock's network.

E. No City-issued device will be used as a hotspot.

F. Configuration of servers, firewalls, switches or other networking devices will only be conducted by authorized City of Little Rock Information Technology Department Staff.

VI. NEW ACCOUNT, EMPLOYEE ACCESS, & HELPDESK TICKETS:

A. Written permission in the form of a HelpDesk Ticket must be submitted from an authorized Department Administrator, in order to add new network accounts and/or devices, grant network file rights, search archived e-mail, or install new application software. A list of all Authorized Administrators by Department is available on the City of Little Rock Intranet Site in the Helpful Documents, Approval List.

B. Whenever a new account is required to allow an employee access to the network, the Department Director, or their designated Administrator, will submit a HelpDesk Ticket requesting the creation of an employee profile. The HelpDesk Ticket will include all folders that the employee will need to access. The employee will be assigned a generic password until the employee accesses the account for the first time. Once the employee initially logs-in, they will be required to change their password.

C. If the access level changes due to transfer, disciplinary action or the employee separates employment with the City, the Administrator will be responsible for creating a HelpDesk Ticket indicating any changes required or suspending the employee's account.
D. HelpDesk Tickets completed for employment changes requiring the disabling of an account should be logged, no later than the next business day after the change occurs. The ticket should be logged as a Priority #1 on the HelpDesk screen.
E. The Information Technology Director or the Network Security Manager should be notified of any employment action requiring the immediate disabling of a network account.

VII. PASSWORD:

A. Passwords must be complex with a minimum of eight (8) characters in length and containing at least three (3) of the four (4) categories: uppercase letters; lowercase letters; numerical characters; or non-alphanumeric characters.
B. Personnel will change their system password every thirty (30) days, as prompted, when logging into the network, and the same password will not be used more than once during a twelve (12)-month period.
C. A user account is locked after five (5) unsuccessful attempts to log into an account. Once an account is locked, the user may contact the HelpDesk for assistance in unlocking the account or wait sixty (60) minutes for the account to re-activate, allowing the user to enter their password again. Anytime a user account is locked, a notification will be sent to the HelpDesk. The user must provide proper identification or have a Department Director or their designee contact the HelpDesk to verify the user identification.
D. It shall be the assigned employee's responsibility to ensure the security of their computer against unauthorized use. Employees are required to keep their passwords confidential and are prohibited from allowing another individual to use their USER ID or password to gain access to any City resources, such as, Virtual Private Network (VPN), the City's e-mail, Infor or any other secure system utilized.
E. Employees are responsible for all activities that transpire under their USER ID.
F. To prevent breeches in security, employees shall abide by the following measures:
    1. Log off or lock your computer before leaving your workstation unattended.
    2. All employees are required to log-off their workstation, prior to leaving work for the day.
        a) Never shutdown your computer at the end of the day, unless instructed to do so by the Information Technology Department.

b) Patches and updates are conducted during non-business hours and can only be applied when the computer is on.

3. Secure your computer in a manner that will deter theft, such as a locked office or desk.
4. Secure your passwords, ensuring that they are not visible to others.

G. In accordance with CJIS requirements, a City computer that is inactive for a period of fifteen (15) minutes, will be automatically logged-off and the employee will be required to log-in, once they return and access the computer.

VIII. REMOTE ACCESS:

A. There are many instances when authorized individuals require remote access to the City's information technology resources. Examples of remote access include, but are not limited to, employees checking e-mail while traveling, submitting reports or updating databases while out of the office and contractors or service providers accessing the network to troubleshoot problem or update systems. Access to the City's network shall be monitored and regulated to minimize the risk of compromise.

B. City-owned laptops shall be encrypted and will have the latest version of anti-virus software.

C. Secure remote access must be strictly controlled. Control will be via password authentication.

D. Any device accessing the City's Internal Network via remote access technology must be up-to-date on all patches, updates and anti-virus software.

E. In the event that the City's equipment becomes infected with a virus, and the infection is traced to a personally-owned computer system, or data storage device, the individual transferring the virus to the system may be held liable for the cost of removing the virus from the equipment.

IX. NETWORK COMPONENT PASSWORDS – CONTINGENCY ACCESS:

A. Network operations related passwords (servers, Apps, switches, firewalls and other equipment) are to be stored in a secure and password protected management application.

B. In the event that the appropriate Information Technology ddministrator is not available in an emergency, access to the password management file can be obtained by one of the following:
   1. Information Technology Director.
   2. Network Security Manager.
   3. Operations Manager.
   4. Applications Development Manager.
   5. HelpDesk Supervisor.

C. Network operations related passwords must be changed:
   1. At least once every 180 days.

2. In the event that a password or system becomes compromised, all infrastructure passwords are to be changed, as soon as possible.

X. REPORTING SUSPICIOUS ACTIVITY AND ANNUAL TRAINING:

A. All employees will be required to complete training on information security awareness.
B. All employees will practice security awareness and remain vigilant against fraudulent activities.
C. Any employees aware of an information security incident, a breach of information, a suspicious activity involving the City's Network, an actual or imminent breach of PII, or a compromise of computer or Network Security Guidelines will immediately notify their direct Supervisors and the Information Technology Director or his/her designee.
D. When it has been suspected that an actual or imminent breach of PII has occurred, it shall be reported to the LRIT. In the event LRIT determines that an actual or imminent breach of PII has occurred, when applicable, it shall report the occurrence to the City's Grant Manager as soon as possible, but no later than twenty-two (22) hours after the determination. This shall be accomplished by the LRIT contacting the City's Grant Manager who will directly contact the appropriate DOJ Office of Justice Programs Manager. This will ensure compliance with the DOJ's reporting requirements.
E. An information security incident is generally defined as any known or highly suspected circumstance that results in an actual or possible unauthorized release of information deemed sensitive by the City of Little Rock, subject to CJIS regulations, or subject to ATF regulations.
F. Examples of an information security incident may include but are not limited to:
    1. Theft or physical loss of computer equipment (laptops, mobile devices, flash drives, hard drives, etc.) known to hold sensitive data, CJIS information, or NIBIN information.
    2. A server known to hold sensitive data is accessed or otherwise compromised by an unauthorized party.
    3. A firewall is accessed by an unauthorized entity.
    4. A network outage is attributed to the activities of an unauthorized entity.
    5. An outside entity is subjected to a Distributed Denial of Service attack originating from within the City's network.
G. The Information Technology Department will work with the specific Department to:
    1. Assess the seriousness of the incident.
    2. Assess the extent of damage.
    3. Identify the vulnerability created.
    4. Estimate what additional resources are required to mitigate the incident.

H. When warranted, members of the City's Internal Audit Team and the Little Rock Police Department will be notified.
I. Additional resources may be obtained from the Department of Homeland Security, InfraGardm the Multi-State Information Sharing and Analysis Center and the ATF.
J. Users will note and report observed or suspected security weaknesses to systems and services directly to their immediate supervisors and the Information Technology Department.
K. If the incident involves a CJIS violation, the Information Technology Department will work with the Little Rock Police Department and the Arkansas Crime Information Center (ACIC) to mitigate the issue, as soon as possible.
L. The Information Technology Department will work with Police personnel to ensure that the "IT Security Incident Response Form" is completed and submitted to the ACIC. A copy of the form will be retain by the Information Technology Department.
M. If the incident involves a breach of PII or an imminent breach of PII related to the NIBIN System, the City shall report the actual or imminent breach of PII to an Office of Justice Programs Manager no later than twenty-four (24) hours after such an occurrence.
N. The City shall ensure that actual or imminent breaches of PII on systems owned or operated by the City, including those owned or operated by City contractors or grantees on behalf of the City, are identified, tracked, and responded to in an effective, consistent, and timely manner.

XI. DISPOSAL OF MEDIA AND CONFIDENTIAL DOCUMENTS:

A. Disposal of confidential information will be conducted in a manner that protects sensitive and classified information. Inappropriate handling and disposal of sensitive and classified document can causes a risk to State, Local, Federal organizations, their employees and the individual or entity it pertains to.
B. This section applies to all equipment that processes, stores, or transmits Federal Bureau of Investigation Criminal Justice Information (FBI CJI) and/or classified and sensitive data that is owned or leased by the City of Little Rock.
C. When hard drives, diskettes, tape cartridges, CDs, hard copies, print-outs and other similar items used to process, store or transmit, FBI CJI or City classified and sensitive data are no longer needed and ready to be destroyed, they shall be disposed of in accordance with this directive.
D. Physical media (print-outs, confidential paper documents) shall be disposed of by one of the following methods:
    1. Shredded using an on-site, City-issued/owned shredder.
    2. Placed in a locked shredding bin owned by an approved contract vendor. The contract requires the vendor to shred all documents

on-site. City personnel will witness the shredding of all sensitive and confidential information.

E. Electronic media (hard drives, tape cartridges, CDs, flash drives, printer and copier hard drives, etc. shall be disposed of by one of the following methods:
   1. Placed in a locked shredding bin owned by an approved contract vendor: The contract requires the vendor to shred all documents on-site. City personnel will witness the shredding of all sensitive and confidential information.
   2. Physical Destruction: Physically dismantled by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.
   3. Overwriting: an effective method of clearing data from magnetic media. Overwriting uses a program to write (1s, 0s, or a combination of both) on to the location of the media where the file to be sanitized is located.

F. Information Technology Systems that have been used to process, store or transmit FBI CJI, NIBIN information, and/or sensitive and classified information shall not be released from any Department of the City of Little Rock's control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.
   1. Employees shall contact the Information Technology Department for assistance when they are unable to comply with this directive.

XII. VIOLATION OF DIRECTIVE:

A. Employees suspected of violating any section of this directive will have their access immediately suspended until an investigation can be completed and the outcome determined.

B. Any employee who is determined to be in violation of any section of this directive may be subject to disciplinary action, up to and including termination.

XIII. E-MAIL USAGE AND RETENTION:

A. The following procedures recognize the importance of the City's Electronic Communication System (e-mail) while establishing the proper use, storage and maintenance of information communicated in this manner. The e-mail system will be utilized as a method of communication, not a primary storage system. If there is a need to retain the information in an e-mail, the information shall be transferred to a storage system.

B. This Policy applies to all City employees, volunteers, full-time, part-time, etc., who have access to a City device or who has a City of Little Rock e-mail account.

C. Definitions:

1. E-Mail System: Network of computers handling electronic mail (e-mail) on the Internet and City's network. This system includes user machines running programs that compose, send, retrieve, and view messages. User devices accessing e-mail are all part of the Mail Handling System.
2. E-Mail: The transmission of messages over communication networks. Messages distributed, sent or received by electronic means from one computer by a user to one or more recipients via a network.
3. Primary Storage System: The software application and equipment that houses the data in a location specific to the information contained in the e-mail. For example, an e-mail concerning a 311 Request, if retention is necessary must be transferred/entered into the database of the 311 System.
4. Confidential: Ensuring that only authorized users can access confidential or sensitive information. By precisely defining groups of users, logging all access and regularly auditing the accuracy and consistency of those groups, limits and controls can be placed on who has access to which data. Through a variety of policies, practices and systems, staff works to ensure that only those who are authorized will access any given data resource.
5. Personal Storage Table (PST): An open proprietary file format used to store copies of e-mails, calendar events, contacts notes and other items. PST is not a primary storage location.
6. Mailbox: The destination to which electronic mail messages are delivered. Electronic mail messages can be moved to folders connected to the mailbox, including, but not limited to: inbox; trash; junk; deleted; sent; or other user created personal folders.
7. Inbox: An electronic folder in which e-mails received by an individual are held for pending action.
8. Sent Folder: An area that stores and e-mail that has been sent from the user mailbox. Items in this folder must be manually deleted or automated with 'Do Not Save'.
9. Delete Folder: Folder that holds all deleted items that have not been purged. Items in this folder must be manually deleted or automated to delete.
10. Transitory E-Mail: The e-mail has little value after its review and no information requiring retention. Unsolicited advertising, marketing, spam, unwanted mail that is of no value to the operation the end user is supporting.
11. Essential Mail: Notifications or mail that documents the administrative, financial, legal or archival needs of the City; those include, but are not limited to: legal documents; procurement documentation; grant documents; projects; employee time and attendance; software licenses; and architecture plans.

D. Procedure:
   1. E-mail should be retained only as long as it takes to transfer the data to the primary system of storage for that data. This should be accomplished within thirty (30) days unless the business and/or legal function requires additional time.
   2. Employees shall at all times exercise caution when opening or forwarding e-mails to limit exposure to phishing attempts and viruses. If an e-mail appears suspicious, the user shall forward the e-mail to SpamReport, without opening any attachment or clicking on any links.
   3. E-mails determined to be transitory, shall be purged from the users mailbox and all deleted folders immediately.
   4. If it is essential to retain any data contained in an e-mail, the information should be reviewed and forwarded to the appropriate Department for transfer into the Primary Storage System.
   5. Users are prohibited from sending a City of Little Rock e-mail containing confidential or protected data (PII, HIPPA, CJIS) to a third-party e-mail system, without the data being encrypted. Individual messages forwarded outside the City's network must not contain non-encrypted, confidential or protected data.
   6. E-mails shall not be set-up in a manner that allows automatic forwarding to third-party e-mail addresses.
   7. Users must adhere to the Administrative Policy and Procedures, Section 5, Electronic Communications Equipment Resources and Systems and the City of Little Rock Network Security Policy.
   8. Any variance from this Policy shall require written approval from the City Manager or his designee.

E. Violations:
   1. Any employee who is determined to be in violation of any section of this directive may be subject to disciplinary action.
   2. Documents that are subject to litigation holds, Freedom of Information Act requests, or are subject to Court Order are excluded from this Subsection.

Approved:

Bruce T. Moore
City Manager