CITY OF TONTITOWN, AR

PHYSICAL ACCESS SECURITY POLICY

Purpose

The purpose of this policy is to establish the rules for the granting, controlling, monitoring and removal of physical access to City facilities that house network infrastructure equipment and data storage.

Policy

1. All network infrastructure equipment and data storage must be physically protected based on risk identified by the equipment or data owner and the Mayor/Recorder/IT Director.

2. Physical access safeguards help to establish best practices for the appropriate granting, controlling, and monitoring of physical access for all facilities supporting network infrastructure equipment and data storage. Physical access safeguards include the following:

   2.1 All facilities supporting network infrastructure equipment and data storage must be physically protected in proportion to the criticality and confidentiality of their function.

   2.2 All facilities supporting network infrastructure equipment and data storage must have physical access controls in proportion to the importance, sensitivity, and accountability requirements of the data and systems housed in that facility.

   2.3 Access to facilities supporting network infrastructure equipment and data storage will only be granted to authorized personnel of the City and other contractors or personnel whose job responsibilities require such action.

   2.4 Access cards and/or keys must not be shared with others.

   2.5 Access cards and/or keys and badges that are no longer required must be returned to the responsible department contact. All returned access cards must be forwarded to the Mayor/Recorder/IT Director as soon as possible. Cards must not be reallocated to another individual, thereby bypassing the return process.

   2.6 Lost or stolen access cards and/or keys will have access removed and must be reported to the Mayor/Recorder/IT Director as soon as possible.

   2.7 Access and log records for facilities supporting network infrastructure equipment and data storage are the responsibility of the department that manages the facility.

   2.8 The department in charge of facilities supporting network infrastructure equipment and data storage must be notified within 1 business day if individuals who had access to these facilities should no longer need access due to a change in roles, completion of contract, or other cause that negates their need for further access.

   2.9 Visitors must be escorted in controlled areas of facilities supporting network infrastructure equipment and data storage.

2.10 The department in charge of facilities supporting network infrastructure equipment and data storage must review access records on a periodic basis and investigate any unusual access.

2.11 Signage for restricted access rooms and locations must be practical. Minimal discernible evidence of the importance of the location should be displayed.

2.12 All physical security systems must comply with applicable regulations, including but not limited to, building codes and fire prevention codes.

2.13 Physical access to all network infrastructure equipment and data storage restricted facilities must be documented and managed.

2.14 All network infrastructure equipment and data storage facilities must be physically protected in proportion to the criticality or importance of their function at the City.

2.15 The process for granting card and/or key access to network infrastructure equipment and data storage facilities must include the approval of the person responsible for the facility.

2.16 Requests for access must come from the applicable City data/system owner.

2.17 Cards and/or keys must not have identifying information other than a return mail address.

2.18 All network infrastructure equipment and data storage facilities that allow access to visitors will track visitor access with a sign in/out log.

2.19 Card access records and visitor logs for network infrastructure equipment and data storage facilities must be kept for routine review based upon the criticality of the Information Resources being protected.

2.20 The person responsible for the network infrastructure equipment and data storage facility must remove the card and/or key access rights of individuals who change roles within the City or are separated from their relationship with the City.

Policy Compliance

1. Compliance Measurement – The City will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the Mayor/Recorder/IT Director.
2. Exceptions – Any exception to the policy must be approved in advance by the Mayor/Recorder/IT Director.
3. Non-Compliance – An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

CITY OF TONTITOWN, AR

REMOTE ACCESS POLICY

Purpose

The purpose of this policy is to define requirements for connecting to the City's network (or any network managed by the City) from an outside entity. 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 information, damage to public image and damage to critical City internal systems.

Scope

The policy applies to all City employees, contractors, vendors and agents with a City-owned or personally-owned computer used to connect to the City network. This policy applies to remote access connections used to perform work on behalf of the City including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to City networks.

Policy

1. General
    1. Storage of confidential information on any non-City-owned device is prohibited. Confidential information may not be stored on any City-owned portable device without prior written approval from the Mayor/Recorder/IT Director. Approved storage on any portable device must be encrypted.
    2. It is the responsibility of City employees and contractors with remote access privileges to the City's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the City network.
    3. All remote access users are expected comply with City policies, may not perform illegal activities, and may not use the access for outside business interests.

2. Requirements
    1. Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs) or other approved SSL connections) and strong pass-phrases.
    2. Authorized users shall protect their login and password, even from family members.
    3. While using a City-owned computer to remotely connect to the City's network, authorized users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an authorized user or third party.
    4. Use of external resources to conduct City business must be approved in advance by the Mayor/Recorder/IT Director.
    5. All hosts that are connected to the City's internal networks via remote access technologies must use the most up-to-date anti-virus software and be current on all security patches. This includes personal computers.
    6. Personal equipment used to connect to the City's networks must meet the requirements of City-owned equipment for remote access.

Policy Compliance

1. Compliance Measurement – The City will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the Mayor/Recorder/IT Director.
2. Exceptions – Any exception to the policy must be approved in advance by the Mayor/Recorder/IT Director.
3. Non-Compliance – An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Acknowledgement of REMOTE ACCESS POLICY

Each employee with computer and network privileges is required to sign an acknowledgement in the form below and such acknowledgement will be placed in their personnel file. Failure to sign such acknowledgement does not excuse violations of the foregoing policies.

Employee Signature
I have received and read the above policy and have had the opportunity to ask any questions.
I understand that my failure to follow this policy may result in disciplinary action including revocation of system privileges or termination.

_____ _____
Employee Signature Date

_____
Print Name

City of TONTITOWN, AR

TECHNOLOGY, INTERNET ACCESS, ELECTRONIC MAIL, COMPUTER/NETWORK ACCEPTABLE USAGE POLICY

INTERNET POLICY

Purpose

The purpose of this policy is to define allowable and appropriate uses of the City's internet.

Internet Access

Internet access can be made available to any City user on the City's network. Department heads shall be the authorizing agent in determining whether an employee shall have Internet access and the level of access.

Internet Use

All City employees are responsible for using computer resources in an ethical, responsible and legal manner. Use of the Internet through City equipment, including e-mail accounts accessed on the Internet, is only for City employees, and primarily for purposes related to City business. Personal use should be kept to a minimum and must not interfere with work responsibilities.

Department Heads are responsible for managing use of the Internet by their staff, restricting use or limiting time as they see appropriate.

Users should consider their Internet activity as public information and manage their activity accordingly. All Internet traffic travels beyond the City's protected network into the World Wide Web. Such information is not secure.

The City's Information Systems maintains a log of the Internet activity on the City network. This information is available to the Department Heads as deemed necessary.

Viewing and downloading offensive material from the Internet is prohibited and may result in disciplinary action, including termination. The City's E-mail/Internet systems should not be used to create or disseminate any discriminatory, defamatory, offensive, disruptive, or otherwise inappropriate or unprofessional communications. Among those considered inappropriate or unprofessional are any communications concerning sex, that contain sexual implications, racial slurs, gender-specific comments, or any other comment that inappropriately or unprofessionally address someone's age, race, religious beliefs, national origin, or disability. Viewing streaming audio or video of a personal nature is prohibited.

The City's E-Mail/Internet systems should not be used to access any discriminatory, defamatory, offensive, disruptive or otherwise inappropriate or unprofessional web sites (e.g. pornographic sites, hate speech, criminal skills, illegal drugs, etc.) All copyrighted information and software found on the Internet must be respected to avoid violations of the law.

When using the Internet through City resources, employees are representing the City. Thus all communications across the Internet shall be professional. Employees also must be sensitive to the different backgrounds, cultures and countries of the people that you may communicate with while on the Internet.

All E-mail/Internet records are considered records of the City and are subject to inspection and disclosure under the Freedom of Information Act (FOIA) or court subpoena.

Employees are prohibited from performing any act that is illegal or otherwise in violation of any applicable federal, state, or local laws. Encryption shall be used to transmit confidential information over the Internet.

ELECTRONIC MAIL (E-Mail) POLICY

Purpose

The purpose of this policy is to assure proper use of electronic mail by the employees of the City.

Electronic Mail (email)

The City's electronic mail system is to be used for City business and, as such, department heads may authorize inspection of messages at any time. Every email user will have a user name unique in the e-mail system. All employees must check their mailbox on a regular basis.

Using your City e-mail address to establish personal online accounts or electronic subscriptions is strictly prohibited.

Personal Use

The City allows access to personal e-mail accounts, by way of the Internet, as well as personal Internet usage in much the same manner as it allows for personal phone calls. Personal usage of all electronic devices and access to the Internet should be kept to a minimum.

Procedure

Junk Mail. The email system will not be used as a method of communicating non-essential information to City staff. Do not forward junk mail (such as chain letters) through the email system wasting City resources and staff time.

Business and City Email is not private. No employee shall have any expectation of privacy in email. System administrators have the capability to read any messages if requested by a Department Head.
Encryption shall be used to transmit confidential information.

Instant Messaging (IM)

The City provides staff with resources or tools to communicate by Instant Messaging when conducting City business. Without regard to the abbreviated nature of IM, users should be aware that they may be creating records that are public using this application.

COMPUTER AND NETWORK POLICY

Purpose

The purpose of this policy is to assure proper use of the City Computers and Network.

The City maintains a local area network allowing various office communications and communications to the Internet. In order to protect our communication networks from virus infiltration and to ensure reliability and integrity of our systems, it has become necessary that we establish and enforce a set of policies.

All computers, software, related hardware and electronic data are the property of the City. To protect your privacy, personal information should be removed. Incidental and occasional personal use of the City's computers is permitted; however, personal use is prohibited if it:

i) interferes with the user's productivity or work performance, or with any other employee's productivity or work performance;

ii) adversely affects the efficient operations of the computer system.

Games are for home usage and should not be installed on any City owned PC.

To reduce the number of malware infections, online games are strictly prohibited.

Server data is backed up daily and backups are stored offsite in a secured area. It is important that you save all critical data to an appropriate server directory on the network. If you save data on your local machine (i.e.; C: drive) you will be responsible for the loss of this data. The information and technology department will not be responsible for the recovery of this data if lost. If you are unsure of how to save data or need help in setting up backup procedures, please contact the information technology department.

Peripheral tools or personal storage devices shall not be attached to City computers. If you have a need for an external storage device, a secure device will be issued to you. Prior to loading any data from an outside source (floppy disk, USB drive, CD, DVD, Internet), you should check it using virus protection software. A Virus could not only infect the City owned PC, it can and will infect the entire network.

A unique login and password will allow you access to the City network. Do not share your password with anyone. File access is controlled by this login and everything you do will be audited and logged under your login ID. For your protection, you should never share your password. If you need help changing it, please contact the information technology department.

Security measures are now in place to help protect your data. Limited password retries, limited password life, and system auditing have been implemented. Audit logs will be reviewed on a regular basis to prevent unauthorized access to our network. Outside attacks to our network are always a possibility. If you forget your password or have difficultly accessing the network, please contact the information technology department.

If a laptop or mobile device is lost or stolen, it shall be reported immediately to your supervisor and the information technology manager.

Certain staff may be given the ability to access the City's computer systems from remote locations or from home, using City owned equipment. Employees with remote access privileges will be given specific instructions on how to protect City equipment and information sources.

Every software package must have a software license. Any software running on your machine that does not have a license is illegal and will be removed; this is not an option. Routine PC audits will be conducted without notice. If you have a need for a new software package, your department head will submit the request

to the information technology manager for approval and purchase. ALL SOFTWARE MUST BE APPROVED FOR USE.

Employees shall be liable for any damage caused to City equipment as a result of personal use. Employees are prohibited from removing City data and work related information from the City work site without prior authorization. The use of non-City computers to process or store City data and work related information is prohibited. City data and work related information stored on mobile devices shall be encrypted.

Freedom of Information Act
The electronic files, including electronic mail files, of public employees are potentially subject to public inspection and copying under the Freedom of Information Act ("FOIA"). The City is considered a public entity and its employees are considered public employees that are subject to the FOIA.

The FOIA defines "public records" to include "data compilations in any form, required by law to be kept or otherwise kept,...which constitute a record of the performance or lack of performance of official functions which are or should be carried out by a public official or employee [or] a governmental agency…". All records maintained in public offices or by public employees within the scope of their employment are presumed to be public records.

Government Rules and Regulations
The City's operations are quite varied and as a result a myriad of laws and regulations are applicable, in whole or in part, to the City and its employees and officers. It is the express intent of the City to comply with all Federal, State and local laws and regulations. The City routinely reviews its operations to ensure such compliance. These policies and guidelines will be observed and applied in a manner consistent with such laws and regulations.

No Expectation of Privacy
The City reserves the right to monitor or disclose any electronic communication sent, received, or stored using its electronic communications facilities. Any and all software, data, or other information stored on or accessed by the City's computer system may be monitored, read, examined, seized, or confiscated as necessary. Monitoring, investigation, and examination of electronic content can be conducted at any time. The City reserves the right to monitor any use of its electronic communications systems, including use of these systems while the employee is on his/her own time, to access any information on these systems, and to take any action it determines to be appropriate with respect to that information. Employees should understand that e-mail messages and Internet transactions, including those they delete or erase from their own files, may be backed up or recorded and stored centrally for system security and investigative purposes and may be available to the public under the Freedom of Information Act. E-mails and records of Internet activities may be retrieved and viewed by anyone with proper authority at a later date. It is the user's responsibility to use care in communicating information not meant for public viewing. Use of the City's electronic communication facilities shall be deemed to constitute consent to allow monitoring of all communications and agreement to abide by all applicable policies.

Enforcement
As a City employee you are required to adhere to these policies. If you do not follow these policies, disciplinary action may be taken, including termination.

Acknowledgement of TECHNOLOGY, INTERNET ACCESS, ELECTRONIC MAIL, COMPUTER/NETWORK ACCEPTABLE USAGE POLICY

Each employee with computer and network privileges is required to sign an acknowledgement in the form below and such acknowledgement will be placed in their personnel file. Failure to sign such acknowledgement does not excuse violations of the foregoing policies.

Employee Signature
I have received and read the above policy and have had the opportunity to ask any questions.
I understand that my failure to follow this policy may result in disciplinary action including revocation of system privileges or termination.

_____ _____
Employee Signature Date

_____
Print Name

CITY OF TONTITOWN, AR

WIRELESS NETWORK POLICY

Purpose

The purpose of this policy is to secure and protect the information assets owned by the City. 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 policy specifies the minimum security requirements for City wireless networks, as well as the conditions that wireless infrastructure devices must satisfy to connect to the City network. Only those wireless networks and wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Mayor/Recorder/IT Director are approved for connectivity to the 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 policy. This policy 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 tablets. This includes any form of wireless communication device capable of transmitting packet data.

Policy

1. General Requirements
All wireless infrastructure devices that provide direct access to a City network, must adhere to the following:

- Be installed, supported, and maintained by an approved support team.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other departments.
- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS)
- When enabling WPA-PSK, configure a complex shared secret key (at least 12 characters) on the wireless client and the wireless access point
- Change the default SSID name
- Change the default administrative account password

2. Guest Network Requirements
Any wireless network designated for use by guests, must adhere to the following:

- No access to the internal City network or resources
- Terms of use displayed when device connects

Policy Compliance

1. Compliance Measurement – The City will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the Mayor/Recorder/IT Director.
2. Exceptions – Any exception to the policy must be approved in advance by the Mayor/Recorder/IT Director.
3. Non-Compliance – An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Acknowledgement of WIRELESS NETWORK POLICY

Each employee with computer and network privileges is required to sign an acknowledgement in the form below and such acknowledgement will be placed in their personnel file. Failure to sign such acknowledgement does not excuse violations of the foregoing policies.

Employee Signature
I have received and read the above policy and have had the opportunity to ask any questions.
I understand that my failure to follow this policy may result in disciplinary action including revocation of system privileges or termination.

_____ _____
Employee Signature Date

_____
Print Name