ORDINANCE NO. _____

AN ORDINANCE ESTABLISHING INFORMATION TECHNOLOGY SECURITY POLICY AND PROCEDURES

WHEREAS, the Tontitown City Council deems it advisable to maintain the City of Tontitown Information Network for use by City Offices and Departments; and

WHEREAS, the Tontitown City Council deems it advisable to establish a security policy and procedures governing the use and development of the City of Tontitown Information Network;

NOW, THEREFORE, BE IT ORDAINED by the Tontitown City Council, that the security policy and procedures for the City of Tontitown Information Network are as follows:

Article I. Scope

Every user of Information Technology Resources (ITR) and the City of Tontitown Information Network (CTIN) will be responsible to abide by the policies and procedures outlined in this document.

This ordinance governs, without limitation, the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by the City, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at, and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with policies and standards, and local laws and regulations. Exceptions to this policy must be approved by the responsible elected official in advance. This policy applies to employees, contractors, consultants, temporaries, and other workers at this City, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the City.

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. These systems are to be used for business purposes in serving the interests of the City, and of our customers in the course of normal operations. An employee may access, use or sharing proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties.

Article II. Definitions

1. **City of Tontitown Information Network (CTIN):** An in-house intranet that serves the employees of City of Tontitown. An Intranet is not a site that is accessed by the general public.
2. **Computer:** For the purpose of this ordinance, a computer shall be defined as any electronic device capable of performing on the following—(1) Access of internet or intranet; (2) Access email; (3) Ability to transfer or download data; or (4) ability to create and store data. Such devices include but may not be limited to tablets; smart phones; laptop or desktop computers; servers; and work stations.
3. **Data**: The words, numbers, and graphics that describe people, events, things and ideas.

4. **Downloading**: The process of transferring a copy of a file from a remote computer to another computer's disk drive.
5. **Electronic Mail (E-Mail)**: A typed message or image sent electronically from one user to another.
6. **E-Mail Attachment**: A file such as a document, worksheet, or graphic that travels through the e-mail system along with e-mail messages.
7. **Encryption**: To put into code or cipher or to scramble access codes to computerized information so as to prevent unauthorized access.
8. **Extranet**: Systems used to give tours and demos, including webex. Systems used to schedule events, manage projects, streamline document workflow, improve collaboration between employees, vendors, etc.
9. **Information Technology Resources (ITR)**: Includes, but is not limited to computers, databases, software, servers, and the CTIN (CTIN); files, folders, and documents; Internet access and web pages; and electronic mail including both Intranet and Internet.
10. **Internet**: A collection of local, regional, national, and international computer networks that are linked together to exchange data and distribute processing tasks.
11. **Intranet**: An infrastructure using Web technology for internal communication.
12. **Network**: A group of connected computers that allow users to share information.
13. **Server**: A computer and software that make data available to other computers.
14. **Software License**: A legal contract that defines the ways in which one may use a computer program.
15. **Virus/Malware**: A generic term for a number of different types of malicious codes or programs designed to attach itself to a file, reproduce, and spread from one file to another, destroying data, displaying an irritating message, or otherwise disrupting or rendering a computer system useless.
16. **Use**: Includes, but is not limited to transmitting; uploading; downloading; cutting, pasting and copying; forwarding or retransmitting; attaching to e-mail messages; attaching to chat messages; posting in a public access area; printing; saving to disk or other storage medium; and sending by FAX.

Article III. General Conditions of Use

A. Applicability

The conditions of this Article are applicable to all who use Information Technology Resources (ITR) and the CTIN (CTIN). This includes, but is not limited to all Departments, Offices, contractors, and others.

B. Privacy and Monitoring

1. The City of Tontitown reserves the right to access, monitor, and disclose all Intranet and Internet e-mail, Internet usage and web sites visited, and any information stored on City of Tontitown computer systems at any time with or without notice to employees.
2. Employees should recognize that electronic information might be used in disciplinary proceedings, may be referred to the Sheriff's Office or other government agencies for criminal investigation, may be subpoenaed for legal proceedings, and may be subject to Freedom of Information Act requests.
3. Employees should assume that any e-mail or Internet communication, whether business-

related or personal, created, sent, received, or stored on the CTIN might be read or heard by someone other than the intended recipient, including but not limited to the Department Head or Elected Official for the office in which the message was created.

C. Computer Access

1. The Mayor, or his designee, will authorize which contractors, consultants or others have access to the City of Tontitown computers, CTIN, e-mail, and Internet access.
2. The Mayor, or his designee, will determine the level of access to the CTIN, e-mail, internet, and intranet to which employees will have access.
3. Former City Employees, Officials, contractors, consultants, and others are explicitly prohibited from accessing City of Tontitown computers, CTIN, and e-mail.

D. Remote Access

1. To facilitate end-user support in the computer environment, remote control software can be utilized to help resolve an issue or to upgrade software configurations remotely, only if first authorized by the Mayor. It is acknowledged that remote control software, when authorized, grants complete access/control to another computing device whether or not it is logged into the network. The software can be used to transfer files to/from another PC, to access any file on the remote PC or the network, to view and update those files, to update application software, to change PC configurations, and to view what is currently displayed on the screen of the remote PC.
2. Remote control software, and remote access software such as VPN, is prohibited from being permanently enabled on all City computers and devices, with the exception of mobile computers and devices designated to be used to monitor the water and sewer Supervisory Control and Data Acquisition (SCADA) system and SCADA System server.
3. The remote control software will be used in a professional manner and only in direct support of City business objectives. Any remote control software used must have the capability to log access activity. Unless authorized in writing by a department head and approved by the Mayor, remote control software utilization that is not directly related to resolving an electronic device issue is prohibited. Remote control software shall not be used to view financial or accounting data, unless by proper authorities, or by the accounting software vendor to resolve technical issues.
4. After the use of any remote control software, a log of the activity shall be provided. Said log shall be signed by the person who supervised the activity, and provided to the Mayor.

E. E-Mail Retention

There shall be no requirement to retain E-mails. E-mails saved by employees that are more than sixty (60) days old shall have properly redacted copies for the purpose of responding to Arkansas Freedom of Information Act requests. No E-mails older than sixty (60) days will be kept on the email server.

F. Passwords

1. Employees may never share or reveal their password for access to CTIN, mainframe

computer menus, e-mail, or Internet. Employees are advised that they are solely responsible for actions conducted under their password or with their user name. Users shall not let unauthorized individuals have access to or use City of Tontitown's e-mail, or access to the Internet through City of Tontitown's ITR.

2. Employees will sign off, log off the CTIN, and the Internet when not using them. Employees should sign off, log off, or lock the work station when not in the physical presence of the computer or electronic device to which they have access. Employees should recognize that signing off the City of Tontitown computer or electronic device does not sign them off of the e-mail network or Internet Access.
3. Users shall not knowingly utilize employees or officials user names and passwords unless authorized to resolve a computer issue. Employees shall notify the Mayor in writing if unauthorized use is discovered.
4. There shall be a password credential requirement of at least one capital letter, one number, one special character, and must be at least 8 characters in length. System level and user level passwords must comply with this password policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited. This includes family and other household members when work is being done at home.

G. Law Enforcement Agency Data Systems Requirements

The Arkansas State Police requires users to follow established criteria in order to access law enforcement systems. These criteria are incorporated herein by reference, and are applicable to those Departments and Offices which use such systems, unless those Department Heads state otherwise in their Departmental or Office policies. It is the Department Head's responsibility to ensure the ITR is compliant with established law enforcement criteria for such use.

H. Software

1. Each Department Head shall insure computer virus protection software is installed on all ITR equipment on the CTIN. Nothing shall be done to intentionally disable this software.
2. Software applications used on City of Tontitown computers and electronic devices that are connected to the CTIN must be authorized by the Mayor.
3. Installation of encryption or authentication (digital signature) software, other than that contained within standard software applications is prohibited on computers and electronic devices, unless authorized by the Mayor

I. Department Head and Elected Official Responsibility

Elected Officials and Department Heads are responsible for all stand-alone computers and their contents located in their departments and offices, and in remote locations.

J. Prohibited usage:

1. Never intentionally use a City of Tontitown computer or electronic device in any way that violates local, state, federal, or international law; or any vendor agreement, software license agreements, or Internet Service Provider conditions.
2. Never initiate any activity that is damaging in any way to the CTIN, the e-mail, internet and intranet systems, or the World Wide Web. Never intentionally damage,

destruct, deface or compromise any equipment or software of the City of Tontitown. Never intentionally damage, destruct, deface or compromise any data in CTIN without proper authorization.

3. Any exception to the policy must be approved by the responsible Elected Official in advance.

K. Virus/Malware Reporting

If an employee suspects a virus has been introduced to a computer they should notify their Department Head immediately. The Department Head shall immediately advise the Mayor, who may then authorize the installation of software to scan incoming e-mails for viruses. If this is done, all e-mails shall be so scanned before they are opened.

L. Monitoring

1. The Mayor may authorize the monitoring of City of Tontitown networks and systems for appropriate use and compliance.
2. The Mayor may establish usage criteria for e-mail, Internet, intranet, networks, web page, and web page development.

M. Release of Information

1. Internet or e-mail Freedom of Information Act requests must contain the name and mailing address of the requestor to be accepted. If an e-mail or internet FOIA request is received, it shall be forwarded to the Mayor for proper referral or disposition.
2. Unless specifically authorized by Departmental or Elected Official Policies, confidential information as defined by the Arkansas Freedom of Information Act shall not be released or divulged without prior approval of the relevant Department Head or Elected Official.

N. Prohibited Computer Usage

1. Never use an e-mail account at work (or elsewhere for City business) other than the one assigned by the Mayor. Never attempt to gain access to any files, folders, e-mail accounts, or documents without proper authorization. Employees may not intentionally intercept, eavesdrop, record, or alter another person's e-mail. Nor may employees use the internet to intentionally intercept, eavesdrop, record, or alter another person's information. Never attempt to use the Internet to gain unauthorized access to remote computers or other systems.
2. Employees shall not use or attempt to use alternate methods of connecting to the Internet other than what is authorized by the Mayor.
3. Never use your computer in violation of any City of Tontitown Ordinance or Policy applicable to your Department or Office.
4. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. If there is any uncertainty, employees should consult their supervisor or manager.
5. Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing City resources. Computers may not be used to receive, transmit, create, or do any of the following intentionally:
   a. obscenity, sexually explicit messages, pornography, or child pornography;

b. threats, fighting words, or intimidation;
c. libel, defamation, or slander;
d. harassment of any kind, including harassment on the basis of race, sex, religion, ethnic origin, or other protected status;
e. humor or jokes that are intended to offend, harass, or intimidate, or are likely to offend, harass or intimidate a reasonable person;
f. software piracy;
g. chain letters; unsolicited e-mail and "spamming"; anonymous e-mails or e-mails with altered or incorrect return addresses;
h. multilevel marketing opportunities, pyramid schemes, franchises, business opportunity ventures, investments; or
i. violate the privacy of any individual.

6. Computers may not intentionally be used for the unauthorized copying or transmission of:
   a. text;
   b. other communications;
   c. computer software;
   d. photographs;
   e. video images;
   f. graphics;
   g. music; or
   h. sound recordings.
7. Never download, delete, or install any software or program onto a computer or electric device connected to CTIN; and never disable any firewall or virus protection.
8. Any communications, including e-mails, made in or from the CTIN may be attributable to City of Tontitown and the Elected Office or Department from which it is made. All such communications must be professional and comply with this policy.

O. Attachments to E-Mails

Employees who receive e-mails from unknown sources that have attachments will delete those messages from their in-box folder without opening them, and then delete those messages from the deleted items folder, if they have not been scanned for viruses.

P. Purchases, Conditions, and Fines

1. An Employee is responsible for understanding and complying with conditions specified in any public domain or shareware software that is downloaded, and for arranging approval and payment through normal Department or City procedures for any fines or fees associated with such use.
2. Employees may only make credit card purchases on the Internet from City of Tontitown ITR when authorized to do so by the relevant Department Head or Elected Official. Employees will verify the web site is a secure site before making such a purchase.

Q. Discipline

1. Employees observing violations of this ordinance should report the violations to the Department Head or Elected Official supervising their office or department. Alleged violations will be investigated and employees shall cooperate with any investigations concerning violations of this policy.
2. Violations of this ordinance may result in disciplinary action, up to, and including, dismissal from employment and, if applicable, possible criminal or civil penalties or other

legal action.

3. Violations of this ordinance may result in termination of any contract or consulting contract, and may result in criminal or civil penalties or other legal action.

R. Lost or Stolen Items

All users have a responsibility to promptly report the theft, loss or unauthorized disclosure of proprietary information.

S. Blogging/Social Media

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 the Policy. Limited and occasional use of the City's 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 the City's systems is also subject to monitoring.
2. Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by this policy.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of and/or any of its employees. 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.
4. Employees may also not attribute personal statements, opinions or beliefs to when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the City. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the City's trademarks, logos, and any other intellectual property may also not be used in connection with any blogging activity.

Article IV. Repeal Clause

All ordinances and codes and parts of ordinances and codes in conflict herewith are hereby repealed.

Passed and approved this _____day of _____, 2015.

_____

Mayor

Attest:

_____

_____

Sponsor