**AGENDA**
**CITY OF HARRISONVILLE**
**FINANCE/PERSONNEL COMMITTEE**
**REGULAR MEETING**
**CITY HALL**
**AUGUST 1, 2018**
**6:00 PM**

**I. Call to Order**

**1. Roll Call**

**II. Approve Minutes**

**1. Finance/Personnel Committee - Regular Meeting - May 15, 2018 6:00 PM**

**III. Agenda Items**

**1. Banking Services Contract**

**2. Technology Policy**

**IV. General Discussion**

**V. Adjournment**

**Posted on City Hall Bulletin Board this 25th day of July 2018**

_____
**Randall K. Jones, City Clerk**

**The Board of Aldermen meeting is an open meeting but is not a meeting of the public. There is a place on the agenda for comments of citizens under PUBLIC PARTICIPATION. Our rule is that comments by any individual or group shall not exceed (4) minutes. The Board of Aldermen request that concerns be initially addressed at the appropriate action level before coming to the Board of Alderman**

*Publish*

DRAFT

# MINUTES
# CITY OF HARRISONVILLE
# FINANCE/PERSONNEL COMMITTEE
# REGULAR MEETING
# CITY HALL
# MAY 15, 2018
# 6:00 PM



## I. Call to Order

The meeting was called to order at 6:00 PM by Chair Brian Hasek

| Attendee Name | Organization | Title | Status | Arrived |
|---|---|---|---|---|
| David Dickerson | Harrisonville | Member | Present | |
| Brian Hasek | Harrisonville | Chair | Present | |
| Clint Long | Harrisonville | Member | Absent | |
| Brad Bockelman | Harrisonville | Member | Present | |
| Judy Reece | Harrisonville | Member | Present | |

*Others present were: City Administrator Happy Welch, Finance Director Marcella McCoy and City Clerk Randall Jones Recording.*

## II. Approve Minutes

### 1. Finance/Personnel Committee - Regular Meeting - Dec 14, 2017 6:00 PM

| | |
|---|---|
| **RESULT:** | **ACCEPTED [UNANIMOUS]** |
| **MOVER:** | David Dickerson, Member |
| **SECONDER:** | Judy Reece, Member |
| **AYES:** | David Dickerson, Brian Hasek, Brad Bockelman, Judy Reece |
| **ABSENT:** | Clint Long |

## III. Agenda Items

### 1. Personnel Policy Review

*City Administrator Happy Welch presented policy changes. It was decided to add to the definitions the term "consanguinity". There was discussion on mileage reimbursement changes and discussion on holidays observed.*

| | |
|---|---|
| **RESULT:** | **APPROVED [UNANIMOUS]** |
| **MOVER:** | David Dickerson, Member |
| **SECONDER:** | Brian Hasek, Chair |
| **AYES:** | David Dickerson, Brian Hasek, Brad Bockelman, Judy Reece |

| | |
|---|---|
| **ABSENT:** | Clint Long |

**2. 457 Provider**

*City Administrator Happy Welch presented staff report.*

| | |
|---|---|
| **RESULT:** | **APPROVED [UNANIMOUS]** |
| **MOVER:** | David Dickerson, Member |
| **SECONDER:** | Judy Reece, Member |
| **AYES:** | David Dickerson, Brian Hasek, Brad Bockelman, Judy Reece |
| **ABSENT:** | Clint Long |

**3. Gas Card**

*City Administrator presented staff report.*

| | |
|---|---|
| **RESULT:** | **APPROVED [UNANIMOUS]** |
| **MOVER:** | David Dickerson, Member |
| **SECONDER:** | Brian Hasek, Chair |
| **AYES:** | David Dickerson, Brian Hasek, Brad Bockelman, Judy Reece |
| **ABSENT:** | Clint Long |

**4. College Agreements**

*City Administrator Happy Welch presented staff report.*

| | |
|---|---|
| **RESULT:** | **APPROVED [UNANIMOUS]** |
| **MOVER:** | David Dickerson, Member |
| **SECONDER:** | Judy Reece, Member |
| **AYES:** | David Dickerson, Brian Hasek, Brad Bockelman, Judy Reece |
| **ABSENT:** | Clint Long |

## IV. General Discussion

none.

## V. Adjournment

Motion to adjourn by Alderman Dickerson with second by Mayor Hasek. Meeting adjourned at 7:10 p.m.

The meeting was closed at 7:10 PM

Brian Hasek, Mayor & Ex-Officio
Chairman of the Board of Aldermen

ATTEST:

_____

Randall K. Jones, City Clerk

City of Harrisonville est. 1836

STAFF REPORT

**TO:** **Finance/Personnel Committee**

**FROM:** **Marcella McCoy, Director**

**DATE:** **July 24, 2018**

**SUBJECT:** **Banking Services Contract**

**Type of Item:** *Contract*

The purpose of this memo is to outline the process used to recommend banking services including the timeline for the request for proposals and staff's recommendation for depositary bank.

DISCUSSION

The City last went out for banking proposals in 2011. Community Bank was recipient of that contract for a period of three years and have renewed the service each year thereafter. Procedures are to go out for banking service bids every five years.

Request for proposals for bank services that are Federal, or State of Missouri chartered, and have at least a main office in the State of Missouri and a branch in or near the city for day-to-day transaction services were published on May 25, 2018. Letters were sent to each local branch bank referencing the request for proposals be submitted. The sealed proposals were due in my office by 2pm on June 26, 2018. Two proposals were received, our current bank, Community Bank of Raymore, and Commerce Bank.

Staff that reviewed the proposals were Debbie Phelps, Accounting Specialist, Happy Welch, City Administrator, and myself. Debbie is a key resource in this process because she is the one that works with the bank daily and completes the reconciliation, bond payments, investments, and numerous other functions that involve bank transactions. Debbie has put together a list of advantages and disadvantages for each bank based on daily tasks and review of the request for proposals requirements. They are attached for reference.

One of the hardest part of this process was putting a cost on not having several advantages compared to the cost of transactions and services. Community Bank currently does not charge a monthly fee for any service provided and their proposal is to continue that practice. As you will see, there are several disadvantages listed for Community. The biggest factor to consider is risk. We have recently seen a local company subjected to some major risk with Information Technology. A key factor to avoiding or minimizing that risk is a disaster recovery plan and the availability of multiple locations apart from the same geographic area.

There are a few challenges that have been encountered with previous banking services.

They include items such as date verification, completing transactions when account numbers don't match up, and not following up with a person or verifying information contained in a file. These are not all Community Bank related nor do we believe there is a fool proof system out there that will catch every human error. However, we believe that Commerce is well prepared to provide such checks and balances.

The attached documents outlining the advantages and disadvantages clearing shows Commerce complying with the complete request for proposal requirements. Staff is recommending Commerce Bank be awarded the banking services contract.

**1. Action Item (ID # 2953)**

Banking Services Contract

Attachments:

RFP Comparitive Narrative (PDF)

# Community Bank of Raymore

*Advantages:*

- No cost
- Current bank – no conversion

*Disadvantages:*

- No disaster recovery plan outlined in RFP
- Chartered bank
- Equity of $19.1 million
- $238.6 million in assets
- Three offices with 44 total employees
- Offices are geographically close making the susceptible to disaster risk
- No ACH credit option available for accounts payable vendors
- Does not offer bank owned merchant services
- Wire transfers currently made via emailing PDF file containing banking information and transfer amount to bank employees
- City of Harrisonville is only customer with CBR that uses the Positive Pay Function. Recently during a software conversion at CBR this option was inadvertently eliminated, and the City was not notified but instead discovered when attempting to use the Positive Pay Option

# Commerce Bank

*Advantages:*

- Detailed disaster recovery plan
- Multi state presence minimizes disaster risk
- Online wire and ACH debit and credit capabilities available through multiple layers of security
- Currently services Harrisonville School District
- Dual approval controls for cash transactions done online through Commerce Connections
- $6.4 billion in Market Cap
- $24.8 billion in assets
- Instant online reports
- Online return notification
- Commerce Markets is current broker for the City's investments
- Overnight interest sweep
- Commerce Bank owned merchant services available
- Multitude of optional services available
- Higher security than what is now being used by the City
- Detailed account analysis online
- DirectCheck Card available to those who do not receive paychecks via ACH
- Access to Benefits Banking service to employees

*Disadvantages:*

- Cost for service

City of Harrisonville est. 1836

STAFF REPORT

**TO:** **Finance/Personnel Committee**

**FROM:** **Happy Welch, City Administrator**

**DATE:** **July 16, 2018**

**SUBJECT:** **Technology Policy**

**Type of Item:** *Approval*

**Background:**

We adopted the new Personnel Policy back in June and in an effort to streamline it we pulled out the Technology Policy so it could be updated on its own, since technology and social media and other tech items are changing so quickly.

**Issue:**

We have reviewed the policy, updated it and need approval from the committee.

**Recommendation:**

Approve the new and improved Technology Policy to be a separate document for distribution to full and part-time employees. This has been reviewed by our City Attorney for compliance.

**2. Action Item (ID # 2952)**

Technology Policy

Attachments:

2018Technology Policy Markup - CLEAN COPYjf redline v2 (002)hw rvw 7-10-18 rev JF 7-16-18 initial cleanup (003) (PDF)

# City of Harrisonville

TECHNOLOGY AND COMPUTER POLICY

## Contents

# City of Harrisonville

TECHNOLOGY AND COMPUTER POLICY

## T-1. Introduction

It is the express purpose of this Technology and Computer **Policy** (sometimes herein "Policy") to establish guidelines and standards for the use of **City** owned computing equipment. It is also intended to give employees a clear understanding of the expected and accepted use of the **City's** computer/internet/voice mail & **E-mail** systems. Contained in the sections following are guidelines, standards, and other material that may be helpful to the computer **User**. It outlines the **City's** position on monitoring and access to **Employee City** computer files and is designed to inform employees under what circumstances all **City** computer files may be accessed. It is fully expected that the material contained herein will

be revised and supplemented as new products are introduced and understanding evolves on how best to accommodate information processing needs.

The **City** maintains as part of his technological platform electronic media systems which include, but are not limited to, telephones, email, fax systems, voicemail, computers, hard drives, network devices, systems supporting email, **Internet** access, voice communication, CDs and diskettes. All electronic media systems and the data stored on them are, and remain at all times, the property of the **City**. They are provided to assist in the conduct of business within the **City** and are to be used by authorized personnel only.

Just because a particular activity is not expressly stated or prohibited by the policy does not mean that an **Employee** is allowed to engage in it. General established personnel policies and guidelines will be used to address situations that are not expressly written in the **Policy**.

This **Policy** applies to all employees, part-time employees, volunteers, and other individuals who are provided access to the **City**'s computer system. Employees who separate from **City** service have no right to the contents of their **City** or job-related computer files and are not allowed access to the **City** computer system without permission of the **City Administrator**.

This **Policy** may only be changed upon the written approval of the **City Administrator**.

The **City Administrator** may authorize upon request additional individual department policies.

The general standards of conduct expected of a **City Employee** or public official also apply to the use of **City** computing resources.

The **City** resources include:

- Hardware - Physical equipment used for processing or communications.
- Software - Programs, programming languages, instructions, or routines, which are used to perform work on a computer.
- Data - Information such as records, files or textual material stored on or accessible through a computer.
- Communication lines - Telephone, ethernet, mobile phones, fiber optics or communication lines that allow the transfer of electronic data between computer servers and the **Internet**.
- System - The hardware, software, data, communication lines and equipment that form the computer network for the **City** of Harrisonville.

**City** computing resources are made available to individuals to assist in the pursuit of organizational goals. It is expected that **Users** will cooperate with each other to promote the most effective use of computing resources and will respect each other's work even though it is in electronic rather than printed form. Individuals and organizations will be held no less accountable for their actions involving computers than they would be in other situations.

While the **City** recognizes the civil, personal and property rights of those actually using its computing resources, the **City** also must protect the confidentiality of **City** records stored on its computer systems from unauthorized access.

## T-2. No Expectation of Privacy with City Computers/Equipment.

The **City** respects the individual privacy of its employees. However, **Employee** privacy does not extend to the **Employee**'s work-related conduct, to the use of **City** provided equipment or supplies, or to any email, file or data created on or saved to **City** computers, or any such files, data or information transmitted or received through **City** equipment.

All information, files, data, text, images or emails that are on **City** equipment may be disclosed to law enforcement or other third parties at the sole discretion of **City** without the prior consent of the sender or receiver.

**Regardless of any statement contained herein, employees shall not have an expectation of privacy regarding any work performed or files stored on the City's computer system.**

## T-3. Definitions.

### T-3.1. City.

Means the **City** of Harrisonville, Missouri.

### T-3.2. City Administrator.

Means the **City Administrator** for the **City** of Harrisonville, Missouri.

### T-3.3. City Computers/Equipment.

The words or similar phrases like **City** computer or computers, Computers or computer, **City** computer system or systems, **City** computer property, **City** computer resources, Computer information system or systems, computer network or **City** electronic equipment shall include any type of **City** computer, network, system or electronic equipment owned or leased by the **City**.

### T-3.4. Downloading.

The transmission of a file from one computer system to another, usually smaller, computer system.

### T-3.5. Electronic Mail.

The exchange of computer-stored messages by telecommunication.

### T-3.6. Employee.

Includes any full or part-time **Employee** of the **City** of Harrisonville, Missouri.

**T**-3.7. **Freeware.**

Programming that is offered at no cost. However, it is copyrighted so that you can't incorporate its programming into anything you may be developing.

**T**-3.8. **Incidental Use.**

A subordinate use that does not interfere with the overall business use and does not have a negative impact on the operation of the system.

**T**-3.9. **Internet.**

The **Internet** is the global system of interconnected computer networks that use the **Internet** protocol suite (TCP/IP) to link devices worldwide. It is a *network of networks* that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The **Internet** carries a vast range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing.

**T**-3.10. **Internet Access.**

Connection to the internet through a modem or other portal access.

**T**-3.11. **Internet E-mail: E-mail (electronic mail).**

Is the exchange of computer-stored messages over the **Internet**.

**T**-3.12. **Listserv:**

A small program that automatically redistributes **E-mail** to names on a mailing list. **Users** can subscribe to a mailing list by sending an **E-mail** note to a mailing list they learn about; listserv will automatically add the name and distribute future **E-mail** postings to every subscriber.

**T**-3.13. **Malware.**

Short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other intentionally harmful programs. It can take the form of executable code, scripts, active content, and other software. Malware is defined by its malicious intent, acting against the requirements of the computer **User** — and so does not include software that causes unintentional harm due to some deficiency.

**T**-3.14. **Phishing.**

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

**T**-3.15. **Pharming.**

The fraudulent practice of directing **Internet Users** to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal information such as passwords, account numbers, etc.

**T**-3.16. **Public Information Officer ("PIO").**

Maintains the **City**'s online presence with Facebook, Twitter, Instagram, Snapchat, and other online media sources. Is responsible for **City**'s website maintenance.

**T**-3.17. **Shareware:**

Software that is distributed free on a trial basis that the **User** may need to pay for later or there is some advertising associated with it.

**T**-3.18. **Spam:**

Irrelevant or inappropriate messages sent on the **Internet** to a large number of recipients.

**T**-3.19. **Spyware:**

Software that aims to gather information about a person or organization without their knowledge, that may send such information to another entity without the consumer's consent, or that asserts control over a device without the consumer's knowledge.

**T**-3.20. **Systems Administrator:**

Which shall also mean the IT Department and include any references to it and its personnel, and over-sees operations of **City**'s information systems.

**T**-3.21. **User or Users:**

Shall include any **City Employee**, staff, contractor, volunteer or other individual who is granted access to and/or uses **City** owned or leased computer equipment.

**T**-3.22. **Virus:**

A piece of programming code inserted into other programming to cause some unexpected and, for the victim, usually undesirable event. Viruses can be transmitted by downloading programming from other sites or be present on a diskette. The source of the file you're downloading or of a diskette you've received is often unaware of the virus. The virus lies dormant until circumstances cause its code to be executed by the computer. Some viruses

are playful in intent and effect and some can be quite harmful, erasing data or causing your hard disk to require formatting.

## T-4. User-ID.

The **City's Computer System** requires that each **User** have a unique identity, referred to as a "**User**-ID", protected by a "Password", which allows a **User** to gain access to the system. The computer identity is used to represent a **User** in various system activities; to provide access to certain software and data, based on the **Users**' credibility and purpose for requiring such access, and to associate the **User**'s own software and data with the **User**'s identity. As such, this computer identity is another instrument of identification and its misuse constitutes forgery/ misrepresentation.

## T-5. General Guidelines.

**Violation of this Policy, any guideline, or prohibited activity may result in disciplinary action up to and including termination of employment.**

### T-5.1. Personal Use of Computers.

The **City**'s computer systems are very valuable and are intended solely for **City** job-related activities. **Users** are prohibited from using the **City**'s computer systems for personal or private benefit. The **User**'s Supervisor must approve incidental personal use of the **City** computer. In the event a question regarding the appropriateness of the use exists, the Supervisor shall discuss such use with the **City Administrator**.

There are times that employees take part in organizations outside of the **City** that benefit the **City**, such as professional organizations, civic clubs, etc. Since the **City** encourages participation in these organizations, use of **City** computers for these types of activities may be authorized by the **User**'s Supervisor. A copy of the **Employee**'s written request, along with the Supervisor's written approval, must be sent to the **City** Department Head and the **City Administrator**. Common sense is to be used when utilizing the **City**'s computer resources.

To insure the integrity of the **City**'s computer systems, using the **City**'s systems to store personal data and to play computer games is not permitted. **Users** are also prohibited from allowing family members to utilize the **City**'s computers during or after business hours. This will prevent accidental damage to the system by **Users** who are not trained on such equipment.

Personal computers or cell phones shall not be connected to any **City** equipment or network without the express written approval of the **City Administrator**, **Systems Administrator** and appropriate **City** Department Head. Doing so provides an opportunity for cross contamination of malware. This includes (but not limited to): any storage or USB device, phones, SD cards, computers, network drives, or wireless devices and electronics.

**T-5.2. Harassment.**

The **City**'s electronic equipment may not be used to harass anyone. This includes without limitation sending sexual comments or images, insulting or fraudulent statements, sexist gender-specific comments, racist comments or slurs, obscene, or use of suggestive electronic mail and/or internet sites, or sending comments that would offend someone on the basis of their age, religious or political beliefs, national origin, pregnancy or disability; tampering with others' files; and invasive access of others' equipment. In addition, **Users** of any electronic communication facilities - such as email, networks, bulletin boards, and news groups - are obligated to comply with the restrictions and acceptable practices established by the **City** herein and for those specific facilities.

Certain types of communications are expressly forbidden, examples of which are listed in Section T-11.1..

**T-5.3. Waste and Abuse.**

The **City**'s computer systems are a valuable resource, and they should not be abused or wasted. **Users** must avoid any activity around computer workstations that may result in damage to hardware, software, or information. Eating or drinking while in close proximity to equipment should be minimized as food crumbs and liquid spills can cause severe damage to computer equipment causing it to have to be replaced.

Departments have to share computer resources, therefore, be considerate of fellow employees. Avoid monopolizing systems, bandwidth, disk space, printing equipment, and other computer resources.

**T-5.4. User Responsibility.**

**Users** are responsible for their own actions with respect to the **City**'s computer-use guidelines, this **Policy** and other **City** policies. Disciplinary action may be warranted in cases of abuse or disregard of these guidelines. **Users** also are required to participate in assuring the legal and ethical use of **City** computers and **User** accounts. Any violation of these guidelines should be reported through the normal chain of command.

**T-5.5. Enforcement.**

The **City** will investigate all alleged abuses of its computer resources. As part of that investigation, the **City** may, without notice to employees, access the electronic files of its employees. If the investigation indicates that **City** computer privileges have been violated, the **City** may limit the access of employees found to be using computer systems improperly. In the course of its investigation, the **City** may reveal flagrant abuses and private, **Employee**-related information to supervisory and management personnel or law enforcement authorities. Due to the municipal ownership of the system, employees shall not have an expectation of privacy in any work performed or files stored on any **City** municipal property or computer equipment.

**T-5.6. Workplace Monitoring.**

The **City** has the obligation to ensure that its computer resources are used properly and within the established guidelines. In pursuit of that goal, the **City** reserves the right to monitor the **City** electronic and computer system for signs of illegal or unauthorized activity on any **City** electronic equipment. The **Systems Administrator** will be completing regular reviews and audits of equipment and software. Any unauthorized activity on a PC will be dealt with at that time. All situations will be reported to a **User**'s supervisor.

**T-5.7. User and Department Needs/Wants.**

The **Systems Administrator** is available at all reasonable times for discussion regarding the **City** computer system. If a **User** or department has a request for hardware, software, programming, etc. it must be submitted in writing to the **Systems Administrator** via the **User**'s Supervisor. If a Department has suggestions as to how a **User**'s work environment could be improved via the computer system, it should be discussed with the **Systems Administrator**. Every effort will be made to accommodate requests that fit into the overall plan of the **City**'s computer system.

**T-5.8. Open Records Law.**

All files, **E-mail** and other data created on the **City** computer system are subject to the Missouri Sunshine Law, also known as the Open Meetings and Open Records Law. Files which would be deemed closed records under the Missouri Sunshine Law if not otherwise stored in the system shall be deemed closed records and inaccessible to the public. Any questions regarding the interpretation of the Sunshine Law should be referred to the **City** Clerk or the custodian of records. Legal confidentiality of records must be maintained.

## T-6. Security Training.

Security Training is administered by the **Systems Administrator** and is required of all **Users** who log into the **City** computer system. Employees not completing the required training will have their credentials disabled and refusal to complete training in the time frame required will be grounds for disciplinary action.

## T-7. Computer Software.

**T-**7.1. **Licensed Software.**

"Licensed software" refers to software the **City** has purchased or that has been given under authorized permission from a software company.

The **City** works hard to maintain an accurate list of software and maintain appropriate **User** licenses for all software. The breaking of software licensing agreements is a serious action and could cause financial loss to the **City** if software protection laws are not adhered to.

It is the **City**'s policy that copying or use of software other than under the stated conditions of the respective license agreement is prohibited. This includes the copying and distribution of associated documentation.

In all situations, the **City** must hold the actual license for the software before it is installed on the **City**'s computer systems. Any software installed without the license held by the **City** is illegal and will be removed from the **City**'s systems immediately.

### **T**-7.2. **Unauthorized Use of Software**

**Users** are prohibited from loading any software, including demos, on any **City** owned computer system except with Supervisor or designated personnel approval. This includes commercial, shareware, and freeware software. Further, **Users** are expressly prohibited from using **City** computers to make illegal copies of licensed or copyrighted software. Copyrighted software must only be used in accordance with its license or purchase agreement. **Users** do not have the right to make unauthorized copies of software for themselves or anyone else.

**Users** are prohibited from using software that is designed to destroy data, provide unauthorized access to the computer systems, or disrupt computing processes in any other way. Using viruses or any other invasive software is expressly prohibited.

Absolutely no software or files from home/personal computers or other agencies are to be installed or placed on the **City**'s computers without System Administrator approval.

### **T-7.3. Software Installation and Removal.**

In a networked environment, it is extremely important that individuals not install software. Software installations often cause changes to the system settings of the computer operating system. These changes could significantly impact the way a computer runs or its ability to access the network. Therefore, the **Systems Administrator** is the only person authorized to install and remove all software programs, including demos. This will allow for consistency between workstations and provide the **City** with an accurate accounting of what is contained on every local computer and network. **City** employees often receive flash drives, CD's and various computer media from other cities, clients or businesses that contain computer files. These items must be evaluated by the **Systems Administrator** before they are loaded on the **City**'s computer system. Once the **Systems Administrator** has evaluated and virus checked the item, only the **Systems Administrator** is authorized to put the item in a location that is accessible to the **User**.

### **T-7.4. Shareware/Freeware.**

Shareware and freeware will be evaluated for use by the **Systems Administrator** just as any other piece of software. Departments will follow the proper procedures for submitting a request for the purchase of shareware or the use of freeware.

### T-7.5. Images, Screensavers, Wallpaper and Sound Files.

It is not appropriate or an accepted practice to load screen savers or wallpaper backgrounds from other computers onto the **City**'s computers. The addition of image files (i.e. pictures of miscellaneous items), screen savers, wallpaper or sounds to the **City**'s computer system is considered to be an installation. Wallpaper backgrounds utilize unnecessary disk space and could potentially cause problems if large numbers of these items are loaded. Files such as these also often carry the potential for viruses and shall not be allowed on the **City**'s computer systems unless put there by the **Systems Administrator**.

### T-7.6. Software Inventory.

The **Systems Administrator** will maintain a software inventory. If the **City** owns only one copy of a specific piece of software, the **Systems Administrator** will maintain manuals. The **Systems Administrator**, for easy access, retrieval and tracking, will maintain all software in a safe location.

All software disks will be located in the **Systems Administrator** office at city hall for proper storage and security.

## T-8. Internal and External Electronic Mail (E-Mail)

The **City**'s electronic mail system ("E-mail") is designed to facilitate **City** business communication among employees and other **City** business associates for messages and memoranda.

### T-8.1. E-Mail Not For Sensitive Materials.

Since no computer system is completely secure, the **E-mail** system is not intended and shall not be used to transmit sensitive materials, such as personnel decisions and other similar information which may be more appropriately communicated by written memorandum or personal communication, unless expressly authorized by the **City Administrator**. Furthermore, senders of confidential information via **E-mail** must label transmissions accordingly, so those receivers handle the data properly.

### T-8.2. E-Mail System Is Solely For City Business.

**E-mail** is to be used solely for **City** related business. Such system is not to be used for **Employee** personal benefit or to support or advocate for non-**City** related business or purposes, unless it has been specifically authorized in writing through the Supervisor or the **City Administrator**. All data and other electronic messages within the **Computer System** are the property of the **City** of Harrisonville. **E-mail** messages are **City** records and therefore need to adhere to department data retention schedules. **Users** are prohibited from transmitting fraudulent, harassing, or obscene messages and files. **Users** must not send any electronic mail or other form of electronic mail communication by forging another person's identity or attempt to conceal the origin of the message in any other way. **Users** are prohibited from distributing their **E-mail** addresses to **Users** that are not for professional or **City** use

**T-8.3. Personal E-Mail Use.**

Incidental and occasional personal use of **E-mail** is permitted, with prior written approval of the Supervisor, by the **City** of Harrisonville, but these messages will be treated the same as other messages. The **City** reserves the right to access and disclose as necessary all messages sent over its **E-mail** system without regard to content, and without notice to the **User**, sender or receiver. Since the **City**, without prior notice, can access each **User's** personal messages, **Users** should not use **E-mail** to transmit any messages such **User** would not want read by a third party. For examples of forbidden usage see Section T-11.1.

**UsersT-8.4. City May Review Any Employee's Emails.**

Although each **Employee** has an individual password to access this **System**, it belongs to the **City** and the contents of **E-mail** communications are accessible at all times by the **Systems Administrator** for any **City** purpose. Accordingly, the **City** reserves the right to, at any time, review the contents of an **Employee**'s **E-mail** communications without notification to the **Employee**. Employees shall not intentionally intercept, eavesdrop, record, read, alter, or receive other persons' **E-mail** messages without proper written authorization. The misuse of **E-mail** privileges shall be subject to discipline in accordance with the Personnel Manual, and/or applicable rules or laws.

**T-8.5. External Email Messages.**

**Users/Employees** shall not use the **City System** for their external or personal email accounts and shall not use **City Email** or **Internet** to post any message or comment that does not reflect the official **City** position. Employees when using their personal or public external or internet e-mail must be aware of and at all times attempt to prevent potential **City** liability in their use of the **Internet**.

**T**-8.6. **Retention of E-Mail**

Generally, **E-mail** messages are temporary communication, which are non-vital and may be discarded according to **City** retention policies. However, depending on the content of the **E-mail** message, it may be considered a more formal record and should be retained pursuant to a Department's record retention schedules. These **E-mail** messages are similar to printed communication and should be written with the same care. Each Supervisor shall establish and maintaining department retention schedules for the information communicated through the **E-mail** system. Retention schedules per requirements of the Secretary of State are available from the **City** Clerk.

Employees should be aware that when they have deleted a message from their mailbox it likely is not deleted from the **E-mail** system. The message may be residing in the recipient's mailbox, forwarded to other recipients or be sitting on the **E-mail** server. Furthermore, the message may be stored on the computer's backup system.

**T**-8.7. **Review of E-Mail**

It is important that **E-mail** (incoming messages) be reviewed and responded to appropriately, usually by the end of the business day. Supervisors are responsible to ensure appropriate use.

**T**-8.8. **Deleting Files**

Files may be deleted pursuant to written department policy approved by the **City Administrator**.

**T**-8.9. **Computer Games**

Since games are not proper business software, all computer games will be removed from **City** owned computer systems.

**T**-8.10. **Data Files**

If a **User**'s computer is connected to a network, all files created by that machine will be saved to a **User**'s account on the fileserver. No data is to be saved to the hard drive of a local network machine. The exceptions to this are laptops connected to a network or with Supervisor approval files may be saved on certain machines. This is for the protection of the **User**. Local machines are not normally backed up. Therefore, if a system were to crash, files stored on the local hard drive would be lost.

Saving of data created by computers not on a network will have locations specified by the **Systems Administrator**. Default directory paths of software applications are not to be changed unless otherwise approved by the **Systems Administrator**.

## T-9. Radio Communication.

**T-9.1. Generally.**

Radio communications is a tool that has been provided to employees that work in the field to better communicate with other staff and to provide another resource to contact dispatch in an emergency.

An **Employee** may hear sensitive information from the police, fire, or EMS crews. This information shall not be repeated by those not involved in the incident.

There are federal laws that prohibit the dissemination of these types of sensitive information. Under no circumstances shall privileged or sensitive information or investigations information be discussed with any unauthorized person. If the information is in question, then it will be considered privileged or sensitive and not disclosed. The information shall not be written down or recorded by non-emergency personnel.

The individual assigned a radio or has access to a portable, mobile, or desk top radio shall be required to be trained on its proper use and handling of the information that comes across the radio.

### T-9.2. Radio Procedures: Non-Fire/EMS and non-Police Department Radios

T-**9.2.1.** Radio Channels.

Radios shall not be turned to the police or fire talk groups unless it is needed for emergency communications.

T-**9.2.2.** Radio Traffic.

Information heard across these talk groups shall not be disclosed or disseminated in any fashion. This includes the following information:

9.2.2.1. Location of an incident

9.2.2.2. Type of Incident

9.2.2.3. Names

9.2.2.4. Personal Information

T-**9.2.3.** Emergency Zones.

Personnel shall refrain from traveling through an area that has been identified as an emergency, unless your department has been called to assist in the mitigation of the incident.

T-**9.2.4.** Security and Training.

Due to the sensitive nature of these two radio talk groups, all personnel associated with the radio usage shall be fingerprinted by Harrisonville Police Department and complete "Security Awareness Training". Those employees shall also sign a form indicating their acknowledgement of the policy regarding the radios and their usage.

## T-10. Voice Mail.

This policy applies to the use of Voice Mail by all **City** Departments **City** wide.

### T-10.1. Legal Obligations.

Use of **City** telephones is subject to all federal, state and local law, including but not limited to:

- RSMo. 569.094-569.099 concerning computer crime;
- RSMo. 573.010-573.065 concerning pornography and related offenses; and
- The Federal Communications Decency Act of 1996
- The Missouri Sunshine Law (RSMo. 610.029), which specifically provides that electronically stored data is subject to an information request, applies to all electronic information, including voice mail, unless otherwise exempted by state law.

### T-10.2. Sanctions

Penalties for violation of this **Policy** range from the loss of voice mail privileges to dismissal from **City** employment, prosecution and/or civil action. Each case will be determined separately on its merits in accordance with **City** policies and federal, state and local law.

### T-10.3. Definition of Terms

Voice Mail is an electronic voice messaging system that gives you an easy, fast, and dependable way to communicate with people. It allows you to:

- listen to, record, edit, and send messages
- send a message to more than one person
- set a date and time for message delivery
- play back message either at your desk, or from almost anywhere

External Calls are calls made outside your phone system to the **City**.

Internal Calls are calls made within our phone system by dialing a four-digit extension number (380 does not need to be dialed).

Voice Mailbox Denotes the ability to accept a voice mail at a specific phone number by dialing into the system.

### T-10.4. Responsibilities.

**City** Departments are encouraged to use voice mail to better serve both internal and external customers. Voice mail is never to be used as a mechanism for screening calls. Such action is subject to discipline. Each department is allowed to set up and enforce additional written voice mail or telephone policies, which may be applicable to its activities. Such policies may not conflict with this **Policy** or any other **City** policy.

**City** telephone numbers published to the general public should not use voice mail as the primary means of answering the phone during business hours. Those phones may have the voice mail option for after hours and internal messages but should always be answered by a "live" person during business hours. However, there are situations where call trees will need to be established for a department that will benefit the caller and employees who answer the phone by directing the caller to their preferred destination. These call trees are to be approved by the **City Administrator** with input from the Department Head.

The goal is to use voice mail primarily for employees to not miss an external phone call, and to minimize the number of times a citizen gets connected with voice mail. There is the option of a voice mail box to service the internal customer. If you experience a problem, the department should be told right away so they can solve it or track the problem.

Messages should reflect when the **Employee** is gone for more than a day (or else the phone should be forwarded to someone else). Calls should never be transferred from voice mail to voice mail.

The following are acceptable Voice Mail practices:

- Greetings placed on **City** voice mail for incoming calls must be kept current. If an **Employee** with voice mail privileges is out of town or away from the desk for an extended period, the message must reflect when calls will be returned.

- It is important that voice mail (incoming messages) be reviewed and responded to appropriately, usually by the end of the business day. Supervisors are responsible to ensure appropriate use.

- It is advised that every voice mail offer the option to the caller of pushing "O" for operator assistance.

- Voice mail messages (incoming or outgoing) should be business-like and professional. Use of obscenity or other offensive language is grounds for discipline or termination.

- Employees should be aware that voice mail messages might be monitored. A supervisor through the **Systems Administrator** may access individual voice mail accounts.

- There must be a "live person" at the end of any calling cycle - departments are responsible to check their system to make sure no black holes exist and that all calls roll to a live answer during business hours.

## T-11. Internet Access

The **Internet** provides the **City** with significant access and dissemination of information to individuals outside the **City** of Harrisonville. The use of the **City**'s **Internet** system access and dissemination is intended to serve solely **City** business interests. **Internet** access for personal use is prohibited. Like all **E-mail** messages, **Internet** messages are capable of being forwarded without the express permission of the original author. Therefore, **Users** must use caution in the transmission and dissemination of messages outside of the **City** and must and strictly comply with this **Policy** as well as all state and federal laws.

A wide variety of information is available on the **Internet**. Some individuals may find some information on the **Internet** offensive or otherwise objectionable. Individual **Users** should be aware that the **City** has no control over and can therefore not be responsible for the content of information on the **Internet**.

### T-11.1. Prohibited Internet Activities, Some Examples.

Though the **City** may provide **Users** with **Internet** access to help you do your job. **Internet** usage is solely intended for job-related activities.

This **Policy** is intended to prevent the misuse of **Internet** access. The following are some examples, by way of illustration and not limitation, of prohibited activities that violate this **Internet** policy:

- Sending or posting discriminatory, harassing, or threatening messages or images;
- The random mailing of messages; the sending of obscene, harassing, or threatening material; the use of the facilities for commercial or political purposes, or any other inappropriate or forbidden communication described in this policy or any other policy of the **City**.
- Employees shall not intentionally intercept, eavesdrop, record, read, alter, or receive other persons' **E-mail** messages without proper written authorization.
- Misrepresenting an individual's opinion as **City** policy or opinion.
- Improperly downloading files that contain viruses that may contaminate **City** information systems and databases.
- Using the **City**'s time and resources for personal gain.
- **Users** shall not use the **City E-mail** for gossip, including personal information about themselves or others, for forwarding information under circumstances likely to embarrass the sender or for emotional responses to business correspondence or work situations.
- Use of work time to browse the **Internet** for private interests. Use of private or personal time will be allowed with prior approval from Supervisor during non-work hours
- Stealing, using, or disclosing someone else's code or password
- Copying, pirating, or downloading software and electronic files
- Sending or posting confidential material, trade secrets, or proprietary information outside of the **City**
- Violating copyright law
- Failing to observe licensing agreements
- Engaging in unauthorized transactions that may incur a cost to the **City** or initiate unwanted **Internet** services and transmissions
- Sending or posting messages or material that could damage the **City**'s image or reputation
- Accessing objectionable or improper material, including participating in the viewing or exchange of pornography, sexually explicit or obscene materials. With the limited exception when such material pertains directly to research in the line of work. Also included in this prohibition are sites such as chat rooms that contain this type of material
- Sending or posting messages that defame or slander other individuals
- Attempting to break into the computer system of another organization or person

- Refusing to cooperate with a security investigation
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Using the **Internet** for political causes or activities, religious activities, or any sort of gambling
- Jeopardizing the security of the **City**'s electronic communications systems
- Sending or posting messages that disparage another organization's products or services
- Passing off personal views as representing those of the **City**
- Sending anonymous **E-mail** messages
- Engaging in any illegal activities
- Watching video content that is not part of a training series or department approved webinar.

**Some of the policies, guidelines and rules listed above are described in more detail herein.**

**T-11.2. Download, Program, App, or Resource Fees.**

Download, program, app, or resources of any kind for which there is a fee must not be accessed or downloaded without prior written approval of a Supervisor.

**T**-11.3. **Granting Internet Access.**

The **City**'s resources to access the **Internet** are limited; because of this the number of people with access to this resource must be closely monitored. Access to the **Internet** will be evaluated on a per **User** basis by the Supervisor, and notice shall be made to the **City Administrator** by the Supervisor. In general, it is advised that the Supervisor only request access for employees who would make frequent use of the **Internet** as a routine part of their jobs. Other authorized **Users** should support employees making only occasional use of the **Internet**.

**T-11.4. Generally Accepted Internet Policies.**

No one may participate in any activity which violates the spirit of cooperation that is the basis of the **Internet**. The individual is responsible for his/her image on the **Internet** as well as the image of the **City**. Any **Employee** of the **City** who has **Internet** access is expected to comply with this **Policy**, these use guidelines, the generally accepted **City** policies and practices of the **Internet** and the local policies and procedures that apply to a resource to which the **User** may have access.

**T-11.5. Listservs.**

A **User** enlisting their **E-mail** address into a listserv is strictly prohibited. Inundation of **E-mail** from listservs could potentially cause an overload in the **City's E-mail** system. Listservs from professional organizations and business-related topics will be considered through the individual's Supervisor.

If written approval is granted to use a listserv, **Users** must unsubscribe from the service when leaving town for an extended period of time, thus not allowing outside mail to bottleneck the **City**'s resources.

## T-12. System Security

It is the responsibility of each **User** to ensure that the **City**'s computer system is adequately protected against unauthorized access. All **Users** will use the access controls and other security measures provided and will take prudent and reasonable steps to limit unauthorized access to individual **User** accounts, such as connecting flash drives and cell phones to a computer without first getting written authorization from the System **Administrator**.

Use of computer facilities must be authorized by the account holder/**User** or by the System **Administrator**.

### T-12.1. Attacking the System

**Users** must not deliberately attempt to degrade the performance of the **City**'s computer system or subvert it in any other way. Deliberately trying to crash the system is expressly forbidden.

### T-12.2. Logging Off/Powering Off the Computer

**Users** should be aware that the system is susceptible to security breach whenever computers are left unattended or left on. Appropriate measures should be taken to protect individual **User** accounts and the entire computer system.

If you are away from your desk for 15 minutes or more, employees should log off and the system locked to restrict access. Screensavers should be password protected and self-initiate at no longer than 15 minutes. If you are going to be out of the building it is recommended logging out completely in case of power failure, etc. Leave computers on so that updates can process at night and not cause startup delays when ready to start work the next day.

### T-12.3. Passwords

Keep passwords and accounts confidential. When creating a password, **Users** should avoid using their name, name of a spouse, child, friend or pet, or a password that could easily be guessed.

The network is secure, and each **User** will have a private directory to which only they have access. For individual files that an **Employee** wishes to restrict access they should place that file in a network directory only accessible to those with permissions to view the document, such as Department Heads file would be used for Department Head files to share with those employees. Do not password protect individual files.

### T-12.4. Unauthorized Access to Files and Directories

**Users** must not engage in any activity that is intended to circumvent **City** computer security controls, including but not limited to, attempts to crack passwords, discover unprotected files, or decode encrypted files. This also includes creating, modifying, or executing programs that are designed to secretly penetrate computer systems.

**Users** must not access the accounts of others with the intent to read, browse, modify, copy, or delete files and directories unless specific written authorization has been given.

Accounts may not be used for purposes not authorized when the account was established, including personal and commercial uses.

## T-13. Online Presence

In order for the City to maintain a consistent, quality presence on the **Internet** and to assist departments in creating and publishing information on the website, the City has established web page design templates, with the **Public Information Officer** in charge of adding or subtracting information, and is the person responsible for placing information on all platforms except for police dispatch who is responsible for the police department's Facebook page and the Parks Department who is responsible for the Parks Facebook page. No other platforms will be utilized without the approval of the System **Administrator**, PIO and **City Administrator**.

Other forms of online presence include Instagram, Snapchat, LinkedIn, and Twitter, and others.

Departments are ultimately responsible for information as it appears on their web pages. The PIO reserves the right to review the website for accuracy and appearance. The PIO also reserves the right to request immediate changes or removal of pages if the content is deemed inaccurate or inappropriate for publication. In the event of a disagreement, the PIO will work with the appropriate department director to resolve the issue.

The System **Administrator**, the **City Administrator** and the Department Head will consult and determine if an individual department needs to create an online media presence, what the purpose of the online presence is, who specifically, in writing, will be responsible for information disseminated to the public (a coordinator), and how often the information will be updated. The coordinator's responsibilities should include ensuring the timeliness and accuracy of the content of the department's web pages.

Departments may not create or contract for their own web sites on a non-city server without approval of **City Administrator**.

## T-14. System Administration

### T-14.1. Computer System Settings

The computers are setup for consistency and to ease management of the network. **Users** may only change wallpaper and window colors, screen savers, toolbars and application icon locations. Items other than those specified are not to be tampered with. It is extremely important that no other changes are made to the system. All other system settings will be established and maintained by the **Systems Administrator**. This allows for a level of consistency to be created throughout the **City**'s computer system allowing for **Users** to move from one system to another and still be familiar with the software and hardware. It also creates an environment that is conducive to quick troubleshooting techniques for the System **Administrator**.

If **Users** should need assistance with changing the computer system settings specified above, see the **Systems Administrator** for help.

If **Users** share a computer with other **Users**, please be considerate of their preferences. Do not change computer system settings, etc. unless mutually agreed upon.

### T-14.2. Backup Schedules

Designated staff may complete nightly backups as identified by the **Systems Administrator**.

Nightly backups are scheduled as designated.

**Users** are asked to be logged out of the system if possible during the backup times. Failure to do this will cause files to be skipped that should have been backed up.

All servers complete a full back up on a nightly basis, with the exception of the **E-mail** server which is on a hosted web server.

### T-14.3. Preventative Maintenance

Routine preventive maintenance will be the responsibilities of the **Systems Administrator** and of the computer **User**. Dusting keyboards, screens, and the external cover of the CPU will be the responsibility of the computer **User**. It is requested that the **User** provide the above listed preventative maintenance at least once a month to their workstation. The proper supplies for these practices will be available from the **Systems Administrator**. Routine preventive maintenance will significantly increase the life of a computer and its operations.

The **Systems Administrator** will be responsible for any internal cleaning of CPU's and printers. Additional preventative maintenance is completed through an outside vendor under a bid maintenance contract.

### **T**-14.4. **Computer Supplies**

All computer supplies will be budgeted and purchased through the Supervisor to allow for better inventory control.

### **T**-14.5. **User Support**

The **Systems Administrator** is the primary support for all software and hardware issues. All questions on computer related activity should be directed to the **Systems Administrator**. If the **Systems Administrator** is unavailable or unable to assist the **User** at that time, **Users** will be referred to someone that can help within the department or tech support for certain programs.

All hardware and software issues should immediately be brought to the attention of the **Systems Administrator**. **Users** are not to try to fix hardware and software problems on their own.

Other **Users** are a means of support, however, be conscientious of time when asking others for assistance.

### **T**-14.6. **Training/Documentation Library**

Most software instruction manuals are available online with the specific computer program an **Employee** is using.

## **T**-15. Social Media

At the **City**, we understand that social media can be a fun and rewarding way to interact with family, friends and co-workers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines.

This policy applies to all employees who are employed by the **City** in any capacity.

### **T**-15.1. **Guidelines**

In the rapidly expanding world of electronic communication, *social media* can mean many things. *Social media* includes all means of communicating or posting information or content of any sort on the **Internet**, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with the **City**, as well as any other form of electronic communication. The same principles and guidelines found in the **City** policies apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved, and strictly comply with this **Policy** and any other **City** policy that may apply. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow associates or otherwise adversely affects members,

customers, suppliers, people who work on behalf of the **City** may result in disciplinary action up to and including termination.

**T**-15.2. **Know and follow the rules**

Carefully read this **Policy**, these guidelines and the Harassment **Policy**, and ensure your postings are consistent with these policies. Inappropriate postings that may include, by way of illustration and not limitation, discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

**T**-15.3. **Be respectful**

Always be fair and courteous to fellow employees, customers, board and commission members, suppliers or people who work or volunteer on behalf of the **City**. Employees have an obligation to the **City** of Harrisonville to ensure that any public communication they make, including social media communications, must not negatively impact the reputation of the **City**, fellow employees, elected officials, board and commission members, customers, suppliers, volunteers, and other people working on behalf of the **City**.

**T**-15.4. **Be honest and accurate.**

Make sure you are always honest and accurate when posting information or news and follow this **Policy** and avoid anything similar to the prohibited actions described in Section T-11.1., and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the **Internet** archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about the **City**, fellow employees, board and commission members, customers, suppliers, volunteers, and other people working on behalf of the **City**.

See Section **17.** for violation of this policy.

**T**-15.5. **Post only appropriate and respectful content.**

- Maintain the confidentiality of the **City**'s private or confidential information. Do not post internal reports, policies, procedures or other internal City-related confidential communications.
- Respect Missouri State Ethics laws.
- Do not create a link from your blog, website or other social networking site to a **City** website, unless specifically authorized in writing by the **City Administrator** under the conditions specified in that written authorization. **CityEmployee**

The policy and use of social media sites will be monitored by the authorized administrators and will be enforced by Department Supervisors.

See Section **17.** for violation of this policy.

**T**-15.6. **Using social media at work**

Employees and **Users** are prohibited from using social media while on work time or on equipment the **City** provides, unless it is work-related as authorized by your manager or consistent with this **Policy**. Do not use the **City** email addresses to register on social networks, blogs or other online tools utilized for personal use.

**T**-15.7. **Retaliation is prohibited**

The **City** prohibits taking negative action against any **Employee** for reporting a possible deviation from this **Policy** or for cooperating in an investigation. Any **Employee** who retaliates against another **Employee** for reporting a possible deviation from this **Policy** or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

**T**-15.8. **Media contacts**

Employees shall not speak to the media on the **City**'s behalf without written approval from the **City Administrator** or his/her designee. All media inquiries shall be directed to the **Public Information Officer** or the **City Administrator**.

**T**-15.9. **For more information**

If you have questions or need further guidance, please contact Human Resources.

## T-16. Cell Phones

Our **Employee cell phone policy** outlines our guidelines for using cell phones at work.

We recognize that cell phones (and smartphones especially) have become an integral part of everyday life. They may be a great asset if used correctly (for productivity apps, calendars, business calls etc.). Compensation for use of personal cell phones will be within the IRS guidelines for "substantial non-compensatory business reasons." **City** cell phones will be purchased through the System **Administrator**.

However, cell phones may also cause problems when used imprudently or excessively.

This policy applies to all our employees.

Employees who use **City** or personal cell phones for business at work will install MaaS Management Software as mandated by the System **Administrator**.

**T-16.1 Policy elements**

Despite their benefits, personal cell phones may cause problems in the workplace. Employees who use their cell phones excessively may:

- Get distracted from their work.
- Disturb colleagues by speaking on their phones.
- Cause security issues from inappropriate use of company-issued equipment or misuse of the **City**'s internet connection.
- Cause accidents when they illegally use their phones inside company vehicles or near areas where using phones are prohibited.

Our company expects employees to use their cell phones prudently during working hours.

**T-16.2 Allowed Cell Phone Use:**

Use city-issued phones for business purposes and not damage the phone.
Use city cell phone for limited personal use.
Use personnel cell phone for limited calls and city related internet use.
Surf the internet, text and talk on the phone within the plan limits per month.
To make business calls.
To use productivity apps.
To check important messages.
To make brief personal calls away from the working space of colleagues.
Employees can use their phones during breaks or at lunch hour and while on a stationary vehicle.

**T-16.3 Nonallowed Cell Phone Activity:**

Play games on the city issued cell phone at all times or personal cell phone during working hours.
Use cell phone for any reason while driving a company vehicle.
Use cell phone camera or microphone to record confidential information.
Download or upload inappropriate, illegal or obscene material on a city cell phone at any time or using a city internet connection for a personal cell phone.

**T-16.4 Disciplinary Consequences**

The **City** retains the right to monitor employees for excessive or inappropriate use of their cell phones. If an **Employee**'s phone usage causes a decline in productivity or interferes with operations, we'll ban that **Employee** from using their cell phone.

Employees may face severe disciplinary action up to and including termination, in cases when they:

- Cause a security breach.
- Violate our confidentiality policy.
- Cause an accident by recklessly using their phones.

## T-17. Violations of This Policy

Violations of this **Policy** may be grounds for corrective action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment per the **City** Personnel **Policy** or other governing policies or laws. Supervisors are responsible for the implementation and adherence of this **Policy** within their departments. If any department or division policy contradicts this **Policy**, this **Policy** shall govern.

Abuses of **City** computing resources or violations of this **Policy** will be referred to the **Employee**'s Supervisor and may be referred to the **City Administrator** for consideration under the **City**'s disciplinary processes or other appropriate remedies. Any referral may be accompanied by a temporary suspension of computing privileges awaiting the outcome of the disciplinary process or investigation. If software or files have been installed, the application or file will be immediately deleted, with no consideration of allowing time for backups or copies. In addition, Missouri and Federal laws contain specific criminal statutes with respect to improper use of computers. Therefore, inappropriate use of **City** computing resources may be subject to criminal or civil legal action in addition to **City** disciplinary action.