**CITY OF SULTAN**
**SULTAN WASHINGTON**

**RESOLUTION 20-20**

**A RESOLUTION OF THE CITY OF SULTAN ADOPTIING AN IT POLICY**

WHEREAS, the City of Sultan utilizes technology in its day to day operations of serving the community, and

WHEREAS, the use of this technology is to be used for City business, and

WHEREAS, the State Auditor encourage the adoption of written IT policy, and

WHEREAS, this policy is designed to be a document that each staff member will utilize as a framework for their day to day use of the City's technology, and

WHEREAS, this policy is a living document that we will review each year as new technology and systems evolve, and

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Sultan that the attached document entitled "Operating Reserve Policy" is hereby adopted.

PASSED AND ADOPTED this 24TH day of September 2020.

Russell Wiita, Mayor

ATTEST:

Tami Pevey, City Clerk

# ELECTRONIC COMMUNICATIONS AND TECHNOLOGY CHAPTER

Electronic communications and technology changes rapidly, with new devices and new software programs emerging every year. City staff utilizes a variety of modern communications tools in carrying out city business. These devices are useful and often essential in daily work, but in emergencies they become critically important.

This chapter is designed to provide procedures and processes that City employees will follow to protect the City's information as well the employees. With technology constantly changing the information provided within this chapter is not inclusive of all the procedures and processes employees will follow. The City asks that employees follow a commonsense approach to technology with an eye towards security.

Within this chapter technology refers to hardware and software that is owned by the City.

- Internet access, whether on a desktop PC, a laptop PC, a smart phone, a tablet, or any other electronic technology device
- Any use of a telephone (i.e., cellular, smart phone, land line, etc.)
- Any use of a fax machine
- Any transmittal of messages, information, or other electronic signals via devices owned by the City
- Any transmittal of messages, information, or other electronic signals involving or related to City business via devices not owned by the City
- Any posting of information on internet sites using City devices
- Any posting of City-related information on internet sites using devices not owned by the City.

Definitions:

Business calls: Calls directly related to City business.

Desktop PC: A computer which generally consists of a monitor, keyboard, and computer, and which is therefore not easily portable. Typically (though not always) it is linked to the internet.

Hands-free: A telephone or other electronic device designed to be operated without using the hands.

Laptop PC: A portable computer with most, if not all, of the functions of a desktop computer. May include wireless internet connectivity.

Mobile Device: Device for transmitting information and/or data from a variety of locations. It is not tethered by a cord or by the need to remain close to a short-range transmitter. Mobile device may be a computer tablet, smart phone or laptop enabled with wireless connectivity.

Personal calls: Calls not directly related to City business.

Remote Access: Ability to remotely connect to the City's network from any host. Only persons authorized in accordance with the Remote Access Section will be granted remote accessibility.

Voice Over Internet Protocol (VOIP): A method of speaking in real time over an internet connection. This is usually done via a service such as Skype, FaceTime or Google Voice, and may include voice only or voice and video connections. It may also be used for videoconferencing.

Virtual Private Network (VPN): Secure connection between two networks over a non-trusted network (such as the internet). VPNs are very useful when sensitive information must be transmitted or received over the Internet. VPN prevents third parties from reading or modifying the information in transit. The connection is controlled and secured by the software installed at the connection end-points. This software implements authentication, key exchange, and data encryption according to standards. Authorization for VPN access is limited and available only for those authorized in accordance with the Remote Access Section.

This chapter is broken down into the following sections:

- Use of City devices, ranging from computers, to laptops, to cellphones
- Sensitivity of information and the public records act
- Passwords, their complexity and how often they should be changed, and who has access to them?
- Vendors access to the City's information
- Use of Springbrook, the City's financial software and other programs like Office 365 and Aktivov. Who has access and why?
- The process the City follows when an employee leaves the City
- Authorities within the City's systems. Who has and who does not have the authority to manage the City's electronic data?
- Compatibility of hardware and software
- Remote access policy
- Shared Drive and folder, process for saving documents and sharing them
- Audit reviews of Springbrook activity. Who reviews what

**Use of City devices, ranging from computers to laptops, to cellphones:**

The City issues devices to all its employees. These range from computers, to laptops to cellphones, to iPads. These devices are to be used for City business and the content on them is subject to the Public Records Act.

Some of these tools and devices have the potential for personal use, and many employees own similar devices. Yet a City provided device will be used for City business and a personal device used for an employee's personal use. It is important that each employee who is issued a device treat it with the same respect they would their own device. In addition, it is important to protect

the device from theft and damage. The following rules apply to employee use of City-owned wireless devices, or the use of employee-owned devices while conducting City business:

- Wireless communication devices shall not be used while driving unless they are handsfree. To make or receive calls or text messages, or to access or view data while in a vehicle, the vehicle must be parked. Even hands-free devices can be a distraction from safe driving and should be used minimally and only when necessary for legitimate business purposes.
- The display or transmission of any message or image that contains ethnic slurs, racial epithets, or anything that is harassing or disparaging of others based on their race, national origin, sex, sexual orientation, age, disability, religious, political beliefs, or any other protected class, is not permitted on City-owned devices. This applies before, during or after business hours, and applies whether or not on City property.
- The display or transmission of sexually explicit images, messages or cartoons on City owned equipment (unless a job requirement) is not permitted. This applies before, during or after business hours, and applies whether or not on City property.
- Employees shall use care and common sense with open websites, especially when visitors are in the area, to avoid inadvertent offense.
- The display or transmission of any political message or image for the purpose of lobbying or endorsing a candidate or political message is not permitted on City-owned devices. This applies before, during or after business hours, and applies whether or not on City property.
- Solicitation, promotion, or advertising of any organization, product or service is not permitted on City-owned devices. This applies before, during or after business hours, and applies whether on City property. The only exceptions are for activities that are clearly part of or supportive of official City business, or promotion of a charitable effort as endorsed by the City.
- Using appropriate sites for business purposes is unrestricted as long as it is reasonable.
- Downloading or copying from any device or service including the internet should be done with caution as it confers potential risk to the City. Data storage is a potential problem; therefore, the amount of downloaded material should be kept to a minimum.
- The City has the right and capability to monitor internet browsing by each user on its system. However, the City's goal is that employees will make this unnecessary.
- The City does not endorse personal electronic mail or other personal data on City devices. Recognizing that it may occur occasionally, it is to be kept to a minimum; personal electronic mail should be sent or received seldom and should be as brief as possible. Personal correspondence and data on City equipment is subject to review in response to public records requests.
- The City reserves the right to determine when an employee is accessing or transmitting inappropriate types or amounts of images or messages.

**Sensitivity of information and the public records act**

By using the City's technology systems, employees acknowledge and agree that they have no expectation of privacy or confidentiality in their use of these systems or in any data that they create, store, or transmit on or over the systems, including any data created, stored or transmitted during an employee's incidental personal use of the City systems as permitted under this section.

To ensure appropriate use, employees' use of the systems may be monitored and any data that they create, store, or transmit on or over City systems may be inspected by City management at any time.

Employees should understand that certain email messages, other electronic communications and documents created on City computer systems (to include printers, copiers, scanners, fax machines, etc.), or on personal devices where it relates to City business, may be considered a public record subject to disclosure and/or subject to discovery in the event of litigation.

Costs.

Expenses incurred for the purchase and use of City-owned devices should be billed directly to the City. Expenses incurred for the purchase of employee-owned wireless communication devices and airtime usage should be billed directly to the employee.

Equipment.

To preserve the integrity and security of City technology, the following rules must be observed:

- All mobile devices connected to the City network shall comply in total with the City's standards for hardware and software.
- The City has the right to require the removal of specific software or files from any device connecting to the City's network.
- City-owned devices are assigned to a specific position and the employee in that position is responsible for the device(s). When an employee for which a device was approved has left their position, the device, software and accessories will be returned to that position's manager/supervisor.
- All devices connected to the City network environment shall have password, PIN, or other access protection enabled.
- All City-owned devices may be inspected for existence of unauthorized use or organization data and security compliance.
- All non-City owned devices (e.g., personal iPhone) must be compatible as determined by the City prior to being used to access City information.

The public records act is designed to provide a portal for individuals and businesses access to the City's information. That is why it is important that employees think about what they are writing or doing and how it is a public record that can be requested. Therefore, employees need to think about what they do or say when utilizing a City device.

**Passwords, their complexity and how often they should be changed and who has access to them**

The City utilizes Office 365. It is a web-based platform for the suite of Microsoft Office products. Since employees can access their email and files remotely, it is critical that they protect their passwords. These passwords should be protected by the employee and changed every 90-days. These passwords are not stored by any employee and there will not be a database of passwords saved by any employee.

Employees must observe the following rules and guidelines to protect City systems and the confidentiality of information on City systems:

- Passwords are an important aspect of computer/data security. All City employees, interns, temporary employees, volunteers, as well as contractors and vendors with access to City systems, are responsible for selecting strong passwords, changing them frequently and keeping them secure.
- Do not use the same City password for other non-City access; keep City passwords different from personal passwords.
- Passwords are to be treated as sensitive, confidential information. Strong passwords must follow the following characteristics:
    - Contain upper- and lower-case characters (i.e., a-z, A-Z)
    - Contain digits and punctuation characters (i.e., 0-9, $%(*!}>+)
    - Contain at least 8 characters and must contain at least one small letter, one capital letter, one number, and one punctuation character, is not a word in any language, slang, dialect, jargon, etc.
    - Is not based on personal information, names of family, etc.
    - Create passwords that can be easily remembered
- Invasion of the City's mail system by viruses is a daily risk. Users must remain aware of all policies and procedures that are published to assist in the prevention of virus attacks or improper entry into the data systems. Attempting to disable any security or monitoring tools without City approval is not allowed.
- Electronic mail is a City asset and is subject to review or monitoring at any time without notice by designated IT personnel.
- IT Consultant will provide support for installation of City standard software in connection with City-owned devices. Support for hardware will be coordinated with the hardware vendor.

The City has two administrators who have access to the system. They are the City Clerk and the City Administrator. The City does have an IT consultant that works with employees on a wide range of software and hardware needs. The IT consultant does not have access to the employee's passwords, yet he can assist the employee with resetting their password.

**Vendors access to the City's information**

Time to time, the City retains the services from different vendors. These range from consultants to contractors who work on a variety of projects and programs. These vendors have limited access to the City's systems. Who is granted access is dependent on the tasks they have been

hired to perform. Example, a finance consultant will only have reporting access to the City's financial software Springbrook. In other cases, vendors are not given access to the City's system.

**Use of Springbrook, City's financial software and other programs like Office 365 and Aktivov**

The City has a variety of software programs that help with the different functions of the City. Each of the programs is assigned to specific users. Each user is granted access based on their job function. Example, the Finance Director has access to Springbrook to handle the day to day functions of the City's finances. That employees' level of access is different than the utility billing specialist or the City Clerk.

With respect to Office 365, each employee is given a username and they need to establish a password. Each employee is responsible for the privacy of their passwords and these passwords are not shared with other employees.

With respect to Aktivov. This program is used by the utility department. Certain Public Works and Finance employees utilize this program and have access to it. Employees in other departments do not have access, because they do not work on the utilities.

The job function of the employee determines their access and authority within the different systems. In addition, there are checks and balances within the system. These range from secondary reviews to approvals. Each year the City reviews the job functions and makes any changes it needs to based on the need for access and authority.

**The process the City follows when an employee leaves the City**

Employees leave the City voluntarily or under the direction of the City Administrator. Either way the process the City follows is the same.

When an employee leaves, the City Administrator meets with the employee and obtains all the equipment they were assigned. The Administrator then reaches out to the IT consultant who will shut off their access to Office 365, which includes their email. If the employee has access to other systems, such as Springbrook, the administrator will revoke their access.

**Authorities within the City's systems. Who and who does not have the authority to manage the City's electronic data**

Within the City's systems there are levels of authority granted based on the roles and responsibilities employees have. The highest level of authority is granted to the City Administrator. This role is the administrator to Office 365 and Springbrook. The next level of authority are the department heads. They have read write authority within the different systems, but they cannot add or delete a user.

The third level are the employees and as described in a previous section, their access is based on the job duties. The department director that they report to, is the secondary reviewer except for Springbrook and the Finance Director. The secondary review is either done by the City Administrator or the Deputy Treasurer.

**Compatibility of hardware and software**

The City's IT consultant will work with the City Administrator and the department directors on different needs that arise. The goal of any hardware and software is that it must be compatible with the existing systems.

When a department director sees the need for new hardware or software, they must take the following steps to assure they would be compatible with the existing systems.

- The hardware or software must meet a need that an existing system does not offer
- The IT consultant needs to report to the Administrator that the purchase is compatible with existing systems
- The hardware or software needs to provide a direct benefit to the City

Once these questions have been answered, and the budget exists for the purchase, the department director with approval from the City Administrator or elected body, can purchase the system.

**Remote Access Policy**

The purpose of this section is to define requirements for connecting to the City's network (or any network managed by the City) from an external entry point. These requirements are designed to minimize the potential exposure to the City from damages which may result from unauthorized use of the City's resources. Damages include the loss of sensitive or confidential information, damage to public image and damage critical to the City's internal systems.

Applicability.

This section applies to all City employees, contractors, vendors and agents with a City-owned or personally owned device(s) used to connect to the City's network. This section applies to remote access connections used to perform work on behalf of the City, including reading or sending email and viewing internet web resources.

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

Definitions.

Cable Modem: Cable companies provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the internet.

Dial-in Modem: A peripheral device that connects computers to each other for sending communications via the telephone lines.

Digital Subscriber Line (DSL): A form of high-speed Internet access competing with cable modems.

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device. Examples include being logged into the City network via a local Ethernet connection, and dialing into some other Internet Service Provider (ISP).

Mobile Device: Device for transmitting information and/or data from a variety of locations. It is not tethered by a cord or by the need to remain close to a short-range transmitter. A mobile device may be a computer tablet, phone or laptop enabled with wireless connectivity.

Remote Access: Ability to remotely connect to the City's network from any host. This includes, but is not limited to, an employee accessing the City's Outlook system while away from work. Only persons authorized in accordance with this section will be granted remote accessibility.

Split Tunneling: Simultaneous direct access to a non-City network (such as the internet, or a home network) from a remote device (PC, iPhone, etc.) while connected into the City's network via a VPN tunnel.

Voice Over Internet Protocol (VOIP): A method of speaking in real time over an internet connection. This is usually done via a service such as Skype, FaceTime or Google Voice, and may include voice only or voice and video connections. It may also be used for videoconferencing.

Virtual Private Network (VPN): Secure connection between two networks over a non-trusted network (such as the Internet). VPNs are very useful when sensitive information must be transmitted or received over the Internet. VPN prevents third parties from reading or modifying the information in transit. The connection is controlled and secured by the software installed at the connection end-points. This software implements authentication, key exchange, and data encryption according to standards. Authorization for VPN access is limited and available only for those authorized in accordance with this section.

Wi-Fi: Wireless networking technology that uses radio waves to provide wireless highspeed Internet and network connections. A Wi-Fi enabled device such as a PC or cell phone can connect to the Internet when within range of a wireless network.

General Information

Only approved City employees and authorized third parties may be granted remote access to the City's network. To receive approval for remote access, an employee must obtain approval from their manager and/or director. Upon approval by the employee's department, the request for remote access will be forwarded to the IT Department for appropriate device deployment, set up, and/or approval of non-City owned devices. Once approved, remote access usage is subject to the following:

- It is the responsibility of City employees, contractors, vendors, and agents with remote access privileges to the City's network to ensure that their remote access connection is used in accordance with the City's network section.
- General access to the internet for recreational use by the employee or immediate household members through the City's network on personal computers or devices is not permitted. The City employee bears responsibility for the consequences should access be misused.
    - At no time should any user covered under this section provide any City login or password credentials to anyone, not even family members.

- Authorized users with remote access privileges to the City's network must not use non-City email accounts (e.g., personal Hotmail, Gmail) or other external resources to conduct City business.

**Shared Drive and folders, process for saving documents and sharing them**

The City has a shared drive that all employees have access to. The drive is designed as a library of information that employees can utilize to locate past documents, save new documents and store images of different projects or programs. Within this server there are many folders. Some are organized by department and others by project or program.

The shared drive is to be utilized for City business only. Employees are not to store personal information or information that is not related to the City on the shared drive. In addition, the shared drive is subject to public disclosure requests. All employees need to be professional in the documents they write and store on the shared drive.

Once a year a committee of City employees will review the documents within the drive and determine which ones can be deleted and which ones need to be saved. This committee will also develop a process so only one copy of a document remains.

**Audit reviews of Springbrook activity**

Secondary reviews of the activity within Springbrook is critical. Each month the Finance Director and the City Administrator will review the previous months activity as well as any adjustments within the system.

Once a year, prior to the City submitting its annual report, a review of the City's financials by an independent entity will occur. The individual or organization will review the years financials and any adjustments, reconciliations or changes to the year's financials. The entity will submit a report to the Mayor and City Administrator on their findings.

This chapter within the personnel policy is designed as a guideline for employees to follow. It is not comprehensive of all the situations or issues that may arise. Each year the City Administrator with the help of the IT consultant and department heads will review the policy and make any adjustments.