CITY OF CRESTVIEW			
Policy Name: IT/IS		*Policy Number: 20-01*	*Date: 01/01/2021*
	POLICIES & PROCEDURES MANUAL DEPT: Finance	*Section: Administrative Services*	*Department Head: Leavins*
		Subject: Information Technology and Systems Policy	*Approval:*
	Revision Dates:		

Policy

A. This Policy governs the use of the Technology resources owned and operated by the City of Crestview by employees, volunteers, vendors, contractors and all other authorized users. Technology includes, but is not limited to, desktops, laptops, mobile devices, networking equipment, networked devices, servers, software, electronic mail, phones, cellular phones, control systems, Internet, Intranet, and all other Enterprise electronic systems or devices.

B. The Information Technology Division (IT) shall establish and maintain specific rules and requirements relating to the safe and secure operation of all devices and the storage of data while connected to City resources. Adherence to these standards is a requirement for all persons utilizing City-owned devices or storing and accessing data on city technology infrastructure. These standards shall be amended as necessary to remain current with various needs and risks and are included in this policy by reference. Failure to comply with these rules and requirements shall be considered an improper use.

II. Definitions

A. For the purposes of this Policy and Procedure, the following definitions shall apply:

1. Improper Material - Pictures, posters, calendars, graffiti, objects, promotional materials, reading materials, or other materials that are racist, sexually suggestive, sexually/racially demeaning, pornographic, offensive, intimidating, harassing, disparaging, and/or hostile on the

basis of age, disability, gender, national origin, race, color, religion, or any other legally protected characteristic.

2. IT Manager - The Manager of the Information Technology division of the City of Crestview.

3. Department Head/Department Director - The head of an administrative department of the City of Crestview, or designee.

4. Employee - For the purpose of this policy, an employee is defined as an individual employed by the City on a full-time, part-time, seasonal, temporary or internship basis.

5. Mobile Device - Means a device intended to be portable, carried on one's person, or readily moved from location to location, such as smartphones, cell phones, radios, pagers, laptops, tablets, and others.

6. Authorized user - An authorized user is a current employee, contractor, vendor, or other party who has been granted lawful access by the IT Manager to the City of Crestview network, applications, or services.

III. Procedures

A. Applicability

1. This policy shall apply to all City employees, volunteers, vendors, contractors, and other authorized users as defined herein. Departments may develop departmental policies and procedures which provide greater direction to their employees, as long as that direction is consistent with the City's interdepartmental policy and procedure.

B. Authorized Use

1. The City electronic communications and technology resources are provided for the purpose of conducting City business. Personal usage is permitted, as long as the personal use is reasonable and prudent. Responsibility and accountability for the appropriate use of City electronic communication and technology resources ultimately rest with the individual employee.

2. Improper use of the City's electronic communications and technology resources may result in disciplinary action, up to and including termination.

C. Privacy

1. No user accessing or using computers or telecommunications resources owned and/or operated by the City of Crestview can have any expectation of privacy. The City of Crestview reserves the right to monitor, intercept, archive, view, or distribute any communications and/or content transmitted over resource which it owns, leases, or operates subject to all applicable laws.

a) IT Staff may be required to access any and all material located on those resources.

b) Department Heads may monitor employee use of the Internet and email, and may revoke an employee's access to the Internet and/or email by notifying the IT Manager.

c) Authorized users must be aware that any digital record residing on a city-owned device may be subject to lawful open records requests. In addition, any data regarding City business stored on a personal device or file sharing service is also subject to lawful open records requests.

d) The department to whom an electronic device has been issued is responsible for all costs associated with the damage or loss of any device which has been issued by the IT department. See III, I, 6 for clarification on mobile device repair and replacement.

D. Resource Access Requirements

1. Work Product

a) No employee shall use the Internet or e-mail to present his or her own personal views, ideas, questions, or actions, as

representing the positions or policies of the City unless

doing so in an official capacity and authorized by the City Manager or his/her designee.

b) Unless otherwise specified by contract, any work produced by a vendor, contractor, or other third party acting as an agent, consultant, or contractor to the City, is the property of the City, and employees shall take steps to ensure that such property is properly stored on City resources to prevent loss.

c) No employee shall use any City-owned equipment or resources in violation of any applicable law.

2. Identity

a) Each person authorized to access the City of Crestview's computer and network resources must do so using a unique user name (login name) assigned by the IT Division. The use of group accounts will be limited to only those circumstances approved by the IT Manager. Employees shall not share their account information, or permit other employees to log in using their credentials excepting properly identified members of the IT Division. Electronic communications authored by the employee must clearly originate from the user's unique account.

3. New Employees

a) It is the responsibility of each department to notify the IT Division at least five working days prior to the start date of any new employee or authorized user who needs access to the City's electronic resources, so that appropriate access can be provided on a timely basis.

b) New employees must receive a copy of this policy, and acknowledge that they have read, and will adhere to, the contents of this document.

c) It is the responsibility of each department to immediately notify the IT Division in the event of the termination, resignation, or retirement of any employee within their department who previously had access to City computers

and/or network resources, so that such employee user accounts may be removed.

4. Remote Access to Resources – The City maintains various systems to permit users to access internal systems from non-secured locations, like the Internet. These services are intended to augment the productivity of employees.

   a) Employees must take extra precautions when accessing City resources from non-city devices. The use of a virus scanner is required.

   b) It is the responsibility of the employee using the remote access facility to ensure that unauthorized persons cannot utilize their account to gain access to City resources. Employees are not to provide their passwords to anyone, including family members.

   c) Users must understand that using their personal device or computer to access City resources may impose a possibility of open records access responsibility. This means you may be required to provide records from your personal device or submit your personal device to a search for either an open records or legal request if it accesses City systems.

   d) Unless specifically authorized by their department head, non-exempt employees may not use electronic devices to conduct City business outside their normal working hours.

5. Data Storage

   a) Employees should not store information exclusively on the local drive (C:, D:, etc.) of a PC or laptop or tablet. By storing the file outside of network or cloud storage provided by the City, the data is neither searchable nor backed up. Employees are instead required to utilize network drives, City-provided cloud storage, such as Microsoft OneDrive and SharePoint Online, or City-owned content management systems for the purposes of data storage.

E. Internet - It is the policy of the City of Crestview to offer connectivity to the Internet for employees requiring its use as a part of their normally assigned duties. The purpose of this policy is not to discourage the use of the Internet, but to provide a uniform approach

to the usage of this

resource, to safeguard City interests in the use of the Internet, to meet all applicable laws, and to protect the assets attached to City networks from unauthorized access. The City of Crestview reserves the right to monitor all Internet usage on City-owned and City-connected devices including reviewing all sites that are viewed by the employee's browser and the amount of time spent at each site.

1. Appropriate Uses of Internet Resources - All City-owned Internet resources are to be used only in the pursuit of appropriate city business interests.

2. Bringing improper material into the work environment or workplace, or possessing any improper material at work to read, display, or view at work, or otherwise publicizing it in the work environment is prohibited.

3. No employee shall connect to any web site that contains improper material (Exception: sanctioned CPD employees performing assigned investigative work). The city reserves the right to block employee access to such web sites.

4. No employee shall operate or advertise any non-city business on the Internet using City equipment at any time.

5. No employee shall send chain letters, pyramid schemes, or unsolicited bulk email using City equipment at any time.

6. No employee shall use official City email addresses to distribute jokes, virus warnings, sentimental missives, rumors, political commentary, or other non-work-related material to other employees or the general public. (NOTE: Only IT employees and PAMRO, acting in their official capacity, are to transmit virus warnings.)

7. Personal email messages or other non-city related usage of Internet resources should be held to a minimum, as with telephone calls. Personal Internet usage or usage of electronic devices should not impede the conduct of City business; only incidental amounts of employee time comparable to reasonable coffee breaks during the day should be used to attend to personal matters. Questions regarding the extent of this policy should be discussed with departmental supervisors. Personal use of Internet resources is a privilege, not a right. As such, the

privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action.

8. All employees shall use only their city-assigned email address during the performance of their assigned job duties. No private or "ghost" accounts shall be used, except by network administrators as part of their function (e.g., account names like "Webmaster," "Postmaster," "root," etc.) and special investigations. All requests for exceptions to this policy must be approved by the Department Head.

9. Email received from citizens should be handled with the same seriousness as any other form of citizen contact. Employees should always maintain professional decorum in their responses, seek approval from supervisors where appropriate, and reply to messages promptly.

10. Unless specifically approved by the IT Manager, all Internet email transmissions shall be routed though the official City gateway service (Exception: sanctioned CPD employees performing assigned investigation work). No department or employees shall operate within City networks any email servers, mail forwarding services, or other email transmission or reception services for use by any person or automated system.

11. Internet traffic will be filtered to prevent access to inappropriate sites and those deemed detrimental to network services.

F. Personal Device Usage

1. The City of Crestview reserves the right to disconnect, or prevent connection to City network resources of any device, by any user, at any time, or for any reason, without any notice whatsoever.

2. The employee attaching their personal device to a City network resource assumes full liability for any risks, including, but not limited to, partial or complete data loss, errors, bugs, hardware loss or damage, viruses, malware, or any other issue which may damage the device, in any way whatsoever. The employee assumes all risk by connecting to the resource.

3. The IT Manager, or designee, shall be solely responsible for determining which devices may be connected to City resources.

Employees should contact the IT Help Desk to determine

whether their device is eligible, and to obtain proper user credentials for their device.

4. Support - The IT Division will provide support for network connectivity issues. However, hardware and software support for personal devices will not be provided.

5. Reimbursement - Connection to City-owned network resources is provided to employees as a convenience only. The City will not reimburse any expense, partial or otherwise, for any usage of a personal device, including cell phones, regardless of purpose.

6. Personal Device Security

   a) In order to prevent unauthorized access to City resources, personal devices must be password protected with a strong password or key code. Access to City resources will be denied if this protection is disabled or not present.

   b) Employees that use personal devices for city purposes including but not limited to placing calls or receiving/sending text messages, must sign the attached memorandum of understanding as related to public records law.

   c) Users of personal devices must follow all City policies with respect to acceptable use while attached to City network resources.

   d) Employees must be aware, that the conduct of City business, or use of City data on any personally owned device, may expose that device and the employee to legal obligations with respect to Florida public records laws.

e) Smartphones and tablets belonging to employees that are for personal use only are not allowed to connect to the network unless given an exception in writing by their Department Head and the IT Manager or designee.

f) Employees are not automatically prevented from downloading, installing and using any app, but may be asked to remove apps that have the potential for creating a risk for which the City would become liable.

g) The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the City's data and technology infrastructure.

h) The employee is responsible for backing up all data on their device.

G. Communications Network

1. No employee or other person shall install or move any network device onto the City communications network under any circumstances whatsoever. Only members of the IT Division are permitted access to such equipment.

2. No employee, contractor, or third party may install any device or software intended to monitor, capture, or eavesdrop upon, any portion of data traversing the City Network, excepting members of IT.

3. Employees shall not attach any form of personal network equipment including, but not limited to, switches, routers, or modems to any City network.

4. No employee will permit any third party to connect any device to any Ethernet jack or secure wireless service without the express permission of the IT Manager or designee, unless service is specifically provided for such purpose.

5. No employee shall install or operate any equipment or service which has the effect of redirecting or proxying any network traffic to or from any other network, or disguising the source of any network transmission.

H. Software

1. The City is committed to preventing copyright infringement. It is the policy of the City of Crestview to respect all computer software copyrights and to adhere to the terms of all software licenses to which the City is a party. The City is subject to all copyright laws pertaining to the use of copyrighted software and documentation. Unless expressly authorized by the software licensor/developer, the City of Crestview has no right to make copies of the software except for backup or archival purposes.

2. All software used on a City computer must be licensed to the City for that computer.

3. Employees may not install any software not provided to them by the IT Division without specific authorization by the IT Manager or designee.

4. City employees shall not duplicate, copy, or reproduce any software purchased by and/or licensed to the City, or any related documentation without prior written approval from the IT Manager. City employees shall not give City-purchased or licensed software to any non-employees, including, but not limited to clients, contractors, customers, and others without prior written approval from the IT Manager.

5. Software developed by employees on City time, or on City-owned equipment, or for City projects, shall be the property of the City. Such software is for the exclusive use of the City, its officers, agents, and employees. Such software may not be sold, transferred, or given to any person without the prior written approval of the City Manager or designee.

6. Software must be registered in the name of the City and the Department in which it will be used. Software shall not be registered in an individual employee user's name.

7. Game software is an inappropriate use of City equipment and shall not be tolerated on desktop PCs. Games discovered during audits shall be eliminated and the employee user may be subject to disciplinary action.

I. Mobile Devices, Cellular Telephones

1. Eligibility Criteria – Employees eligible for assignment of City owned mobile devices are those designated by the City Manager, and/or department directors, including (but not limited to):

   a) City Manager's office staff, department directors and employees who are frequently in the field, if the individual must conduct City business by telephone or mobile application in the field and it can be shown that the cost savings and customer service efficiency will be realized through the use of such devices;

   b) City Manager's office staff, department directors and employees who have a critical need to maintain accessibility with other department managers, City management staff and public officials, in order to insure uninterrupted customer service and/or the integrity of the organization; public safety positions and vehicles in order to provide immediate and direct communications with citizens, outside agencies cooperating in operations, or other resource entities outside of City government and to provide for communications which may be inappropriate for mobile radios;

   c) All employees involved in the City's emergency response plan;

   d) Department directors and employees who have responsibility for responding to public safety incidents in the field.

2. Responsibilities of City Management and Department Heads - The City Manager and/or Department Heads are responsible for:

   a) Approving requests for cellular telephones, electronic paging devices, and other wireless communications devices from their respective subordinates;

   b) Insuring that requests are in conformance with the procedures outlined herein, or that exceptions are justified;

c) Insuring that all persons assigned a City-owned cellular telephone, electronic paging device, and/or other wireless communications device, are provided access to a copy of this Policy and Procedure, and that the individual is in compliance with it;

d) Conducting periodic inventories of cellular telephones, electronic paging devices, and other wireless communications devices within their respective departments to insure accountability;

e) Conducting annual reviews of assigned devices to determine if such assignments continue to be justified; and;

f) Informing appropriate employees responsible for City communications of all reassignments of cellular telephones, electronic paging devices, and/or other wireless communications devices.

3. Responsibilities of Employees - Employees who are assigned the use of City-owned cellular telephones, electronic paging devices, and/or other wireless communications devices are responsible for the following:

a) Insuring the physical security of such devices, including the active use of passcodes, passwords, and prevention of misuse by others.

b) Insuring that any personal use does not detract from the employee's availability for completion of assigned duties.

c) If non-exempt, employee and supervisor must read and sign the procedures related to compensating Non-Exempt employees for phone usage time outside of the standard work schedule, as indicated in Exhibit A.

4. Mobile Device Management – In order to safeguard City-owned property, and to prevent breach and/or loss, the City may install device management software on any or all city-owned mobile devices, to include emergency locators, remote device disable, device wipe, and other functions as deemed necessary by the IT Manager. No city staff will have authority to track the location of the device except in the case of a lost asset or an active HR

investigation. There is no expectation of privacy for any communication had on a city device.

5. Requests for new mobile devices must be made using the online or physical request form by the Department Head or designee of the employee requesting the phone. Once approved by the Administrative Services Director, the request will be provided to the IT Manager. The device will then be provisioned for the employee.

6. All Non-Exempt employees and their immediate supervisor must agree to the procedures related to compensating non-exempt employees for phone usage time outside of the standard work schedule, as indicated in Exhibit A.

7. Termination – Upon termination of employment, employees are required to provide the device to IT no less than three (3) business days prior to the employee's termination date. This allows IT to verify the device can be unlocked, wiped and provisioned to another employee. In the case a device is not returned or is returned but is unable to be unlocked and wiped (due to PIN, Google/Apple account lock, etc) the cost of a replacement device may be withheld from the employee's final paycheck.

8. Unreturned assets – If a mobile device is not returned to the IT Division or it is unable to be unlocked within five (5) business days after the employee's termination date, the cost of a replacement device will be deducted from the final paycheck. The City will not accept a device or provide a refund back to the employee once the final paycheck has been processed.

J. Security - It is the responsibility of every employee to operate all City telecommunications, computer, or other electronic equipment in such a way as to minimize the risk of unauthorized access to, or loss of, any City resource by any other party, to ensure that City resources are not

misused by any other person, and to act so as to protect the integrity of the data and resources of the City.

1. Password Policy - Each City employee (who uses computers) must have a unique password.

    a) Passwords may not be written down where they can be found by unauthorized personnel or be shared with other individuals. It is the responsibility of the employee to maintain the secrecy of their passwords.

2. All employees shall immediately report any unauthorized access or unauthorized access attempt, virus infection, spyware infection, or other unauthorized or illegal resource use to the IT Manager or his designee.

3. Employees shall not download or install any software of any kind whatever from the Internet or any storage device or media to any City-owned computer without the prior consent of the IT Manager.

K. Technology Procurement

1. Departments will coordinate all technology or software related purchase requests (including grant proposals, RFPs, bids, contracts, purchase orders, and City credit card purchases) with the IT Manager or designee verbally or in writing prior to purchase. The purpose of this review is:

    a) To ensure that the product(s) obtained are compatible with City standards and existing infrastructure;

    b) To avoid unnecessary and costly duplication of capabilities;

    c) To minimize impacts on support personnel;

    d) To ensure all costs are properly considered; and

    e) To ensure that the proposed equipment or software does not interfere with the operation of existing systems, or create any undue risk to City resources.

    f) Departments will involve the IT Division in the earliest planning stages of any grant proposal, RFP, bid, contracts,

or purchase, etc., which will result in IT related services or products being obtained, prior to the submission of any request to the Finance department or City Council.

EXHIBIT A

City Issued Mobile Devices, Cellular Telephones, Cloud Files and Email Access

Procedures for Compensating Non-Exempt Employees

In order to meet City-wide operational demands, non-exempt employees can access Email and files remotely from the cloud (e.g. Office 365) and some are issued smartphones for business use. The intended use of the phone and cloud files/email is to provide an employee who is regularly working in the field or away from the office, the ability to maintain connectivity and responsiveness during their regularly scheduled work day. The access also allows for pre-approved (by supervisors) monitoring of calls, voicemail, and/or email outside of the regular work schedule. It is essential that monitoring of the phone or access of email outside of work hours is pre-approved because it may result in over-time. It is strictly prohibited for employees to use the City-issued smart phone or access cloud resources outside of their regularly scheduled work day unless they have been instructed by their supervisor to do so, including access of email, voicemail or text messages. Supervisors should limit the number of employees and length of time that employees spend using mobile devices or cloud data outside of regularly scheduled hours. The employee must notify the supervisor the following work day if there was unauthorized use of their City data outside of the standard work schedule in order to properly account for the employee's time. If a non-exempt employee has unauthorized use of their City data, the employee may be subject to disciplinary action up to and including termination.

If a non-exempt employee is instructed or allowed in advance to monitor smartphone voicemails and emails outside of his/her regularly workday, the time spent conducting that task will be considered compensable work hours. All of this type work should be recorded. Employees should log all work performed with a smartphone or access of cloud email/data outside of their regular workday in the following manner:

- Weekly log – Saturday through Friday
- Date and time of work
- Length of time work is performed
- Purpose of work
- Total weekly time using a City-issued smartphone worked outside of regular workday

The log should be submitted to the supervisor at least one time per week (supervisors have the discretion to require the log more frequently). All total weekly time using a city issued smartphone or accessing City cloud data

EXHIBIT A

City Issued Mobile Devices, Cellular Telephones, Cloud Files and Email Access worked outside of the regular work day should be totaled, (rounded up to the nearest 15-minute increment), and recorded at the end of each work week.

In order to reduce additional communication outside of regularly scheduled worktime, employees should ensure outgoing voice messages on phones and out-of-office designation on emails are kept current and contain information that may provide an alternative contact person that is in the office or is the designated on–call contact. Use of smartphones for business use outside of employees' regular work schedules should be limited to critical communication and requires pre-approval by a supervisor.

I have read, understand, and will comply with the City Cell Phone and Cloud Data Usage for Non-Exempt Employees.

Employee	Date
Supervisor	Date