RESOLUTION 2015-54

A RESOLUTION OF THE MAYOR AND COUNCIL OF THE TOWN OF FOUNTAIN HILLS, ARIZONA, ADOPTING AMENDMENTS TO THE TOWN OF FOUNTAIN HILLS PERSONNEL POLICIES AND PROCEDURES, AMENDED AND RESTATED AUGUST 1, 2013, RELATING TO THE INFORMATION TECHNOLOGY POLICIES, VACATION LEAVE POLICY AND PERSONAL LEAVE POLICY; AND DECLARING AN EMERGENCY.

WHEREAS, the Mayor and Council of the Town of Fountain Hills (the "Town Council") approved Resolution No. 2013-39, adopting the Town of Fountain Hills Personnel Policies and Procedures, Amended and Restated August 1, 2013 (the "Personnel Policies"); and

WHEREAS, the Town Council desires to amend the provisions of the Personnel Policies relating to (i) Vacation Leave, (ii) Personal Leave, and (iii) Electronic Mail and Scheduling System, Internet Use, Use of Electronic Devices, iPad/iPhone, and Social Media Policies.

NOW, THEREFORE, BE IT RESOLVED BY THE MAYOR AND COUNCIL OF THE TOWN OF FOUNTAIN HILLS as follows:

SECTION 1. The recitals above are hereby incorporated as if fully set forth herein.

SECTION 2. The Vacation Leave Policy of the Personnel Policies is hereby deleted in its entirety and replaced with the amended Vacation Leave Policy attached hereto as Exhibit A and incorporated herein by reference.

SECTION 3. The Personal Leave Policy of the Personnel Policies is hereby deleted in its entirety and replaced with the amended Personal Leave Policy attached hereto as Exhibit B and incorporated herein by reference.

SECTION 4. The Electronic Mail and Scheduling System, Internet Use, Use of Electronic Devices, iPad/iPhone, and Social Media Policies of the Personnel Policies are hereby deleted in their entirety and replaced with the Acceptable Use of Information Systems, Intranet/Internet and Email, Software/Hardware, and Audit of Information Systems Policies, attached hereto as Exhibit C and incorporated herein by reference.

SECTION 5. The immediate operation of the provisions hereof is necessary for the preservation of the public peace, health and safety and an emergency is hereby declared to exist, and this Resolution shall be in full force and effect from and after its passage by the Town Council and it is hereby exempt from the referendum provisions of the constitution and laws of the State of Arizona.

SECTION 6. The Mayor, the Town Manager, the Town Clerk and the Town Attorney are hereby authorized and directed to take all steps necessary to carry out the purpose and intent of this Resolution.

[SIGNATURES ON FOLLOWING PAGE]

PASSED AND ADOPTED by the Mayor and Council of the Town of Fountain Hills, December 17, 2015.

FOR THE TOWN OF FOUNTAIN HILLS:

Linda M. Kavanagh, Mayor

ATTESTED TO:

Bevelyn J. Bender, Town Clerk

REVIEWED BY:

Grady L. Miller, Town Manager

APPROVED AS TO FORM:

Andrew J. McGuire, Town Attorney

EXHIBIT A
TO
RESOLUTION 2015-54

[AMENDED VACATION LEAVE POLICY]

See following pages

Town of Fountain Hills
Personnel Policies and Procedures

SECTION: FRINGE BENEFITS AND LEAVES
POLICY: VACATION LEAVE
POLICY NO: 903
EFFECTIVE: DECEMBER 17, 2015
REVISED: DECEMBER 17, 2015

PURPOSE: To establish the means by which Town of Fountain Hills employees may earn and use vacation leave and to provide for the compensation of unused vacation leave upon separation from Town service.

STATEMENT OF POLICY: Vacation leave is part of the integrated program of benefits for Town employees. Such leave is intended as a necessary break from normal duties to allow employees to engage in outside recreational activities as a means of achieving and sustaining high levels of productivity during regularly scheduled duty.

SCOPE: All full-time Town employees accrue vacation leave hours. Part-time employees who work a minimum of 20 hours per week on a regular scheduled basis accrue Paid Time Off (PTO). Temporary and seasonal employees do not earn vacation leave or PTO. (See "Eligibility for Benefits" - Policy # 902).

The amount of vacation time and PTO employees receive each year increases with the length of their employment. Vacation time and PTO begin to accrue with the employee's first full bi-weekly pay cycle, subject to the following:

Upon completion of six (6) months of actual service, each full-time employee shall be credited with up to fifty-two (52) hours of vacation and shall accrue vacation thereafter at the rate specified in this policy. Upon completion of six (6) months of actual service, eligible part-time employees shall be credited with up to twenty-six (26) hours of PTO and shall accrue PTO thereafter at the rate specified in this policy.

ACCRUAL RATE & MAXIMUMS – FULL TIME EMPLOYEES:

Length of Service	**Hours per Pay Period/Year**	**Maximum**
Start date through completion of 3rd year	4.00 / 104	208
4th year through completion of 7th year	5.00 / 130	260
8th year through completion of 10th year	6.00 / 156	312
11th year through completion of 15th year	7.00 / 182	364
16 + Years	8.00 / 208	416

Maximum vacation accruals increase with length of service as depicted in the chart and is limited to two times the yearly accrual.

ACCRUAL RATE & MAXIMUMS – PART-TIME EMPLOYEES:

Length of Service	Hours per Pay Period/Year	Maximum
Start date through completion of 3rd year	2.00 / 52	104
4th year through completion of 7th year	2.50 / 65	130
8th year through completion of 10th year	3.00 / 78	156
11th year through completion of 15th year	3.50 / 91	182
16 + Years	4.00 / 104	208

Maximum vacation accruals increase with length of service as depicted in the chart and is limited to two times the yearly accrual.

All vacation leaves and PTO are to be taken at the convenience of the department and shall be approved in writing, or through automation, by the supervisor or his/her designee. It is the responsibility of the employee to schedule his/her vacation time or PTO in compliance with departmental workloads and needs. Requests for vacation time or PTO should be submitted to the supervisor as far in advance as possible. Employees may be recalled from vacation leave or PTO, or may have their scheduled vacation leave or PTO postponed, when deemed necessary by the department director. When an employee is recalled from vacation leave or PTO, the employee's vacation leave or PTO will be rescheduled to the earliest convenient time. Employees will be permitted to use vacation leave or PTO in incremented units of one-half (1/2) hour or more, in any one day. Vacation time or PTO shall not be advanced to an employee nor may vacation time or PTO be transferred between employees.

Vacation time and PTO will not accrue for workweeks in which there are no hours paid by the Town of Fountain Hills. If the employee has an accrued vacation or PTO balance, the vacation time or PTO must be paid out before any unpaid time off is approved. Vacation hours or PTO must be used for sick leave if accrued sick leave hours have been exhausted. Neither vacation hours nor PTO will count toward hours worked for purposes of computing overtime.

If a holiday falls within an employee's vacation or PTO, the employee will not be charged with vacation or PTO hours for the holiday, but will be paid for the holiday at the appropriate holiday rate.

Separation of Employment

Awarded vacation leave hours or PTO will be paid at the employee's regular hourly rate upon separation of employment.

No more than the maximum allowable accrual of vacation leave is compensable upon separation of employment. Vacation leave or PTO accrued during the initial introductory employment period (six months) will not be compensated if separation occurs during the initial introductory period.

EXHIBIT B
TO
RESOLUTION 2015-54

[AMENDED PERSONAL LEAVE POLICY]

See following pages

Town of Fountain Hills
Personnel Policies and Procedures

SECTION: FRINGE BENEFITS AND LEAVES
POLICY: PERSONAL LEAVE (OPTIONAL)
POLICY NO: 907
EFFECTIVE: DECEMBER 17, 2015
REVISED: DECEMBER 17, 2015

The Town of Fountain Hills provides full-time employees with personal leave time. Full-time employees hired before July 1st are eligible for thirty (30) hours of personal leave time during their first calendar year of employment and 30 hours each year thereafter. Full-time employees hired after July 1st but before October 1 are eligible for twenty (20) hours of personal leave time during their first calendar year of employment and thirty (30) hour of personal leave time each year thereafter. Employees hired on or after October 1st do not receive any personal leave time within the balance of the calendar year, but are to receive thirty (30) hours of personal leave time each year thereafter.

There will be no carryover from year to year of personal leave. Terminating employees are not eligible to be paid for unused personal leave time.

Personal leave time must be scheduled in advance whenever possible and approved by the employee's supervisor.

EXHIBIT C
TO
RESOLUTION 2015-54

[AMENDED INFORMATION TECHNOLOGY PROVISIONS]

See following pages

Town of Fountain Hills
Personnel Policies and Procedures

SECTION:	OTHER WORK PLACE POLICIES
POLICY:	ACCEPTABLE USE OF INFORMATION SYSTEMS
POLICY NO:	1104
EFFECTIVE:	DECEMBER 17, 2015
REVISED:	DECEMBER 17, 2015

OVERVIEW

The Town of Fountain Hills ("Town") is committed to protecting its employees and partners from illegal or damaging actions by individuals, either knowingly or unknowingly. The enterprise network and Internet/ Intranet/ Extranet-related systems, mobile communications and data, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the Town. These systems are to be used for business purposes in serving the interests of the town, and our customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Town employee and affiliate who deals with information and/or information systems. It is the responsibility of all computer users to know these guidelines, and to conduct their activities accordingly.

PURPOSE

This policy is intended to outline the acceptable use of computer equipment owned by the Town. These rules are in place to protect the employee and the Town. Inappropriate use exposes the Town to risks including virus attacks, compromise of network systems and services, and legal issues.

SCOPE

This policy applies to employees, contractors, consultants, temporary employees, and other workers at the Town, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Town.

POLICY

General Use and Ownership

- Users should be aware that the data they create on the Town systems remains the property of the Town. Because of the need to protect the Town's network, management cannot guarantee the confidentiality of information stored on any device belonging to the Town.
- Employees should not engage in personal use of Town information systems in a manner that results in a detrimental impact on the Town. Employees should presume that personal use other

than minimal amounts might result in a detrimental impact on the Town. The Information Technology Administrator shall have discretion to determine detrimental use.

- For security and network maintenance purposes, authorized individuals within the Town may monitor equipment, systems and network traffic at any time, per *Information Technology Division's Audit Policy.*
- The Town reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

- Passwords must be kept secure and NOT be shared with other users. Authorized users are responsible for the security of their passwords and accounts. Application passwords should be changed quarterly, network passwords will expire every 75 days and must be changed.
- Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips."
- Postings by employees from a Town e-mail address to any online venue must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the Town, unless the posting is in the course of business duties.
- All hosts used by the employee that are connected to the Town Internet/Intranet/Extranet, shall be continually executing approved virus-scanning software with a current virus database.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders; such attachments may contain malicious programs (e.g. viruses, e-mail bombs, Trojan horse code, etc).

Unacceptable Use

- The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
- Under no circumstances is an employee of the Town authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the Town-owned resources.
- The lists below are by no means exhaustive, but instead are an attempt to provide a framework for activities that fall into the category of unacceptable use.

1. System and Network Activities

The following activities are <u>strictly prohibited</u>:

- The installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Town.
- The installation of "freeware" software applications <u>without</u> the prior authorization of the Information Technology Division.

- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Users should consult the IT Helpdesk prior to export of any material that is in question.
- Knowingly introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Town information systems asset to obtain and/or transmit material could create a hostile and offensive workplace or a sexually charged workplace in violation of applicable law.
- Making fraudulent offers of products, items, or services originating from any Town account.
- Causing security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.
- Port scanning or security scanning is expressly prohibited unless prior notification is made to, and permission has been granted by, the Information Technology Division.
- Executing any form of network monitoring that will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

2. E-mail and Communications Activities

The following is a summarized list of prohibited uses. Please see the *Intranet/Internet and E-mail* for more detailed information.

- Any form of harassment via e-mail, voicemail, telephone or paging, whether through language, frequency, or size of messages.
- Mass mailing of e-mail "junk mail", jokes or non-Town-business-related advertising material to individuals who did not specifically request such material (e-mail spam).
- Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
- E-mail posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Unauthorized use, or forging, of e-mail header information.

- Use of the Town's information systems to engage in threatening, intimidating or harassing conduct including but not limited to constituting the alleged harassment that constitute threats, intimidation or any other kind of act that interferes with the individual's ability to function as an employee of the Town.

Confidential Files

The files of confidential employees will be preserved to contain confidential information, and will not be accessed by IT or anyone else until permission to do so has been granted by a person having authority to do so. Examples of confidential employees are Human Resources and the Town Attorney.

Enforcement

The Town, through its department directors and Information Technology Division, reserves the right to review an employee's use of Town-provided information technology services, such as but not limited to, Internet, LAN, on-line services, telephone and e-mail use to determine whether the system's use is appropriate and conforms to this policy.

If an employee is found to be not conforming to the sections of this policy, Information Technology will inform the employee's supervisor in writing and the department director may authorize the Information Technology Administrator to remove the employee's access to the Town's computer network resources.

Any employee who fails to abide by this policy may be subject to disciplinary action up to and including termination.

Laptop & Personal Electronic Device Security Tips

- Never leave your laptop or personal electronic device in open view in your vehicle; remove it or secure it in the trunk or other secure location! But, of course, don't leave the device stored in the trunk for any great length of time; exposure to either extreme cold or heat can damage the machine. Always use your laptop or personal electronic device in a cool, dry place.

- Never leave your laptop or personal electronic device unattended in a public place. Don't forget to secure all other products associated with your laptop: batteries, power cords, cables, external drives, LCD projectors, etc.

- Never put your laptop or personal electronic device on the airport security x-ray machine belt before you have a clear path to the end of the belt. Check your device's battery and make sure it's fully charged. If you take your machine through an airport, the security checkpoint personnel may ask you to turn it on to prove it isn't a suspicious device.

- Back up all irreplaceable information daily. Remember, it's not just the loss of the device, it is also the loss of the hard work and important information.

Town of Fountain Hills
Personnel Policies and Procedures

SECTION:	OTHER WORK PLACE POLICIES
POLICY:	INTRANET/INTERNET AND EMAIL
POLICY NO:	1105
EFFECTIVE:	DECEMBER 17, 2015
REVISED:	DECEMBER 17, 2015

OVERVIEW

Electronic mail (e-mail) is a fast and efficient way to communicate internally within an organization using an internal e-mail system and Intranet and externally using the Internet. The Internet is also a powerful research tool that can greatly expand the amount of information gathered on a subject and reduce the amount of time it takes to conduct research activities. It is the policy of the Town to encourage the use of e-mail and the Internet to communicate inside and outside our organization. Furthermore, it is the Town's policy to encourage using the Internet as a research tool. Employees should use good judgment and common sense when using e-mail, the Internet, and the Intranet and understand the Town's policy outlined below.

PURPOSE

The purpose of this policy is to ensure that use of the Intranet, Internet and e-mail technologies among employees of the Town is consistent with Town policies, guidelines, operating procedures for use of specific Town resources, all applicable laws, and the individual employee's job responsibilities.

SCOPE

This policy applies:

- To all Intranet/Internet and e-mail services provided, owned, or funded in part or in whole by the Town;
- To all users and holders of Town Intranet/Internet and e-mail systems or accounts, regardless of intended use;
- To all Town Intranet/Internet and e-mail Official Records and/or Public Records in the possession of or generated by Town employees and other users of e-mail services provided by the Town; and
- Equally to transmission and receipt of data including e-mail headers, summaries, and addresses associated with e-mail records and attached files or text.

This policy does not apply to:

- Printed copies of e-mail, but other laws and policy may apply to such documents. Under Arizona public records laws and other state laws, information appearing in this format may need to be retained as Official Records or treated as State Publications under A.R.S. § 35-103.

INTRANET/INTERNET AND E-MAIL ACCESS

Intranet/Internet Access

- Unauthorized access into the Intranet/Internet using Town equipment or Town Intranet/Internet accounts, or another employee's Intranet/Internet account, or through other means, is in violation of policy.

Obtaining e-mail access

- Unless otherwise directed by the employee's immediate supervisor or designated representative, employees are automatically given an e-mail account upon receipt of a LAN account.

Removing Internet or e-mail access

- The department director must submit a request to the IT HELPDESK to remove or disable an employee's Internet and/or e-mail account.
- By request, the department director can be given access to the files in the disabled account for a period of 30 days after notification to disable.
- LAN and e-mail accounts of employees who have separated from the Town will be deleted 30 days after separation of employment to disable the account unless otherwise directed by a department director. Email will be forwarded to a designated address for a period of up to one year.

Access and usage limits

- The Town's Internet access method has a finite capacity and is subject to periods of heavy use. Therefore, employees may be requested to limit access when system capacity is being exceeded.
- Employees must abstain from personal use of Internet or e-mail services for any reason during the time when employees should otherwise be engaged in Town business and performance of their job duties.

Investigative access

- The Town reserves the right to review, audit, intercept, access and disclose all messages created, received or sent over the e-mail system for any purpose. The contents of electronic mail may be received and disclosed without the consent of the originator. Electronic mail messages are public information.
- Request for e-mail messages, calendars, or records may be treated like any other public record in the possession of the Town.
- E-mail contents may be subject to subpoena in legal matters.
- Management reserves the right to retrieve and/or review e-mail messages to monitor or prevent misuse of the system.

Procedures to request access to an employee's e-mail files:

1. Action by department director:

    a) Submit a request to Human Resources for investigative access on the employee's account.

2. Action by Human Resources:

    a) Consult with the Town Manger about the investigative access request.

    b) Coordinate with the Information Technology Administrator.

ACCEPTABLE USE OF THE INTRANET/INTERNET AND E-MAIL

The definition of acceptable use of the Internet is any use that is related to Town business, an issue facing the Town, or any use that furthers the employee's understanding of topics related to an issue.

Research and general information access on behalf of the Town

- Authorized employees may use Internet and e-mail technologies to conduct official Town business, gain technical or analytical advice as part of their jobs, communicate or exchange files and/or data with employees, citizens, clients, vendors and contractors as part of their jobs.

- Databases can be accessed for information as needed as long as they do not require some form of subscription to participate. Access to subscription-based Internet services must be initiated using existing Town policies for purchased services.

Participation in News/Discussion Groups

- Users may participate in news/discussion groups based around a topic in which the Town has an interest.

- Users may participate in news/discussion groups, listservs or web sites created by professional organizations of which the Town or the user in his or her professional capacity is a member.

- Disclaimer: Postings by employees from a Town e-mail address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Town, unless posting is in the course of business duties.

Limited Personal Use

- The Town's Intranet/Internet and e-mail resources are intended for business use in performing the duties of an employee's job. Limited personal use may be permitted, according to the following guiding principles:

- It is incidental, occasional and of short or moderate duration.

- It does not interfere with any employee's job activities.

- It does not result in incremental expense to the Town. Examples of "incremental expense" include, but are not limited to:

    a) If the Town were paying for a limited bandwidth connection to the Internet, and an employee's personal use incurred additional charges; and

b) Long-distance telephone, cellular phone or fax charges.

- The employee has his/her supervisor's prior approval for said personal use, which approval shall only be given when consistent with the requirements of this policy.
- It does not solicit for or promote commercial ventures, religious or political causes, outside organizations or other non-job related solicitations.
- It does not violate the other "unacceptable uses" or other specific limitations outlined in this policy.
- It will not create a real or perceived conflict of interest.

UNACCEPTABLE USES OF THE INTRANET/INTERNET AND E-MAIL

Activities of law enforcement or Town Attorney's office related to criminal investigations, or personal investigations by any department in general, would not constitute a prohibited or inappropriate use. The following are unacceptable uses of the Intranet/Internet and e-mail technologies. All issues raised in the Town of Fountain Hills Code of Ethics are applicable.

The unacceptable uses shall include, but are not limited to:

Inappropriate e-mail and Intranet/Internet content

- Communication of material that is offensive or derogatory, slanderous and/or defaming towards any individual, corporation, agency or organization and disparagement of any trade or product.
- Communication that is derogatory or discriminatory in any way toward persons for reasons of their race, religion, gender, age, disability, lifestyle, political affiliations, social status or any other personal characteristic.
- Communication describing or picturing specified anatomical areas of the human body and communication describing or picturing sexual activities.

Non-IT purchase of software or computer equipment for Town business

- Users must not download any software packages and/or upgrades from the Internet, and must comply with the Town of Fountain Hills software policy.
- The Information Technology Division purchases all software and/or computer equipment (e.g. microcomputers, printers, modems, hubs, speakers, subwoofers, keyboards, mouse, etc). Departments should always submit a request via e-mail to purchase software and/or computer equipment to the IT Helpdesk.

Non-Town business solicitations and subscriptions

- Employees shall refrain from any type of postings or subscriptions, whether on a Web site, to a news group or via e-mail, that constitutes a solicitation of any type (i.e. religious, political, personal gain, or in support of illegal activities).

- Employees shall refrain from using the Town's e-mail or Internet resources for personal for-profit business activities or schemes to generate income or result in personal financial gain.

Advertising

- Employees shall refrain from any type of postings, whether on a web site, to a news group or via e-mail, that are for the purpose of advertising.

Distributing chain and spam e-mail

- Distribution of chain mails, "Ponzi" or other "pyramid" schemes of any type or other communication that is any way in violation of public law or Town policy is prohibited.

- Users should not in any way participate in the further dissemination or re-distribution of e-mail "spam" e-mails, communications with long mailing lists of other recipients, or other inappropriate e-mail communications. Upon receipt of any of these items, a user should immediately delete it from their e-mail in box and trash, and completely refrain from sending it on to other persons in or outside the Town.

Performing copyright infringements and other illegal actions

- Any use of the Internet that violates copyright laws is prohibited. Infringing on third party copyrights or other intellectual property rights, license agreements or other contracts; for example, illegally installing or making available copyrighted software.

- E-mail shall not be used to send (upload) or receive (download) copyrighted materials, and any other unauthorized materials, without prior written authorization of the originator.

- Users will refrain from the posting of any materials that violate federal or state laws.

- Use of the Intranet/Internet or e-mail in support of illegal activities is prohibited.

- Unauthorized attempts to break into any computer whether in the Town or another organization.

Causing disruption of service and performance

- Use of the Intranet/Internet or e-mail must not disrupt the operation of the Town network or the networks of other users.
- Hacking or modifications to the Intranet/Internet and e-mail software in a manner that restricts the ability of the Town to monitor its resources is prohibited.
- One or more files totaling 30mb or more in size should not be attached to internal e-mail messages. Users instead should utilize the network share drives to distribute the files to other users.

Using the Intranet/Internet and e-mail for political purposes

- The Town's Intranet/Internet and e-mail resources are not to be used for political purposes.

For Misrepresentation

- The use of aliases while using the Intranet/Internet is prohibited. Anonymous messages are not to be sent. No employee shall attempt to obscure the origin of any message.

- The misrepresentation of an employee's job title, job description, or position in the Town is prohibited.

- The release of untrue or distorted information regarding Town business is prohibited.

Execute real-time utilization of Intranet/Internet resources for non-Town-business-related services

- The accessing, viewing, downloading, or any other method for retrieving non-Town business information or services that utilizes the Internet resource in real-time is prohibited. This includes, but is not limited to, streaming audio or video (such as Pandora, XMRadio, Hulu, or NetFlix), streaming wallpaper or screen savers.

INTRANET/INTERNET AND E-MAIL PRIVILEGE RESPONSIBILITY

Use and compliance

- Access to the Intranet/Internet and e-mail is a privilege. Employees are expected to use the Intranet/Internet and e-mail in a professional manner that reflects positively upon themselves and the Town.

- Employees and their immediate supervisors are jointly responsible to ensure compliance with this policy.

- Employees are responsible for text, graphic or audio content they place, send or receive over the Intranet/Internet and e-mail. It is recognized that some unsolicited electronic mail may be received or random access to an undesirable Internet site may occur. In those instances, the individual will not be held responsible for that content or undesired site access.

Account

- Employees shall not "loan" their access to the Intranet/Internet to other employees who have not been authorized use of the Internet and e-mail technologies. Employees will be held responsible for all actions taken using their access permissions.

- Employees shall not intercept or disclose messages, or assist in the interception or disclosure of messages unless otherwise authorized. Information Technology, under the authorization of Town Attorney may intercept or disclose messages when misuse of the Town system is suspected.

USER'S RESPONSIBILITIES REGARDING RECEIPT OF OFFENSIVE MATERIAL

Generally, the same policies of appropriate behavior apply in network usage, as apply in the workplace. If you believe that you are the victim of harassment, do not delete the message. Immediately notify your immediate supervisor or department director and Information Technology.

Confidential Disclosure

Public Records and Privacy

- E-mail from an internal system and/or the Internet, is NOT private nor can the security of e-mail be guaranteed. Caution shall be used when conveying confidential or sensitive information, as part of normal business transactions, when confidentiality cannot be maintained. This includes documents such as performance reviews, disciplinary and/or corrective actions, attorney-client-privileged information, personnel information, and health or medical information.

- All e-mail messages (whether created or received) are the property of the Town and may be considered to be public records pursuant to the Arizona Public Records Law. If there is concern about potential public disclosure or internal disclosure, e-mail should not be used.

- The Town reserves the right to review, audit, intercept, access and disclose all messages created, received or sent over the e-mail system for any purpose. The contents of electronic mail may be received and disclosed without the consent of the originator.

- When communicating with legal counsel or seeking legal advice, consideration should always be given to the fact that e-mail may contain information that may not be entirely confidential. It is advisable to check with the Town Attorney's Office as to whether such request should be made by e-mail or through written communication.

- All requests for public disclosure of data shall be routed to the Town Clerk.

E-mail messages may be recoverable

- Deleting e-mail messages from a computer does not guarantee it has been erased from the system. Employees should use good judgment when creating e-mail and always assume that it is discoverable.

Monitoring and auditing

- The Town owns the network providing access to Internet and e-mail technologies. The electronic records created by use of the system may be considered public records under Arizona Revised Statutes and the law governing retention of public records. The Town reserves the right to monitor all electronic records, at any time, to insure compliance with state law and this policy.

Retention of E-Mail

- All e-mail messages that are not subject to a specific retention schedule are stored by Information Technology for 730 days.

- Any messages that are permanent records are required to be copied or moved to the appropriate file location.

- Information Technology is not responsible for backup or restoration of any e-mail items saved outside of the e-mail system by individual users.

- Records retention schedules can be found on the Arizona Secretary of State's Arizona State Library, Archives & Public Records website – www.azlibrary.gov.

Virus Exposure

- Use of the Internet and e-mail risks exposure to viruses that can cause serious damage to Town computer resources.

- Material downloaded from the Internet must be virus checked before use. Inbound and outbound attachments to e-mail will be scanned for viruses.

Plug-Ins and Helper Programs

Plug-ins and Helper programs should be used prudently and only if its purpose is to enhance the browser to provide services that are within the "acceptable uses" and it does not violate the "unacceptable uses" or other specific limitations outlined in this policy.

Enforcement

- The Town, through the Town Manager, its department directors and Information Technology Division, reserves the right to review an employee's use of Town provided information technology services, such as but not limited to, Internet, LAN, on-line services, telephone and e-mail use to determine whether the system's use is appropriate and conforms to this policy.

- If an employee is found violating this policy, the department director together with the Information Technology Administrator may remove the employee's access to the Town's computer network resources.

- Any employee who fails to abide by this policy may be subject to disciplinary action up to and including termination.

Town of Fountain Hills
Personnel Policies and Procedures

SECTION:	OTHER WORK PLACE POLICIES
POLICY:	SOFTWARE/HARDWARE
POLICY NO:	1106
EFFECTIVE:	DECEMBER 17, 2015
REVISED:	DECEMBER 17, 2015

PURPOSE

It is the policy of the Town to respect all software copyrights and to adhere to the terms of all software licenses to which the Town is a party. The Town users may not duplicate any licensed software or related documentation for use either on Town premises or elsewhere unless the Town is expressly authorized in writing to do so by agreement with the licenser. Unauthorized duplication of software may subject users and/or the Town to both civil and criminal penalties under the United States Copyright Act. The purpose of this policy is to prevent copyright infringement and to protect the integrity of Town's computer environment.

SCOPE

This policy applies to employees, contractors, consultants, temporary employees, volunteers and other workers at the Town. This policy applies to all software that is owned or leased by the Town. Contractors with the Town shall become aware of the requirements of this policy.

POLICY

Budgeting for Software/Hardware

- Some software and hardware needs are limited to specific departments. Departments are responsible for requesting new software or hardware specific to the department's needs through the Information Technology Division.

- When requesting such software or hardware, departments must work with the IT Department to ensure technology costs, compatibility, licensing, support, and integration issues are addressed.

Approval for Purchase of Software/Hardware

To purchase software or hardware, users must obtain the approval of their supervisors and the Information Technology Division, then submit a request to the IT Helpdesk to acquire the software/hardware.

Acquisition of Software/Hardware

- All software or hardware acquired for the Town must be purchased through the Information Technology Division.

- Software or hardware may not be purchased through user corporate credit cards or petty cash.
- Software and hardware acquisition channels are restricted to ensure that the Town has a complete record of all software that has been purchased for Town computers and can register, support, and upgrade such software accordingly.
- Freeware software or mobile apps downloaded from the Internet must be authorized by the Information Technology Division.

License Agreements

Software may only be used in compliance with applicable license (including "shrink-wrap" agreements) and purchasing agreements.

Ownership of Software

All software acquired for or on behalf of the Town or developed by Town employees or contract personnel on behalf of the Town is and shall be deemed Town Property. All such software must be used in compliance with applicable purchase and license agreements.

Storage of Software Media/Licenses

- All software media and original license agreements are kept and stored by the Information Technology Division.
- Software media that must be accessed for support of an application (e.g. clip art, GIS data, etc) will be kept with the workstation licensed for its use. Use and distribution of these types of media must be in compliance with the software licensing agreement.
- IT will monitor the license term length and will notify users of any necessary actions

Duplication of software

- Users are not authorized to produce backup or duplicate copies of any software for any purpose.
- Unless otherwise provided in the applicable license or contract document, any duplication of copyrighted software may be a violation of federal and state law and is strictly prohibited.
- The Information Technology Division creates all authorized duplicate media and retains the master copy. The software inventory registry will be updated with this information.

Registration

- The IT Helpdesk is responsible for completing the registration documentation and returning it to the software publisher
- All software that is Town Property must first be delivered to the IT Helpdesk to complete registration and inventory requirements.

- All software must be registered in the name of the Town. Because of personnel turnover, software will never be registered in the name of the individual user. Information Technology maintains a register of all software and will keep a library of software licenses. The register will contain:
    - the title and publisher of the software;
    - the date and source of software acquisition;
    - the location of each installation as well as the serial number of the hardware on which each copy of the software is installed;
    - the name of the authorized user(s);
    - the existence and location of the media and any back-up copies;
    - the software product's serial number and/or key codes.

Installation of Software

- No software, including freeware, may be installed on any Town-owned or leased computer without prior approval by the Information Technology Division and without being registered to the Town.
- After the registration requirements above have been met, the software will be installed with the authorization of, assistance of, or performance by, Information Technology support personnel. Manuals, tutorials and other user materials will be provided to the user.
- Once installed on the hard drive, the original media (USB drives, CD-ROM, DVD, etc) will be kept in a safe storage area maintained by the IT Helpdesk.
- Users may not give software to anyone, including contractors, customers and others.
- Town users may use software on local area networks or on multiple machines only in accordance with applicable license agreements.
- Town computers are Town-owned assets and must be kept both software legal and virus free. Only software purchased through the procedures outlined above may be used on Town machines.
- Installation of personal non-business related software on Town computers is not authorized. The Town will remove any unauthorized software that puts the Town at risk or liability.

Removable Media Drives & USB Drives

To protect the Town's network and computers, restrictions have been placed on external drives including USB hard drives and flash drives, and the following guidelines should be followed to enhance security. In addition, files written to or copied from such devices may be logged and audited to ensure compliance with policy.

- Software may not be executed from external and USB hard drives and flash drives.

- Confidential files or files with sensitive data should be encrypted when saved on removable drives to protect the contents in the event the device is lost or stolen.

- Any removable or USB drive should be scanned for malicious code and viruses prior to use.

Support

Software compatible with installed operating system, client, application and system configuration standards for workstations and/or file servers will be supported by the Information Technology Helpdesk.

Uninstalling Software

- Unauthorized removal of software from Town computers is prohibited.

- Software removals should not be performed without the authorization of, assistance of, or performance by, Information Technology support personnel.

- IT reserves the right to uninstall or remove any software found to be causing a negative impact on the workstation, the Town's enterprise network, or any Internet/Intranet/Extranet-related systems.

User Responsibilities

Each User is individually responsible for reading, understanding, and adhering to all licenses, notices, and agreements in connection with software that he or she causes to be acquired, copied, transmitted, or used or seeks to acquire, copy, transmit, or use. IT will provide all necessary copies of such licenses.

If a computer must be reconfigured or replaced and it contains software that has been licensed specifically for that computer, the user should notify Information Technology of such installation to ensure the software is reinstalled, tested and documentation of the installation location is updated.

Shareware Software

It is the policy of the Town to pay shareware authors the fee they specify for use of their products.

Registration of shareware products will be handled the same way as outlined above.

Software Games

- The installation of computer games on Town computers is prohibited unless there is a Town business or service justification.

- Games packaged with the operating system installation (e.g. FreeCell, Minesweeper, Pinball, and Solitaire) are included in the workstation image and are exceptions. However, IT reserves the right to remove these games.

- Software Games that impact network resources are strictly forbidden.

Screensavers and Wallpaper

- Screensaver and wallpaper software are permissible only after the Software Policy procedures to purchase (commercial and/or shareware), license, register and install have been applied.

Decompiling software

No User shall decompile, disassemble, or reverse-engineer any software.

Transfer of Software

No User may sell, rent, sublicense, lend, transmit, distribute, give, or otherwise convey or make available Town-owned software or an interest therein to any unauthorized individual or entity.

Audits

The Information Technology Division will conduct audits of all PCs, including portables, to ensure that the Town is in compliance with all software licenses. Audits will be conducted using an auditing software product or through manual inspection.

Enforcement

- A Town user who makes, acquires, or uses unauthorized copies of software will be subject to disciplinary action up to and including termination.
- The Town does not condone the illegal duplication of software and will not tolerate it. Any doubts concerning whether any employee may copy or use a given software program should be addressed with IT Helpdesk.
- Any User who suspects an incident of noncompliance with the Software Policy by another User shall promptly notify the Information Technology Division.
- The Town, through its department directors and Information Technology Division, reserves the right to review an employee's use of Town-provided information technology services, such as but not limited to, Internet, LAN, on-line services, telephone and e-mail use to determine whether the system's use is appropriate and conforms to this policy.
- If an employee is found violating the sections of this policy, the Department Director together with the Information Technology Administrator may remove the employee's access to the Town's computer network resources.
- Any employee who fails to abide by this policy may be subject to disciplinary action up to and including termination.

Town of Fountain Hills
Personnel Policies and Procedures

SECTION:	OTHER WORK PLACE POLICIES
POLICY:	AUDIT OF INFORMATION SYSTEMS
POLICY NO:	1107
EFFECTIVE:	DECEMBER 17, 2015
REVISED:	DECEMBER 17, 2015

PURPOSE

To provide the authority for members of Town' Information Technology team to conduct a security audit on any computer or communication system (hardware or software) at the Town.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents
- Monitor user or system activity
- Enforce information system policies

SCOPE

This audit policy covers any equipment owned, leased or otherwise possessed by the Town, including, but not limited to all of the following devices:

1. hand-held devices (iPhone, iPad, etc.)
2. computers (desktop and laptops)

Communication devices, including but not limited to:

1. telephone and voicemail system
2. network hardware (routers, printers, firewalls, etc.)
3. other wireless devices, including pagers

Employees should be aware that loading Town programs or property on their own personal devices may result in public record information being on those devices and creating a Town interest in those devices to the extent such information is present. The use of personally-owned information and communication devices for Town business is discouraged unless a department head and the Information Technology Administrator determines there is a necessary business use for such equipment.

POLICY

When requested, and for the purpose of performing an audit, any access needed will be provided to members of Town' Information Technology team. This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on Town equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on Town networks.

Enforcement

The Town, through its department directors and Information Technology Division, reserves the right to review an employee's use of Town-provided information technology services, such as but not limited to, Internet, LAN, on-line services, telephone and e-mail use to determine whether the system's use is appropriate and conforms to this policy.

If an employee is found to be violating the sections of this policy, the department director together with the Information Technology Administrator, may remove the employee's access to the Town's computer network resources.

Any employee who fails to abide by this policy may be subject to disciplinary action up to and including termination.