ADMINISTRATIVE POLICY NO. 14

INFORMATION TECHNOLOGY POLICY

Policy Purpose:

To establish the proper use of information systems (i.e., computer systems, laptops, tablets, printers, cell phones, etc.) and the use of social media networking sites, provided by the City of Gulf Shores to its employees for the purpose of performing job functions including, but not limited to; communication, information exchange, operational software application transactions, and research.

Definitions:

A. **Information systems** include all hardware and software owned by the City of Gulf Shores and available for official use by City of Gulf Shores employees.

    a. This includes, but is not limited to; computers, computer peripherals, network equipment, software, Internet, electronic and voice mail, cell phones, temporary or permanent files and data which reside in part, or in whole, on any City information system.

B. **Peripheral Devices** includes all hardware or equipment that can be connected either wired or wirelessly to a city information system for the purpose of housing, transporting, saving, or otherwise usage of electronic files, folders, data, or other electronic communication.

    a. This includes, but is not limited to; CDs, DVDs, optical disks, external hard drives, USB memory sticks (also known as flash or thumb drives), media card readers, embedded microchips (including smart cards or mobile SIM cards), MP3 players, digital cameras, backup cassettes, audio tapes, tablets, cell phones, printers, and scanners.

I. Policy

A. General Use and Ownership

i. All information systems are the property of the City of Gulf Shores and therefore users must understand there should be no expectation of privacy when using such systems. Proprietary Information stored on electronic and computing devices whether owned or leased by a City employee or a third party, remains the sole property of our organization.

    1. Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of company proprietary information and/or information systems.

ii. All Internet data that is written, sent, or received through our information systems is part of official City of Gulf Shores records. That means that we can be legally required to show that information to law enforcement or other parties. Therefore, you should always make sure that the business information contained in Internet email messages and other transmissions is accurate, appropriate, ethical, and legal.

B. **Acceptable Uses of Information Systems**

i. City owned computer equipment, access to the Internet, telephones, cell phones, and City provided applications may not be used for purposes that are prohibited by the City of Gulf Shores, ethics rules, or City, State, or Federal law or this policy.

ii. Employees may access, use, or share company information systems only to the extent it is authorized and necessary to fulfill your assigned job duties.

1. **Authorized uses** of information systems include, but are not limited to the following:

    a. To facilitate performance of job functions.

    b. To facilitate the communication of information in a timely manner.

    c. To coordinate meetings of individuals, locations, and City resources.

    d. To communicate and share information with departments throughout the City.

    e. To communicate with outside organizations as required for performing an employee's job functions.

2. **Prohibited uses** of information systems include, but are not limited to, the following:

    a. Theft or vandalism to hardware, software or data.

    b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which our company or the end user does not have an active license.

    c. Unauthorized attempts, modifying or deleting of hardware, system settings, software or data.

    d. Unauthorized access of systems or data, or allowing access by unauthorized persons for any purpose other than conducting company business

    e. Illegal activities.

    f. Threats, harassment, slander, or defamation.

    g. Obscene and/or sexually explicit messages, content, websites, or offensive graphical images.

    h. Political endorsements.

i. Commercial activities.

j. Using non-business software including games or entertainment software.

k. Downloading or opening files that may contain viruses which may contaminate City information systems.

l. Disabling or stopping services or applications that have been installed and/or deployed by the Information Technology Division for the purpose of monitoring and securing information systems.

m. Streaming video and audio files or websites that are not authorized or required as part of an employee's job functions or assigned tasks.

C. **Outlook Email and Calendars**

i. Email account should be used primarily for company business-related purposes; personal communication is permitted on a limited basis, but non-company related commercial uses are prohibited.

ii. All use of email must be consistent with our policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

1. **Prohibited uses** of email and communication activities include, but are not limited to, the following:

a. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

b. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

c. Unauthorized use, or forging, of email header information.

d. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies

e. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

f. Use of unsolicited email originating from within company networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by our company or connected via our company's network

g. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

h. Our email system shall not to be used for the creation or

distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

i. Employees who receive any emails with this content from any company employee should report the matter to their supervisor immediately.

iii. All data contained within an email message or an attachment must be secured according to the Data Protection Standard.

iv. Users are prohibited from automatically forwarding Company email to a third-party email system.

v. Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Company business, to create or memorialize any binding transactions, or to store or retain email on behalf of The City of Gulf Shores

vi. Email that is identified as a company business record shall be retained according to our Record Retention Schedule.

1. Email should be retained only if it qualifies as a company business record.

a. Email is a business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

vii. Employees shall have no expectation of privacy in anything they store, send or receive on the City's email system. Email and other electronic communications may be monitored with or without prior notice.

D. **Internet Access**

i. Internet access shall be limited to City-related business activities.

ii. The City reserves the right to filter Internet access to preclude dangerous or harmful website connections.

iii. Occasional and limited personal use during regular breaks or during meal times is acceptable if the usage is in compliance with authorized use stated in this policy.

iv. Time is to be limited on the Internet to that necessary to conduct City-related business and research.

v. Streaming videos or music consume large amounts of internet and intranet resources and are disallowed unless necessary to conduct City-related business.

E. Viewing and/or visiting websites that contain obscene and/or sexually explicit messages, content, websites, or offensive graphical images from any City owned or personal device, while on the City network, either wired or wirelessly, is strictly prohibited.

F. **Personal Social Networking Guidelines**

i. Your social networking is subject to all of the policies enacted by the City of Gulf Shores, including Code of Conduct, Sexual Harassment, Code of Ethics and any of the rules outlined in the City of Gulf Shores employee handbook.

ii. Employees who engage in social networking should be mindful that their postings, even if done off premises and while off duty, could have an adverse impact on the City of Gulf Shores legitimate business interests. In addition, some readers may view you as a *defacto* spokesperson for the City. To reduce the likelihood that your personal social networking will have an adverse effect on the City, observe the following guidelines when social networking.

1. Do not engage in social networking using any of the City's electronic resources or when you are supposed to be working.

2. Managers/Supervisors should not send "friend" requests to subordinates while on or off duty. Any employee may reject a friend request from any other employee without repercussion.

3. All requests for references or recommendations, even those that are received through social networking, should be handled in accordance with the City of Gulf Shores standard policy for responding to such requests. If someone from the media or press contact you about social networking activities that relate to the City, refer those requests directly to your Supervisor or the Public Information Officer.

4. Make it clear to your readers that the views expressed are yours alone and do not reflect the views of the City of Gulf Shores. A statement similar to the following is acceptable: "The views expressed in this post are my own. They have not been reviewed or approved by the City of Gulf Shores."

5. Do not defame or discredit the City's services, other employees; do not disclose personal or contact information, or post photographs of coworkers or supervisors without their prior permission.

iii. Employees of the City are prohibited from posting, transmitting, and/or disseminating any photographs, video or audio recording, likenesses, or images of departmental logos, emblems, uniforms, badges, patches, marked or unmarked vehicles, equipment, or other material that specifically identifies the City or any of its departments on any personal or social networking website or web page, without the express written permission of the City's official representative.

iv. The City will, in its discretion, review your social networking activities. Please note that this policy applies even if your social networking is anonymous or under a pseudonym. If you do engage in such social networking, you should be aware that in appropriate circumstances, the City will take steps to determine your identity.

v. The City may request, at its sole and absolute discretion, that you temporarily confine your social networking to matters unrelated to the City if the City determines this is necessary or advisable to ensure compliance with any State or

Federal regulations or laws.

vi. Failure to comply with this policy may lead to disciplinary action up to and including termination and if appropriate, the City will pursue all available legal remedies. The City also may report suspected unlawful conduct to appropriate law enforcement authorities. Note, however, that nothing in this policy will be interpreted to limit or interfere with your rights under Section 7 of the National Labor Relations Act.

vii. Any employee becoming aware of or having knowledge of a posting, or of any website or web page violation of the provisions of this policy, shall notify his or her supervisor immediately.

G. **Security**

i. **Monitoring of User Accounts, Files, and Access**

1. The City reserves the right to monitor its information systems and user activity. There is no guarantee of privacy of email, Internet access, system logs, and electronic files related to individual City computer and network accounts.
2. The City may specifically and without notice monitor the activity and accounts of individual users including files, session logs, and content of communication and Internet access for adherence to the acceptable use policy.
3. Individual and associated accounts under investigation are subject to having their activities on City systems monitored and recorded.
4. In the course of monitoring individuals who are improperly using these systems, or in the course of correcting system problems caused by the unauthorized use, the activities and files of authorized users may also be disclosed.

    a. **Unauthorized uses** of information systems requiring the Information Technology Officer and employee's Department Head written approval include, but are not limited to, the following:

        i. Using hardware, related equipment, and/or software not purchased and/or owned by the City.

        ii. Listening to voice mail or reading electronic mail of another employee without prior written approval of the employee's Department Head or executive management.

5. Evidence of criminal activity will be turned over to appropriate City and law enforcement officials.

ii. **Passwords for User Accounts**

1. Passwords are for the security of the City's systems and data, and are to be treated as confidential.

a. Employees are responsible for the protection of their own password. Employees shall not share passwords nor obtain any other user's passwords by any unauthorized means.

b. Passwords must not be inserted into email messages, or any other forms of electronic communication.

2. All user-level and system-level passwords must conform to the Policy for Password Construction Guidelines.

3. Where possible, users must not use the same password for various access needs. Each site should have its own unique password.

4. All user-level passwords (for example, email, web, desktop computer, and so on) must be changed every 120 days.

5. Any user suspecting that his/her password may have been compromised must report the incident and change all passwords immediately.

iii. **Device and Data Protection**

1. Systems should be locked or logged out by users in areas accessible by the public if the user will be away for an extended period of time.

2. Users shall not store personal photos, music, items download from the Internet, or other files on the network file systems unless approved and/or as required for conducting City business.

3. Any personally owned peripheral devices (i.e., flash drives, palm pilots, CDs, DVDs, cell phones, etc.) may only be connected to your local computer and shall also comply with all aspects of this policy.

4. Uploading and/or downloading any data or files from a network location or local drive to any personal peripheral device shall only be for the purposes of City business and must be approved by your Department Head in writing.

5. Deleting any data, files, folders, or other electronic documentation and/or communications from the City network and/or file stores is prohibited.

6. Transporting data, files, folders, or other electronic documentation and/or communications from the City network by means of cell phone, personal computer, peripheral storage device offsite is strictly prohibited, unless and only for the purpose of City business and only when approved by your Department Head in writing.

iv. **Cyber Security Protection Measures**

1. All computer devices connected to the city network or networked resources shall have anti-virus software installed and configured so that the virus definition files are current, routinely and automatically updated. The anti-virus software must be actively running on these

devices at all times.

2. Employees must use extreme caution when opening email attachments received from unknown senders, which may contain malware, ransomware, and/or other potential threats.

3. All suspected intrusions via the Internet or by unauthorized employees or individuals shall be reported to the local Department Head and Information Technology Officer immediately.

4. Employees who have been assigned Cyber Security courses and/or coursework by the Information Technology Division must complete each assigned course or module in the designated timeframe.

v. **File and Data Storage**

1. File storage space is limited on the file server and shall only be used for storage of City-related data

2. Files shall be created using software which is the City standard for that application.

3. Files should be named in such a way that other employees will know what they contain.

4. Each department has a shared folder with read/write/delete capabilities for each member of that department. Files shared between department members should be placed in or moved to this folder. Other departments have read-only access to these files.

5. Each employee has an individual folder in which to place files that they alone are working on. Only supervisors or other authorized employees will have read-only access to these files, and only when it is necessary to fulfill a job function or task.

6. Employees may not store personal music, pictures, or other files on the file server in order to limit valuable storage space to City-related data only.

7. Personal files, pictures or music may be stored locally on the individuals' C-drive if the items are appropriate according to this policy.

8. The Information Technology Division does NOT back up data or files on individual users' local C-Drives and therefore the storage of company and/or work related files, folders, data, and other electronic communications should not be stored locally.

H. **Acquisition, Installation, Upgrades and Disposal**

i. Information Technology will aid department heads with information system planning and budgeting. In order that all departments are able to have

compatible information systems, purchases including upgrades will be processed through Information Technology. New and upgraded information systems will be configured to the City's standard and inventoried prior to being installed by Information Technology. Only systems acquired by the City are allowed on the City's information systems.

ii. When a department no longer has any use for any information system, they should be transferred to Information Technology, through the appropriate property transfer process. Information Technology will maintain a repository of system components and will supply departments with available components as needed.

I. **Technical Support and Training**

i. Information Technology should be contacted regarding any problems or technical support questions related to the network, hardware, workstations, or printers and peripherals. Information Technology staff will provide training on Microsoft tools, i.e. Outlook email, Excel, and Power Point to employees as needs arise.

J. **Operational Software Application Support**

i. Each department shall work directly with software vendor support desk when encountering software problems with department software applications. If the software support contact determines that the problems is not software related, then the Information Technology staff should be contacted to troubleshoot the problem as it relates to hardware, network, or workstation configuration.

II. Policy Enforcement

A. If incidental violations of this policy are discovered, the City will take appropriate actions to resolve the issue and violators may be subject to disciplinary measures.

B. If violations of this policy initiated by careless or deliberate acts are discovered, the City will take appropriate actions to resolve the issue which may include disciplinary measures up to and including separation of employment.

C. If violations of this policy are discovered that are illegal activities, the City will notify appropriate authorities and impose the appropriate discipline.

D. The City reserves the right to pursue appropriate legal actions to recover any financial losses suffered as the result of violations of this policy.