RESOLUTION No. 2011-65
CITY OF SHOREACRES

A RESOLUTION ESTABLISHING A POLICY RELATING TO THE USE OF, AND ACCESS TO, CITY AUTOMATION SYSTEMS AND ELECTRONIC FILES; MAKING VARIOUS FINDINGS AND PROVISIONS RELATING TO THE SUBJECT; FINDING COMPLIANCE WITH THE OPEN MEETINGS LAW; AND PROVIDING AN EFFECTIVE DATE HEREOF.

* * * *

BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF SHOREACRES:

THAT the City Council hereby establishes a policy relating to the use of, and access to, city automation systems and electronic files to protect the interests of the City, it's citizens, employees, and he public; to wit:

INTERNET, E-MAIL, AND COMPUTER USAGE POLICY

Policy Statement

The use of City of Shoreacres (City) automation systems, including computers, fax machines, and all forms of Internet/intranet access, is for City business and for authorized purposes only. Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to the City or otherwise violate this policy.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to the City's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

Use of City computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate City purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms (see below);
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- Intentionally or carelessly disclosing your controlled-access password or the password of others to City computers, networks, e-mail, Internet, City applications, City files, or City data;
- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Defeating or attempting to defeat security restrictions on City systems and applications;
- Making unauthorized copies of City files or other City data;

- Causing congestion, disruption, disablement, alteration, or impairment of City networks or systems;
- Destroying, deleting, erasing, or concealing City files or other City data, or otherwise making such files or data unavailable or inaccessible to the City or to other authorized users of City systems;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the City's networks or systems or those of any other individual or entity;
- Misrepresenting oneself or the City;
- Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way;
- Engaging in unlawful or malicious activities;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging; and/or
- Using recreational games.

Using City automation systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates the City anti-harassment policies and is subject to disciplinary action. The City's electronic mail system, Internet access, and computer systems must not be used to harm others or to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of City resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. The City will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

Unless specifically granted in this policy, any non-business use of the City's automation systems is expressly forbidden.

If you violate these policies, you could be subject to disciplinary action, up to and including dismissal.

Ownership and Access of Electronic Mail, Internet Access, and Computer Files; No Expectation of Privacy

The City owns the rights to all data and files in any computer, network, or other information system used in the City and to all data and files sent or received using any City system or using the City's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property. The City also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the Internet and of computer equipment used to create, view, or access e-mail and Internet content. Employees must be aware that the electronic mail messages sent and received using City equipment or City-provided Internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by City officials at all times. The City has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in

order to assure compliance with City policies and state and federal laws. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate City official.

The City uses software in its electronic information systems that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems. Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on City electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and City use at any time. Further, employees who use City systems and Internet access to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure. Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than City systems or the City-provided Internet access.

The City has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software. Violation of this policy can lead to disciplinary action, up to and including dismissal.

Confidentiality of Electronic Mail

As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable state and federal laws and City rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.

It is a violation of City policy for any employee, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others, unless such access is directly related to that employee's job duties. Employees found to have engaged in such activities will be subject to disciplinary action.

Electronic Mail Tampering

Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

Policy Statement for Internet/Intranet Browser(s)

The Internet is to be used to further the City's mission, to provide effective service of the highest quality to the City's customers and staff, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Intranet access are City resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

Employees are individually liable for any and all damages incurred as a result of violating City

security policy, copyright, and licensing agreements.

All City policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, City information dissemination, standards of conduct, misuse of City resources, anti-harassment, and information and data security.

Personal Electronic Equipment

Employees should not bring personal computers or data storage devices (such as floppy disks, CDs/DVDs, external hard drives, flash drives, iPods, or other data storage media) to the workplace or connect them to City electronic systems unless expressly permitted to do so by the City. Any employee bringing a personal computing device, data storage device, or image-recording device onto City premises thereby gives permission to the City to inspect the personal computer, data storage device, or image-recording device at any time with personnel of the City's choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the personal computer or image-recording device in question. Employees who do not wish such inspections to be done on their personal computers, data storage devices, or imaging devices should not bring such items to work at all.

Violation of this policy, or failure to permit an inspection of any device covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment, depending upon the severity and repeat nature of the offense. In addition, the employee may face both civil and criminal liability from the City, from law enforcement officials, or from individuals whose rights are harmed by the violation.

The City Council officially finds, determines, recites, and declares that a sufficient written notice of the date, hour, place and subject of this meeting of the City Council was posted at a place convenient to the public at the City Hall of the City for the time required by law preceding this meeting, as required by the Open Meetings Law, Chapter 551, Texas Government Code; and that this meeting has been open to the public as required by law at all times during which this resolution and the subject matter thereof has been discussed, considered and formally acted upon. The City Council further ratifies, approves and confirms such written notice and the contents and posting thereof.

This Resolution shall take effect immediately upon passage.

PASSED AND APPROVED, this 8th day of August, 2011.

CITY OF SHOREACRES

By: Dolly N. Arons
Dolly Arons, Mayor

ATTEST:

David K. Stall, City Secretary