# RIVER ACRES WSC

# INTERNET, E-MAIL, AND COMPUTER USE POLICY

## Policy Statement

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

"Excessive" is defined as interfering 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 corporation's business; distract, intimidate, or harass coworkers, board members or third parties; or disrupt the workplace.

Use of corporation's computers, networks, and Internet access is a privilege granted by the board of directors 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 corporation purposes.
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms.
- Accessing or deliberately granting access to any other outside users to networks, servers, drives, folders, or files to which the person has not been granted access or obtained prior authorization from the board of directors with the right to make such a grant.
- Connecting any unapproved or potentially hazardous peripherals.
- Making unauthorized copies of corporation files or other corporation data.

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

*Important exception:* consistent with federal law, you may use the corporation's electronic systems to discuss with other employees the terms and conditions of your and your coworkers' employment. However, any such discussions should take place during non-duty times and should not interfere with your or your coworkers' assigned duties. You must comply with a coworker, and or board member/s stated request to be left out of such discussions.

Using corporation electronic 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 corporation anti-harassment policies and subjects the responsible employee, and or board member/s to disciplinary action. The Corporation's electronic mail system, Internet access, and computer systems must not be used to harm others or to violate the laws regulations, or local jurisdiction Use of corporation resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. Unless specifically granted in this policy, any non-business use of the Company's electronic systems is expressly forbidden.

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

The corporation owns the rights to all data and files in any computer, network, or other information system used in the corporation and to all data and files sent or received using any corporation system or using the corporation's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property. The corporation also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as all use by employees or any board member 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 corporation equipment or corporation-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 the corporation at all times. The corporation has the right to inspect all files stored in private areas of the network or on individual computers or storage media to assure compliance with corporation policies and state and federal laws. No

employee or board member may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or from corporation's board of directors.

The corporation 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, received by, sent, or viewed on such systems. There is no expectation of privacy in any information or activity conducted, sent, performed, or viewed on or with corporation equipment or Internet access. Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on corporation electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and corporation use at any time. Further, employees, or board members who use corporation 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 or board member/s who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than corporation systems or the corporation-provided Internet access.

The corporation 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 or board member 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 always subject to monitoring, and the release of specific information is subject to applicable state and federal laws and corporation 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 corporation policy for any employee, or board member 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 or board members found to have engaged in such activities will be subject to disciplinary action or removal from the board.

**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 corporation's mission, to provide effective service of the highest quality to the corporation's customers, members, 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 corporation 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 or board members are individually liable for all damages incurred as a result of violating company security policy, copyright, and licensing agreements.

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

**Personal Electronic Equipment**

The corporation prohibits the use in the workplace of any type of camera phone, cell phone camera, digital camera, video camera, or other form of recording device to record the image or other personal information of another person, if such use would constitute a violation of a civil or criminal statute that protects the person's right to be free from harassment or from invasion of the person's right to privacy. Employees may take pictures and make recordings during non-working time in a way that does not violate such civil or criminal statutes. The corporation reserves the right to report any illegal use of such devices to appropriate law enforcement authorities.

Due to the significant risk of harm to the corporation's electronic resources, or loss of data, from any unauthorized access that causes data loss or disruption, employees or board members should not bring personal computers or data storage devices (such as floppy disks, CDs/DVDs, external hard drives, USB / flash drives, "smart" phones, iPods/iPads/iTouch or similar devices, laptops or other mobile computing devices, or other data storage media) to the workplace and connect them, via any means, to corporation electronic systems unless expressly permitted to do so by the corporation. To minimize the risk of unauthorized access to or copying of confidential corporation business records and proprietary information that is not available to the general public, any employee or board member connecting a personal computing device, data storage device, or image-recording device to corporation networks or information systems in any manner thereby gives permission to the corporation to inspect the personal computer, data storage device, or image-recording device at any time with personnel and/or electronic resources of the corporation's choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the data-storage device in question in order to ensure that confidential corporation business records and proprietary information have not been taken without authorization. Employees who do not wish such inspections to be done on their personal computers, data storage devices, or imaging devices should not connect them to corporation computers or networks.

Violation of this policy, or failure to permit an inspection of any device under the circumstances covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment, or removal from the board depending upon the severity and repeat nature of the offense. In addition, the employee and or board member/s may face both civil and criminal

liability from the Company, from law enforcement officials, or from individuals whose rights are harmed by the violation.

**Remote Access**

Any employee or board of directors that requires remote access must have permission from the board of directors. Any personal computer that connects to the RAWS network is subject to the same audit and policy as above.

Report all and any unauthorized computer access.