Suggested policy format and content. RTPA specific policies should be developed in consultation with RTPA Legal Counsel, Board of Directors and appropriate regulatory agencies.

13. Technology and Electronic Resources

The policy is intended to apply to all RTPA technology and electronic resources, including, but not limited to: computer systems, software, hardware, servers, networks, electronic mail, cell phones, and computing devices paid for, in whole or in part (including reimbursement of expenses), by RTPA, Internet services, Intranet, voicemail system, facsimile machines, and photocopiers. The term "computing devices" includes, but is not limited to smart phones, PDAs, electronic tablets, and other similar devices. This policy applies to all users of RTPA technology and electronic resources, whether or not they are employees or independent contractors; whether or not they are using RTPA technology or resources during or after work hours; or whether they access the technology or resources from RTPA premises or some other location.

No Expectation of Privacy

Users should not expect that the information placed on or through RTPA electronic resources is private. By using RTPA technology and electronic resources, users consent to the monitoring discussed in this policy, without any additional notice. RTPA may not require or request an employee to (1) disclose a username or password to access personal email/social media; (2) access his or her personal email/social media in the presence of another RTPA employee or representative; or (3) divulge any personal email/social media unless it is reasonably believed that content on the email/social media is relevant to an investigation of allegations of employee misconduct or violation of law, or to access a RTPA-issued electronic device.

Following is a list of some, but not all, circumstances under which a user's activities may be disclosed to others. Note that with regard to computers, data on all drives may be accessed or monitored, not just data on the shared drives.

In order to ensure RTPA technology and electronic resources are not misused, RTPA may monitor or investigate computer files, electronic messages, voicemail, Internet use, and all other information kept or accessed by users on its electronic resources to determine whether a user has misused these resources. Users should not expect information stored on or accessed from RTPA electronic resources to be private, even if passwords, account codes, or other security measures are utilized. Data may be monitored regardless of its origin or content.

Any information retained on or accessed from RTPA property may be disclosed to outside parties, including law enforcement authorities, in the event of an investigation or legal process.

When a user is absent, unavailable, or is terminated, another user may need to access information kept on the unavailable user's or former user's computer or voicemail.

Data scans by law enforcement agencies and RTPA Information Systems (IS) staff are made on an ongoing basis to check for malware, viruses or other illegal access or use of RTPA data or equipment that may have been initiated by persons inside or outside RTPA.

Unacceptable Use

The use of RTPA technology and electronic resources is a privilege that may be revoked at any time. RTPA will not tolerate misuse of its property. Nothing in this policy is meant to prohibit use of electronic

resources for labor activities or First Amendment speech permitted by law. Conduct that may result in discipline includes, but is not limited to:

Damage, theft, duplication, or unauthorized alteration of hardware or software.

Placement of unlawful information, computer viruses, or harmful programs on or through an electronic resource.

Obtaining, downloading, viewing, or otherwise gaining access to materials which may be deemed unlawful, harmful, abusive, obscene, pornographic, descriptive of destructive devices, or which are harmful matter as defined in California Penal Code Section 313(a), or which are otherwise objectionable under current RTPA policies or applicable laws.

Violation of the federal Communications Decency Act or any other federal or state law applicable to computer and/or telecommunications systems.

Use of RTPA electronic resources for personal gain, commercial purpose, or political or religious activity.

Use of RTPA electronic resources to unlawfully harass other persons. Examples: Display or transmission of messages containing ethnic slurs, racial comments, off-color jokes, cartoons with sexual content, or anything that may conflict with the RTPA policy of providing a workplace sensitive to diversity and free of discrimination, harassment, and disrespect.

Unauthorized use, review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of RTPA, a business, or any governmental agency to conduct improper activities, including but not limited to “hacking.”

Use of copyrighted, trademarked, or patented data, software or other materials without peMSDssion from the owner, including, but not limited to, use of data downloaded from the Internet and the creation or maintenance of archival copies of materials obtained through the Internet, unless such materials are in the public domain. This includes use of RTPA owned logos or trademarks without approval from the Executive Director.

Placing RTPA’s confidential, sensitive, or proprietary information in electronic messages or on the Internet.

Creating or utilizing chain letters, chat rooms, or other Multiple User Dimensions (“MUDs”), with the exception of those bulletin boards or electronic mail groups that may be used for specific work-related communications.

Use of social networking sites such as Facebook, Twitter, or Linked-In, or other Internet blogging sites during work hours for non-RTPA business is forbidden if the time taken to do so or the content of the posting could be disruptive to RTPA business. Use of social networking sites for RTPA business is permitted.

Posting information on the Internet or in electronic mail or electronic mail attachments that does not reflect the standards and policies of RTPA. Employees are expected to be respectful of RTPA, its employees, member agencies, and the public. If an employee represents himself or herself on the Internet as a RTPA employee, he/she is expected to ensure the page content complies with professional standards of conduct. Employees are prohibited from accessing, posting, or placing any content using RTPA property that associates RTPA with illegal, unethical, or unprofessional activity.

Establishing Internet or other external network connections that could allow unauthorized persons to gain access to RTPA systems and information. These connections include, but are not limited to, the establishment of hosts with public modem dial-ins, World Wide Web home pages, File Transfer Protocol sites, and peer-to-peer networking (file-sharing) nodes.

Downloading data or visiting websites that are likely to contain computer viruses or other malware.

Spending excessive time browsing the Internet for non-work-related information or sending personal e mail during work periods. This includes time spent texting, instant-messaging, blogging, tweeting, or viewing Facebook, Linked-In, or similar social networking sites.

Use of RTPA resources for non-work related matters that take up too much disk or memory space on an electronic resource, slow down the electronic resource's ability to process data, or deplete RTPA office supplies.

Use of Technology While Operating a Vehicle

RTPA employees are prohibited from utilizing an electronic device such as a cell phone without proper equipment while operating a vehicle to conduct RTPA business. Employees also are prohibited from sending text messages or emails while operating a vehicle if they are using the vehicle to conduct RTPA business.

Consequences of Violating this Policy

The consequences for violating this policy include, but are not limited to, disciplinary action up to and including termination from employment, termination of a user's contract with or services for RTPA, and/or referral to legal authorities for prosecution under California Penal Code Section 502 or other applicable laws.

Reporting of Abnormalities or Misuse

Users should report any misuse, abnormality, or security breach as soon they observe it. Abnormalities or breaches of security should be reported to the Director of Finance and Administrative Services immediately. If any user observes a misuse, such as an electronic communication containing obscene or harassing language, or unauthorized access to electronic resources by an employee or consultant, the user should report the misuse to the Director of Finance and Administrative Services or the Executive Director immediately. The user should not show the misuse or offending material to other users or discuss these matters with anyone other than the Executive Director, or the Director of Finance and Administrative Services.