SDCRAA HUMAN RESOURCES STANDARDS AND PROCEDURES

Section: **Workplace Practices**
Standard: **COMPUTERS, ELECTRONIC MEDIA & MONITORING STANDARD**
Section #: D-08
Effective: March 15, 2011

See Also: Workplace Privacy; Personal Use of Authority Property; Misconduct; Formal Discipline; Use of Authority-Provided Computer Equipment Off-site; Use of Authority-Provided Commercial Cell Phone Devices

General Standard

The purpose of this standard is to ensure the appropriate use of the San Diego County Regional Airport Authority ("Authority") information technology systems. It also establishes guidelines for the proper usage and retention of the Authority's electronic records in compliance with all applicable statutes and policies.

The Authority's information technology systems are intended for the sole purpose of helping employees productively communicate, gather and retain information to achieve Authority business objectives in a way that adds value to the Authority. Added value means it helps you, your co-workers, our customers and tenants to do their jobs and solve problems; helps to improve knowledge or skills; contributes directly or indirectly to the improvement of operations, processes and policies; or helps to promote the Authority's mission, vision and values. The systems include, but are not limited to:

1. Social Networking
2. Software
3. Computers
4. Internet and intranet
5. E-mail and email systems
6. Authority computer systems, including portable systems and desktop systems
7. The Authority intranet and Internet connections
8. Authority pagers, cell phones, and radios

All information processed and contained in the Authority computer systems is the property of the Authority. Violation of these guidelines is grounds for corrective action, including loss of privileges and/or discipline, up to and including termination of employment.

Personal Responsibility

By accepting an account password, related information, accessing Authority's network, intranet and Internet system, an employee and other individuals with approved access to the Authority's information system agree to adhere to the organization's standards and guidelines regarding their use. Individuals also agree to report any misuse related with the Compliance section of this standard.

Access

The Authority reserves the right to suspend an individual's access at any time, without notice, for technical reasons, possible use violations, security or other concerns as deemed or identified by management. Any suspension of an individual's access to the information system must be approved by the Director, Human Resources or his/her designated representative.

Privacy

The Authority's information technology system is intended solely for the business purposes of its employees, authorized contractors, and other specifically designated users. Use of the computer and system must be in compliance with Authority's Standards and Guidelines. Unauthorized use is prohibited. Authority's computer and all information stored within are the property of the organization.

The Authority may monitor any activity on the system, including personal activities such as accessing personal email accounts, social networking sites (e.g., Twitter, Facebook, etc.) and other websites as well as retrieve any historical usage data and information stored within the system. By accessing and using the Authority's computer, individuals are consenting to such monitoring and information retrieval. Users of the Authority's computer systems should have no expectation of privacy as to any communication or information stored within these systems, including information stored locally on the hard drive[s] or other storage media in use with these systems. Individuals are advised that computer activities are automatically stored and copies of the information received or transmitted can be easily recovered and viewed. Internet usage is monitored to ensure that the main use of the Internet connection is for business purposes.

Definition of Electronic Communication Systems/Media

Writing includes any handwriting, typewriting, printing, photostatting, photographing, photocopying, transmitting by electronic mail or facsimile, and any other means of recording upon any tangible thing of any form or communication or representation, including letters, words, pictures, sounds, or symbols or combination thereof and any electronic record thereby created, regardless of the manner in which the record has been stored.

Record includes any document, data, or data set relating to the conduct of public business prepared, owned, used, or retained by the Authority regardless of physical form or characteristics.

Electronic Record as defined by The Uniform Electronic Transaction Act ("UETA"), "A record created, generated, sent, communicated, received or stored by electronic means." The UETA requires that electronic records must be capable of retention by the recipient.

Material is defined as any visual, textual, or auditory article.

Blogs include web -based content consisting primarily of periodic articles or essays listed with the latest entry and visitor comments at the top.

Chat Room includes an online forum where people can broadcast messages to others connected to the same forum in real time.

Instant Messaging (IM) includes a software tool that allows real time electronic messaging or chatting.

Listserv includes an electronic mailing list software application also known as "discussion lists" to send and receive messages from other subscribers.

Online Forum includes a web application where people post messages on specific topics. Forums are also known as web forums, message boards, discussion boards and discussion groups.

Peer to Peer (P2P) File Sharing includes directly sharing content like audio, video, data, software or digitally formatted contents between any two computers.

Social Networks/Social Media includes all on-line communications websites promoting a "circle of friends" or "virtual communities" such as dating websites, Facebook, Friendster, LinkedIn, MySpace, Plaxo, Twitter, and Yahoo! Groups where participants are connected based on various social familiarities or common interests.

Wiki a web application that allows a user to add and edit content.

Ownership & Monitoring

Unless contractual agreements dictate otherwise, all information stored on or transmitted by the Authority computer and communication systems is the Authority's property. To properly protect and maintain this property, the Authority reserves the right to access and/or examine all information stored in or transmitted by these systems at any time, with or without notice, in its sole discretion.

An information technology tool will be used to monitor access of all Authority computer and communications systems. All access, usage and content captured by the monitoring tool will be evaluated periodically by the Human Resources Department for appropriateness. A course of action will be determined in partnership between the Human Resources Department and the department director of an individual who is deemed to have excessively and/or inappropriately operated Authority's information technology systems.

Legal Risks

E-mail is a business communication tool and all individuals with access to the Authority's information systems are obliged to use this tool in a responsible, effective and lawful manner. Although, by its nature, e-mail seems to be less formal than other written communications, the same laws apply. Therefore, it is important that users are aware of

the legal risks of e-mail, text messaging, instant messaging and activities associated with social networking, especially those which may result in the user and the Authority being held liable. Users' adherence to these guidelines can minimize the legal risks involved in the use of e-mail system and other electronic communication tools.

E-mail

Electronic Communication Tools - Prohibited Activities

The use of the Authority's computers, networks, intranet and Internet access are tools to aid individuals with access to the Authority's information systems in achieving the organization's goals and may be revoked at any time for inappropriate conduct. Using the Authority's communications systems to create, view, transmit or receive racist, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited. Such material violates the Authority's work standards guidelines and is subject to disciplinary action.

Individuals must promptly exit, report and not attempt to access again inappropriate sites that are inadvertently accessed on the Authority's computers. Individuals are prohibited from using the Authority's network, e-mail, Internet and/or intranet access for the following (the list is not all inclusive but merely examples):

1. Making offensive or harassing statements based on race, color, religion, national origin, veteran status, ancestry, disability, age, gender, sexual orientation or transgender status.

2. Viewing, listening, sending, printing, forwarding or receiving messages containing defamatory, offensive, harassing, false statements, abusive, obscene, pornographic, threatening, racially offensive, sexual preference or gender related slurs, jokes and/or images that are disrespectful, discriminatory or illegal material.

3. Accessing sites featuring pornography, terrorism, violence or theft.

4. Gambling or engaging in any other activity in violation of any law.

5. Accessing online dating sites.

6. Accessing online streaming videos and online music stations.

7. Engaging in unethical activities or content that encourages the use of controlled substances and/or uses the system with criminal intent.

8. Participating in activities, including the preparation or dissemination of content, which could damage the Authority's image or reputation.

9. Sending, printing or disseminating Authority's proprietary data and protected messages, or any other information deemed confidential, without permission to unauthorized persons.

10. Operating a business, soliciting money for personal gain or otherwise engaging in commercial activity outside the scope of employment or contract.

11. Permitting or granting network or system access to a person outside the organization including, but not limited to, someone whose access has been denied or terminated.

12. Using another individual's password without their consent or impersonating another person while communicating, accessing the network or Internet or sending e-mail using another individual's account without approval.

13. Introducing a virus, harmful component or malicious tampering with any of the Authority's computer systems.

14. Causing congestion, disruption, disablement, alteration, or impairment of the Authority's networks or systems.

15. Using or participating in online games.

16. Defeating or attempting to defeat security restrictions on the Authority's systems and applications.

17. Violating or infringing on the rights of another person, including the right to privacy.

18. Sending unsolicited personal business and/or non-Authority related e-mail messages to groups of recipients (SPAM).

19. Repeated attempts to access sites or content listed in this Prohibited Activities section is a violation of this standard.

Software Usage

Software piracy is both a crime and a violation of the Authority's Software Usage standard. All individuals are to use software strictly in accordance with its license agreement. Unless otherwise provided in the license, unauthorized duplication of software is a violation of the Authority's standards and may be a violation of the law. To ensure compliance with software license agreements, all individuals with access to the Authority's information systems must adhere to the following:

1. Individuals must use software in accordance with the manufacturer's license agreements. The organization does not own the copyright to software licenses. Individuals may not make additional copies of software, unless expressly authorized by management.

2. Individuals are not permitted to install their personal software on the Authority's computer system or copy software from the organization's computer for installation on home or another computer.

3. All software used on Authority owned computers will be purchased through appropriate procedures. Consult the Information Technology Department for guidance on purchase of software and/or computer related tools.

4. Individuals must not be involved in incidents of unapproved system cracking (hacking), password cracking (guessing), file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures, which may be unlawful, and may be considered serious violations of Authority policy.

5. No Authority owned hardware, such as desktop computers, laptops, netbooks, etc; their internal components or other peripherals; may be moved from its current location or taken outside of Authority property by any individual without appropriate approval. An exception is made where a laptop computer is assigned to a specific user or signed out on loan, in which case consent automatically is granted to remove the laptop from Authority property.

6. Each individual is responsible for regularly reviewing, deleting, and generally keeping free of clutter information stored on the Authority's electronic communication systems.

7. Individuals' computer and electronic communication systems passwords must always be kept confidential and not shared with others. If a member of the IT department Help Desk requests, during the course of their duty, and utilizes an individual's login/password, other than their own, the login/password owner must immediately reset their password in order to maintain proper security.

E-mail Standards

The Authority considers e-mail an important means of communication and recognizes the importance of proper e-mail content and speedy replies in conveying a professional image and delivering good customer service. Users should take the same care in drafting e-mail as they would for any other written communication.

Maintenance and Retention

Due to the perceived informality of e-mail, it is easy to forget that e-mail can be a public record and shall be held to the same standards as any physical record and may be discoverable in litigation.

E-mail records classified as "official records" are subject to the Authority's adopted record's retention schedule and must be retained for the same period of time as the record series that most closely matches the subject matter contained in the e-mail message. There are two categories for E-mail: Junk/Transitory and Record

Junk/Transitory e-mail is any e-mail not used in the course of Authority business, and has no administrative or working value, long or short term.

Specific examples of junk/transitory e-mail include personal e-mails, advertisements, meeting or luncheon reminders, work-in-progress messages (messages transmitting draft documents which gives no direction or final decision), social notifications/intra-office notices, phone messages and/or any messages received via "CC" or "BCC". If e-mail is classified as junk/transitory, it should be deleted when it is no longer of value.

An e-mail is considered a record if it explains, justifies, or documents an action or decision in the course or conduct of Authority business. Said e-mail, as with any physical record, will have an active and inactive period and will have the same retention period as any equivalent physical record. Specific examples of this type of e-mail include:

- Memoranda and/or correspondence regarding contracts, agreements, leases, case files or any other identified record within the Authority's records retention schedule.

- Memoranda and/or correspondence e-mail such as those establishing and/or amending policies and guidelines.

- Memoranda and/or correspondence e-mail giving direction to take action.

The sender or generator of the e-mail is typically considered the owner of record and is, therefore, the designated record keeper of that e-mail. However, a recipient may also have recordkeeping responsibilities if he/she is asked to take action that explains, justifies, or documents an action or decision. As the owner of record, one is responsible to print out a file copy or move the e-mail to the appropriate network storage drive for storage. The e-mail should then be retained in the same manner as any other physical record in the same record series or category.

Because the e-mail system is not a record storage and maintenance system, there is a limitation on the size of one's e-mail account. Users will be notified when the capacity is reached and the system will not allow the sending of new messages until action is taken to delete junk/transitory e-mail and/or properly store and maintain e-mail records outside the e-mail system. If an e-mail falls within the record category, it must be maintained as outlined above.

Confidential and Sensitive Information

Confidential and sensitive information, such as performance reviews, disciplinary actions, and similar information, should be designated as private and restricted to those who have a need to know only, when communicated via e-mail.

1. For a private communication, interoffice mail should be used and the item should be marked as "confidential."

2. E-mail can be used to communicate with General Counsel's staff, but should be marked as a "Confidential and Privileged Attorney Client Communication" or "Attorney Work Product", as appropriate.

3. Information regarding confidential matters and negotiations should be marked as "Confidential and Privileged Work Product".

4. If the communication is "confidential and privileged", the intended recipient should be notified prior to transmission.

Electronic Communication Media:

Individuals may exercise limited personal use of Authority systems, so long as such use does not:

1. Suggest or imply that the Authority in any way endorses or supports any views expressed in personal e-mail or other electronic communication.

2. Impede or interfere with the normal processing of e-mail.

3. Hide or misrepresent the sender of the message.

4. Engage in acts of hostility, violence, obscenity, profanity, vulgarity, defamation or cause extended personal use during business hours.

Electronic communications should not replace face-to-face contact and should only be sent when necessary. While engaged in any form of electronic communication, the following standards apply:

1. Primarily used for sending and receiving work-related communications.

2. Must be professional, respect your audience, be discreet and represent the Authority well.

3. Electronic communications including e-mails should be short, well-structured with a descriptive subject line. Electronic communications or statements should clearly state expected action of the recipient.

4. E-mail style is informal and is not always required to follow formal letter format (e.g., salutation/greeting, signature closing, etc.). The style and tone of the e-mail should be tailored to best fit the situation, recipient, and intended outcome of the communication.

5. All electronic communications including e-mails sent externally must contain the sender's name, job title, company name and address, e-mail address and phone number.

6. Links to documents should be used as an alternative to attachments when

communicating internally.

7. Messages should not be written in ALL CAPITALS, as in e-mail etiquette, this is considered shouting.

8. Be sure to select the proper tool to communicate the information---if you would not say it on the air or have it in print in the newspaper, don't say or write it.

9. E-mails should be marked as important only if they really are.

10. Authority's approval is required for authors who use the organization's electronic resources to blog, tweet or post other public messages.

11. Ensure your online profile and related content is consistent with how you wish to present yourself with colleagues. Do not use the Authority's logo and/or trademarks in your profile.

12. Assume at all times you are representing the Authority when engaging in any electronic communications, including social networking.

13. Exercise discretion, thoughtfulness and respect for your colleagues, business associates, customers and our tenants. Do not engage in public criticism or disparagement.

14. Do not discuss internal policies or operations issues in any manner that could reflect poorly on the Authority.

15. Confidential or proprietary Authority information and/or that of a third party should not be shared on any communications and social networking site.

16. Know and follow Authority standards and codes of conducts.

17. Participating in employment and training-related and other Authority business discussions.

18. Be mindful that all public communications that reference the Authority, including social networking communications, are subject to review by the Authority, and may lead to discipline, to the extent the public communications harms the Authority.

Social Computing

The Authority views social media as significant contemporary forms of communication with potential hazards to the Authority's systems due to the proliferation of viruses on such sites. Engaging in social networking during the workday can, when not done in the course of one's work (e.g., Ambassablog), negatively impact productivity and work performance and potentially create systemic risks. Therefore, it is each individual's responsibility to

manage their social networking so that it does not impact productivity, cause performance issues, and/or expose the Authority's systems to risk of viruses and/or hacking.

Compliance

Any individual who becomes aware of a violation of this standard should immediately report the violation to their supervisor, any member of management or a Human Resources Department representative. Identifying the level of discipline will be determined by the department head in conjunction with the Human Resources Department.

Violations of this standard may result in disciplinary action up to and including termination depending on the severity of the situation and its impact on the Authority.