Orange County Power Authority Policy No. 008
Computer Use and Email Management Policy

PURPOSE

The purpose of this Computer Use and Email Management Policy (Policy) is to establish standard operating procedures, guidelines and clear and concise boundaries for the use of the Orange County Power Authority (Authority) Network, as defined below, and ensure that Authority personnel use computing technology in a responsible, efficient, ethical, and legal manner. Use of the Authority Network and the data stored thereon is the property of Authority and is to be used for valid business functions and authorized purposes only. This Policy also prevents the unauthorized access to or disclosure of sensitive information prepared, owned, used, or retained by Authority and complies with the California Electronic Communications Privacy Act.

GENERAL

Personal use of the Authority Network that is deemed to be excessive, interferes with performance by Authority personnel, or that is intended for personal monetary gain, is strictly prohibited.

Those in violation of this Policy could be subject to disciplinary action up to and including dismissal and/or termination of contract, as described in further detail under the "Violations" section of this Policy.

All questions regarding the interpretation or applicability of this Policy should be directed to the Human Resources Department for clarification.

APPLICABILITY

This Policy will apply to all who may have access to or use of the Authority Network or have been issued Authority-owned technology, including all Authority personnel. Furthermore, this Policy applies when Authority-issued technology is used on or off Authority property, when non-Authority devices access the Authority Network or are used to prepare or receive information within the scope of Authority employment, and when private information is prepared, used, or retained by the Authority.

DEFINITIONS

Term	Definition
Authority Network	Any Internet access, computer server, computer network, intranet, local area network, wireless network, email system, cloud storage system, or file-sharing system owned or made available by Authority.
Authority personnel	Collectively refers to all Authority employees, officers (including Board members and members of advisory bodies), consultants, volunteers, and other non-employees who create, transmit, or retain electronic communications related to Authority business.
Electronic communications	Any and all electronic transmissions, and every other means of recording upon any tangible thing in any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored. Without limiting the nature of the foregoing, "electronic communications" include e-mails, texts, voicemails, and also include communications on or within commercial applications (apps) such as Facebook Messenger, Twitter, WhatsApp, etc.
Electronic device	A device depending on the principles of electronics and using the manipulation of electron flow for its operation, including but not limited to cellular telephones, laptops and desktop computers, hotspots, tablets, pagers, cameras, televisions, and DVD/CD players.
Electronic mail (email)	Electronic messages sent within an email application (e.g. Microsoft Outlook) or other email platform(s) (e.g., Gmail, Yahoo!, etc.).
Electronic messaging account	Any account that creates, sends, receives or stores electronic communications, such as email messages or text messages, or voicemail messages.
Excessive use	Use is defined as "excessive" if it interferes with normal job functions, impacts responsiveness, and/or the ability to perform daily job activities.
Listservs	A messaging function hosted by server computers that automatically mails messages to subscribers and can also be referred to as "electronic bulletin boards."

INAPPROPRIATE USE

1. The Authority Network shall not be used for any activity that is a violation of local, state, or federal law or to further private or personal business activities.

2. Authority personnel may not intentionally intercept, eavesdrop, record, read, alter, or receive another person's electronic communications without proper authorization.

3. Authority personnel are prohibited from using the Authority Network to transmit any electronic communication containing or expressing:

a. Messages in support or opposition to campaigns for candidates for an elected office or a ballot measure, or that otherwise involve partisan politics;

b. Messages of a religious nature or promoting or opposing religious beliefs;

c. Messages containing language which is insulting, offensive, disrespectful, demeaning, or sexually suggestive;

d. Messages containing harassment of any form, sexual or ethnic slurs, obscenities, or any representation of obscenities (which violates the Authority's anti-harassment policies and is subject to Authority disciplinary action);

e. Messages that promote, foster, or perpetuate discrimination on the basis of race, creed, color, age, religion, gender, marital status, or status with regard to public assistance, national origin, physical or mental disability or sexual orientation, as well as any other category protected by federal, state, or local laws (which violates the Authority's anti-harassment policies and is subject to Authority disciplinary action);

f. Messages used to send or receive copyrighted material, proprietary financial information or similar materials, unless the transmission of such material is directly related to Authority business;

g. Messages used for gambling or any activity that is a violation of local, state, or federal law;

h. Threats of violence or injury to any person, property, or organization;

i. Messages that conduct or encourage illegal activity;

j. Messages containing pornographic materials;

k. Messages containing chain letters or other forms of junk mail generally containing unsolicited commercial and non-commercial messages transmitted as a mass mailing to a number of recipients;

l. Messages that cause disruption in the performance of reliability of the Authority Network; and

m. Messages that defeat or attempt to defeat security restrictions on the Authority Network.

4. Electronic communications relating to Authority business, whether located on the Authority Network, an Authority device, or a personal electronic device or account:

(a) are considered "public records" under the California Public Records Act and may be subject to disclosure; and (b) may be required to be retained by the Authority under Authority's Records Retention Policy. To help ensure proper retention of records and compliance with the California Public Records Act, the use of personal electronic messaging accounts or personal devices to conduct Authority business where such messages or other records are not saved or otherwise available on the Authority Network is strongly discouraged.

a. Authority personnel should use reasonable efforts to use Authority devices and accounts and/or the Authority Network whenever possible, and are encouraged to forward and/or copy messages sent or received on non-Authority devices or accounts to their Authority devices or accounts or the Authority Network on an ongoing basis. Authority personnel who use a non-Authority device or account for Authority business shall make public records on the device or account available to the Authority upon request.

b. In the event that the Authority receives a Public Records Act ("PRA") request, subpoena, or other request that either explicitly seeks documents on non-Authority devices or accounts or can be reasonably interpreted as such, the Authority will promptly communicate the request to the relevant Authority personnel who may be in possession of responsive records.

c. Authority personnel shall provide responsive public records to the Authority's PRA coordinator. These records are still subject to review and redactions for PRA exemptions before production. Authority personnel shall provide responsive public records regardless of the potential exemptions.

d. Records that do not relate to the conduct of the public's business need not be provided to the PRA coordinator. In the event that any Authority personnel makes a decision to withhold any responsive records that do not qualify as public records, he or she shall submit a statement with facts sufficient to show the record is not related to Authority business. The Authority shall determine whether the statement has sufficient information.

e. Employees who are terminating their employment with the Authority shall provide any public records on their non-Authority devices or accounts to the PRA coordinator before the last day of their employment.

MONITORING

1. Authority personnel have no right or expectation of privacy or confidentiality in any electronic communication created, sent, received, deleted, or stored using the Authority Network or on an Authority-issued device.

2. The Authority owns the rights to all data and files in any computer, network, or other information system used by Authority. The Authority reserves the right to retrieve and make proper and lawful use of any and all electronic communications transmitted through the Authority Network or on Authority-owned technology. As a routine matter, the Authority does not read or monitor the content of electronic communications created, sent, received, deleted, or stored through the Authority Network or on Authority-owned technology. However, the Authority may monitor or access such electronic communications as allowed by the Electronic Communications Privacy Act, the federal Stored Communications Act, and any other applicable federal or State laws.

3. Most communications among Authority personnel are not confidential communications. However, certain communications such as personnel records, customer data, or attorney-client communications may be or contain confidential information. Questions about whether communications are confidential, and how they are to be preserved, should be discussed with the Authority's Record Retention Coordinator or General Counsel if a Records Retention Coordinator is not yet assigned. When in doubt, DO NOT USE email, text messages, or voicemail messages as a means of communication. Furthermore, the use of passwords to protect documents does not guarantee confidentiality or security.

4. Authority personnel shall not disclose personal, confidential, or privileged information prepared, owned, used, or retained by the Authority or on behalf of the Authority, unless expressly permitted by the Authority's legal counsel or required by law.

5. When the release of personal information prepared, owned, used, or retained by the Authority is authorized, Authority personnel will only use Authority-issued electronic messaging accounts or an Authority-approved file sharing or collaboration service to transmit such identifiably personal information.

6. Authority personnel shall not forward messages from their Authority-issued electronic messaging account to any non-governmental account(s) for the purpose of creating a personal email archive of any record related to Authority business.

7. The Authority may comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual computer and email activities. No Authority personnel member may access another's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate Authority official.

ELECTRONIC MAIL

1. All Authority employees (and certain other personnel designated by the Chief Executive Officer) shall be issued an Authority email account, and all Authority business conducted through email must only be done within the Authority email account. However, if Authority personnel must use their personal email account to

conduct Authority business, the personnel member must retain the email message in accordance with this Policy and the Authority's records retention policies.

2. 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 to the Authority. Generally, Authority personnel are not to use email for non-governmental business, including, but not limited to: union activities (unless expressly allowed in the collective bargaining agreement or other binding agreement with the Authority); commercial ventures; or religious or political causes. Incidental use of the Authority Network for personal use is permissible pursuant to Government Code § 8314(b)(1) and Penal Code § 424(c), though not encouraged.

3. Authority personnel are responsible for managing their mailboxes, including organizing and deleting any non-Authority related messages.

4. Authority personnel are expected to remember that email sent from Authority email accounts or on behalf of the Authority is a representation of the Authority. All Authority personnel must use normal standards of professional and personal courtesy and conduct when drafting email messages.

5. Authority personnel should avoid "broadcasting" messages and documents unless the message is of interest to all Authority personnel.

6. Spam can contain malicious software that is harmful to the Authority Network. If an email message does not pertain to Authority business, it should be deleted from your email account and not forwarded. Examples include jokes, thoughts for the day, "chain" type email messages, etc. Users shall contact the IT department/representative immediately after a user clicks on any type of spam or malicious software that user believes may be harmful to the Authority.

7. Avoid the use of Authority email accounts to subscribe to non-work related (personal) newsletters or other mailers, as it may create susceptibility for spam or a malicious attack on the Authority Network.

8. The Authority's email system must not be used 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 Authority resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution.

Retention of E-mails Relating to Authority Business

1. All Authority e-mails shall be automatically retained for ninety (90) days after the email was sent/received and be automatically deleted on a rolling basis thereafter, except as provided below.

2. Electronic communications that are owned by the Authority but in the possession of consultants or contractors must also be retained in accordance with this Policy. Whether such electronic communications are owned by the Authority is governed by the agreement between the Authority and the consultants or contractors.

3. Emails may be subject to longer retention periods as determined by the content of the email. Authority personnel shall retain e-mails subject to a retention period longer than ninety (90) days as determined by applicable laws, regulations, and the Authority's Records Retention Policy/Schedule.

4. It is the responsibility of the Authority personnel member sending or receiving an email to determine if it is subject to a retention period of longer than ninety (90) days.

5. All emails subject to a Public Records Act request, subpoena, request for production, court order, litigation hold, or claim against the Authority shall be retained until the matter is completed, plus any additional period required under the Authority's Records Retention Policy/Schedule. If an email is scheduled for automatic deletion, Authority personnel shall save or otherwise move the e-mail to a safe location where it will be retained for the necessary period.

6. Pursuant to the California Environmental Quality Act ("CEQA") and the Authority's Record Retention Policy/Schedule, the Authority shall retain all records required to be retained by law under Public Resources Code § 21167.6(e). This includes, but is not limited to, all written correspondence, including emails sent or received by the Authority, relating to compliance with CEQA or a "project" under CEQA, as well as internal Authority communications, notes, or memoranda related to CEQA compliance or the project. (Cal. Pub. Res. Code § 21167.6(e)(7), (10); *Golden Door Properties v. Superior Court*, 53 Cal. App. 5th 733 (2003)). Authority personnel shall save or otherwise move the e-mails to a safe location where they will be retained for the required period. Non-substantive emails that provide no insight into CEQA compliance or the project (*e.g.*, the equivalent of sticky notes, calendaring faxes, or social hallway conversations), are not subject to this section and may be discarded after ninety (90) days.

7. Authority personnel shall consider an e-mail's attachments when determining whether the email needs to be retained. Admittedly, many email attachments are simply duplicates of documents that are retained elsewhere or are draft versions of documents that might not be retained by the Authority after the final version of the document is complete. However, if the attachment to the email is an official Authority record that must be retained pursuant to applicable law or Authority's Records Retention Policy/Schedule, Authority staff or officials shall preserve the attachment and discard the e-mail after ninety (90) days. If you need help in determining whether an attachment to an email message must be retained, please contact the Records Coordinator.

8. To the extent that it is practical to do so, prior to any Authority employee's separation from the Authority, the employee shall identify any email(s) subject to a retention period of longer than ninety (90) days. If not practical, the Authority employee's supervisor or other designee shall identity any email(s) subject to a retention period of longer than ninety (90) days. All other e-ails shall be deleted after the ninety (90) day period.

9. The following provisions provide direction regarding storing and filing of emails.:

    a. To aid in the effective organization of retained records, Authority personnel may store emails in subfolders on their exchange email server. Emails in a subfolder shall not be subject to automatic deletion after ninety (90) days.

    b. Authority personnel may also store emails in locations other than subfolders that appropriately retain the email, including metadata.

    c. District personnel shall not use PST files to store emails.

    d. When permitted by applicable law, this Policy, and the Authority's Records Retention Policy/Schedule, mails shall be deleted after ninety (90) days in a timely and cost-efficient manner so as to destroy the record without permitting duplicates, either electronic or hard copies. Authority personnel should consider email servers, archives, back-up systems, shared drives amongst Authority personnel, CDs and DVDs, USB Flash drives in storage, and external hard drives. The confidentiality of a record's contents shall be considered when deciding the level of security used in that record's destruction.

    e. To ensure maximum efficiency in the operation of the email system, Authority personnel are directed to regularly delete email messages that do not pertain to Authority business from their mailboxes. Examples of such messages are personal emails, email advertisements/ announcements, or newsletters received via email.

Electronic Mail Tampering

Email 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 email message.

Authority Listservs

1. Listservs hosted on Authority computers, but not operated by the Authority, are to be subscribed to for Authority business purposes only, because the amount of traffic generated by Listservs can significantly impact the email system.

2. Listservs hosted on Authority servers may be created and subscribed to by Authority personnel, subject to approval by the appropriate Executive Staff member. Appropriate postings to these Authority Listservs include: employee recognition announcements; announcement of birth/adoption of a child; announcement of death in family; announcement of hospitalization/severe illness; announcement of employee retirement; and news from staff of various Authority divisions or departments. However, Authority personnel shall not share or disclose others' personal information unless expressly permitted by the Authority's legal counsel or unless required by law.

INTERNET

1. This Policy applies to all uses of the Internet, but does not supersede any state or federal laws or Authority policies regarding confidentiality, information dissemination, or standards of conduct.

2. The Internet is to be used to further the Authority's mission, to provide effective service of the highest quality to the Authority's customers and staff, and to support other direct job-related purposes. Supervisors should work with Authority personnel to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Intranet access are Authority resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications.

3. While accessing the Internet, Authority personnel should conduct themselves appropriately, exercise good judgment, and behave with common courtesy.

4. Authority personnel are individually liable for any and all damages incurred as a result of violating Authority security policy, copyright, and licensing agreements.

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

6. Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive, inappropriate or violate any applicable laws or Authority policies, occurs during personal time (lunch or other breaks), and does not result in expense to the Authority.

7. If Authority personnel are provided hotspots to access the Internet, the Authority is not responsible for any ancillary charges incurred by Authority personnel. Further, the Authority reserves the right to recover any unanticipated costs arising from Authority personnel using an Authority-owned hotspot.

8. In using Authority-provided Internet access, all users must scan for viruses all files that are downloaded from the Internet and comply with license agreements and policies of networks and on-line services accessible via the Internet. Users shall contact the IT department immediately after a user clicks on any type of virus that user believes may be harmful to the Authority.

9. Authority personnel and other users are specifically prohibited from using Authority-provided Internet access:

    a. In a manner or for any purpose that violates a federal, state, or local law, regulation, or ordinance or resolution;

    b. To access or distribute indecent or obscene material or child pornography (see 18 U.S.C. § 2252);

    c. In a manner that interferes with or disrupts the Authority Network, services, or equipment;

    d. To intentionally seek out information, obtain copies or modify files or other data that are private, confidential or not open to public inspection, unless specifically authorized to do so by the file owner;

    e. To copy software without determining that permission to do so has been granted by the file owner;

    f. To represent oneself electronically as another, unless specific permission to do so has been granted; and

    g. To access a website or location on the Internet where a fee is charged. Authority personnel incurring such charges will bear sole responsibility for them, unless otherwise authorized by the Authority.

10. Violation of these policies and/or state and federal laws can lead to disciplinary action, up to and including dismissal and possible criminal prosecution, as described in further detail under the “Violations” Section of this Policy.

SOFTWARE

The Authority 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 Authority personnel may create, use, or distribute copies of such software in a manner that is not in compliance with the license agreements for the software. Additionally, no software should be downloaded, installed, or otherwise applied to Authority computer resources without prior approval from the IT department.

Valid Software Registration or Licensing

Each piece of proprietary software (*i.e.*, Microsoft Word, Microsoft Excel, etc.) operating on an Authority computer must have valid registration (individually for stand-alone personal computers) or must be covered by users' license (if connected to a local area network). Proprietary software and associated documentation are subject to copyright laws and licensing agreements, and are not to be reproduced unless authorized under a licensing agreement. Appropriate documentation to substantiate the legitimacy of the software is necessary. Employees will not use "unauthorized" software on Authority computer resources.

Downloads

It is illegal under federal law to download copies of copyrighted music, games, or videos, using any copying scheme or media format. Downloading of copyrighted, protected materials or software is strictly prohibited. Additionally, downloading of files, software or other items from email or the internet from unknown sources is to be avoided at all costs. Users should contact the IT department if there is any doubt about a download or its source.

INFORMATION SECURITY

Internet/Intranet Security

1. Authority personnel are responsible for respecting and maintaining the security of Authority Network and other electronic resources.

2. Authority personnel shall only use software and hardware that has been authorized for use by the Authority.

3. Use of the Authority Network or technology to obtain unauthorized information, attempt to access information protected by privacy laws, or impersonate other users is strictly prohibited.

4. Do not try to bypass security settings and filters, including through the use of proxy servers.

5. Do not install or use illegal software or files, including unauthorized software or apps, on any Authority-issued electronic devices.

6. All electronic communications or records created, sent, received, deleted, or stored using the Authority Network, using an Authority-owned device, or on a private device or account but within the scope of Authority employment, are the property of the Authority and may only be accessed by authorized Authority personnel. Authority personnel who are separating from employment have no rights to the contents such communications or records.

7. The Authority has taken the necessary actions to assure the safety and security of our network. Any employee who attempts to disable, defeat, or circumvent Authority security measures is subject to disciplinary action, up to and including dismissal.

Passwords

1. A confidential password does not guarantee privacy, nor does deletion mean the Authority cannot retrieve past communications, nor does it suggest that voice mail or email are the property right of the employee. Please refer back to the section of this Policy on “Monitoring.”

2. Passwords and codes will help secure information, but they do not ensure privacy and security. Passwords should be changed periodically to ensure security. Under no circumstances should users share their passwords with anyone else.

LEGAL

If any paragraph, sentence, clause or phrase of this Policy is held unlawful or invalid for any reason, said unlawfulness or invalidity shall not affect the remaining portions of this Policy. Additionally, due to the ever changing facets of the realm of Information Technology and its related areas, this Policy shall not be construed to be all inclusive. Revisions to this Policy shall be made periodically in an effort to keep up with changing technology.

VIOLATIONS

1. Any Authority personnel found to have violated this Policy may have his/her access to the Authority Network limited or revoked completely. Furthermore, unlawful use may result in referral for criminal prosecution.

2. Additionally, failure of Authority personnel to comply with this Policy, following its adoption, may result in one or more of the following:

    a. Disciplinary action, up to and including termination (for Authority employees);

    b. Breach of contract or termination of contract (for Authority consultants); and

    c. Revocation of electronic device privileges.

Computer Use and E-mail Management Policy Acknowledgment

I hereby acknowledge that I have received a copy of the Orange County Power Authority Computer Use and Email Management Policy and that I understand that I am to read and comply with its contents. I am aware that failure to comply with this policy may lead to disciplinary action, up to and including termination. I further understand that if I have any questions about the policy or its contents, I am to discuss them with my supervisor or the Human Resources Department.

_____

Print Employee Name

_____ _____

Employee Signature Date