San Diego Community Power

Information Technology and Security Policy

1.0 PURPOSE

The purpose of this Information Technology and Security Policy ("Policy") is to establish standard operating procedures, guidelines and clear and concise boundaries for the use of the San Diego Community Power ("SDCP") Network, as defined below, and ensure that SDCP personnel use computing technology in a responsible, efficient, ethical, and legal manner. Use of the SDCP Network and the data stored thereon is the property of SDCP 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 SDCP and complies with the California Electronic Communications Privacy Act.

2.0 GENERAL

Personal use of the SDCP Network that is deemed to be excessive, interferes with performance by SDCP 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 Human Resources for clarification.

3.0 APPLICABILITY

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

4.0 DEFINITIONS

Term	Definition
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."
SDCP 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 SDCP.
SDCP personnel	Collectively refers to all SDCP 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 SDCP business.

5.0 INAPPROPRIATE USE

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

3. SDCP personnel are prohibited from using the SDCP 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 SDCP's anti-harassment policies and is subject to SDCP 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 SDCP's anti-harassment policies and is subject to SDCP 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 SDCP 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 SDCP Network; and

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

4. Electronic communications relating to SDCP business, whether located on the SDCP Network, an SDCP 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 SDCP under SDCP'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 SDCP business where such messages or other records are not saved or otherwise available on the SDCP Network is strongly discouraged.

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

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

c. SDCP personnel shall provide responsive public records to SDCP's PRA coordinator. These records are still subject to review and redactions for PRA exemptions before production. SDCP 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 SDCP 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 SDCP business. SDCP shall determine whether the statement has sufficient information.

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

6.0 MONITORING

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

2. SDCP owns the rights to all data and files in any computer, network, or other information system used by SDCP. SDCP reserves the right to retrieve and make proper and lawful use of any and all electronic communications transmitted through

the SDCP Network or on SDCP-owned technology. As a routine matter, SDCP does not read or monitor the content of electronic communications created, sent, received, deleted, or stored through the SDCP Network or on SDCP-owned technology. However, SDCP 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 SDCP 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 SDCP's Record Retention Coordinator and/or General Counsel. 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. SDCP personnel shall not disclose personal, confidential, or privileged information prepared, owned, used, or retained by SDCP or on behalf of SDCP, unless expressly permitted by SDCP's legal counsel or required by law.

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

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

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

7.0 ELECTRONIC MAIL

1. All SDCP employees (and certain other personnel designated by the Chief Executive Officer) shall be issued an SDCP email account, and all SDCP business conducted through email must only be done within the SDCP email account. However, if SDCP personnel must use their personal email account to conduct SDCP business, the personnel member must retain the email message in accordance with this Policy and SDCP'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 SDCP. Generally, SDCP 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 SDCP); commercial ventures; or religious or political causes. Incidental use of the SDCP Network for personal use is permissible pursuant to Government Code section 8314(b)(1) and Penal Code section 424(c), though not encouraged.

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

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

5. SDCP personnel should avoid “broadcasting” messages and documents unless the message is of interest to all SDCP personnel.

6. Spam can contain malicious software that is harmful to the SDCP Network. If an email message does not pertain to SDCP business, it should be deleted from your email account and not forwarded. Examples include jokes, thoughts for the day, “chain” type e-mail 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 SDCP.

7. Avoid the use of SDCP 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 SDCP Network.

8. The SDCP's electronic mail 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 SDCP resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution.

Retention of E-mails Relating to SDCP Business

1. All SDCP e-mails shall be automatically retained for two (2) years after the e-mail was sent/received and automatically deleted on a rolling basis thereafter, except as provided below.

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

3. E-mails may be subject to longer retention periods as determined by the content of the e-mail. SDCP personnel shall retain e-mails subject to a retention period longer than two (2) years as determined by applicable laws, regulations, and SDCP's Records Retention Policy/Schedule.

4. It is the responsibility of the SDCP personnel member sending or receiving an e-mail to determine if it is subject to a retention period of longer than two (2) years.

5. All e-mails subject to a Public Records Act request, subpoena, request for production, court order, litigation hold, or claim against SDCP shall be retained until the matter is completed, plus any additional period required under SDCP's Records Retention Policy/Schedule. If an e-mail is scheduled for automatic deletion, SDCP 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 SDCP's Record Retention Policy/Schedule, SDCP shall retain all records required to be retained by law under Section 21167.6(e) of the California Public Resources Code. This includes, but is not limited to, all written correspondence, including e-mails sent or received by SDCP, relating to compliance with CEQA or a "project" under CEQA, as well as internal SDCP communications, notes, or memoranda related to CEQA compliance or the project. (Pub. Res. Code § 21167.6(e)(7), (10); *Golden Door Properties v. Superior Court* (2020) 53 Cal.App.5th 733.) SDCP personnel shall save or otherwise move the e-mails to a safe location where they will be retained for the required period. Non-substantive e-mails 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 two (2) years.

7. SDCP personnel shall consider an e-mail's attachments when determining whether the e-mail needs to be retained. Admittedly, many e-mail attachments are simply duplicates of documents that are retained elsewhere or are draft versions of documents that might not be retained by SDCP after the final version of the document is complete. However, if the attachment to the e-mail is an official SDCP record that must be retained pursuant to applicable law or SDCP's Records Retention Policy/Schedule, SDCP staff or officials shall preserve the attachment and discard the e-mail after two (2) years. If you need help in determining whether an attachment to an e-mail message must be retained, please contact the Records Coordinator.

8. To the extent that it is practical to do so, prior to any SDCP employee's separation from SDCP, the employee shall identify any e-mail(s) subject to a retention period of longer than two (2) years. If not practical, the SDCP employee's supervisor or other designee shall identity any e-mail(s) subject to a retention period of longer than two (2) years. All other e-mails shall be deleted after the two (2) year period.

9. The following provisions provide direction regarding storing and filing of e-mails.:

a. To aid in the effective organization of retained records, SDCP personnel may store e-mails in subfolders on their exchange e-mail server. E-mails in a subfolder shall not be subject to automatic deletion after two (2) years.

b. SDCP personnel may also store e-mails in locations other than subfolders that appropriately retain the e-mail, including metadata.

c. District personnel shall not use PST files to store e-mails.

d. When permitted by applicable law, this Policy, and SDCP's Records Retention Policy/Schedule, e-mails shall be deleted after two (2) years in a timely and cost-efficient manner so as to destroy the record without permitting duplicates, either electronic or hard copies. SDCP personnel should consider e-mail servers, archives, back-up systems, shared drives amongst SDCP 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 e-mail system, SDCP personnel are directed to regularly delete e-mail messages that do not pertain to SDCP business from their mailboxes. Examples of such messages are personal e-mails, e-mail advertisements/ announcements, or newsletters received via e-mail.

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.

SDCP Listservs

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

2. Listservs hosted on SDCP servers may be created and subscribed to by SDCP personnel, subject to approval by the appropriate Executive Staff member. Appropriate postings to these SDCP 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 SDCP divisions or departments. However, SDCP personnel shall not share or disclose others' personal information unless expressly permitted by SDCP's legal counsel or unless required by law.

8.0 INTERNET

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

2. The Internet is to be used to further the SDCP's mission, to provide effective service of the highest quality to SDCP's customers and staff, and to support other direct job-related purposes. Supervisors should work with SDCP personnel to determine the appropriateness of using the Internet for professional activities and career development. The various modes of Internet/Intranet access are SDCP 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, SDCP personnel should conduct themselves appropriately, exercise good judgment, and behave with common courtesy.

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

5. All SDCP policies and procedures apply to the conduct of SDCP personnel on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, SDCP information dissemination, standards of conduct, misuse of SDCP 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 SDCP policies, occurs during personal time (lunch or other breaks), and does not result in expense to the SDCP.

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

8. In using SDCP-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 SDCP.

9. SDCP personnel and other users are specifically prohibited from using SDCP-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 SDCP 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. SDCP personnel incurring such charges will bear sole responsibility for them, unless otherwise authorized by the SDCP.

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.

9.0 SOFTWARE

SDCP 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 member of SDCP 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 SDCP computer resources without prior approval from the IT department.

Valid Software Registration or Licensing

Each piece of proprietary software (i.e., Word, Excel, etc.) operating on an SDCP 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 SDCP 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.

10.0 INFORMATION SECURITY

Internet/Intranet Security

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

2. For cloud storage, SDCP authorizes SDCP personnel to use OneDrive a file hosting service and synchronization service operated by Microsoft as well as Azure, a comprehensive cloud hosting service.

3. SDCP personnel shall only use software and hardware that has been authorized for use by SDCP.

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

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

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

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

8. SDCP has taken the necessary actions to assure the safety and security of our network. Any employee who attempts to disable, defeat, or circumvent SDCP 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 SDCP 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.

11.0 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.

12.0 VIOLATIONS

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

2. Additionally, failure of SDCP 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 SDCP employees);

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

    c. Revocation of electronic device privileges.

Information Technology and Security Policy Acknowledgment

I hereby acknowledge that I have received a copy of the San Diego Community Power Information Technology and Security 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 SDCP's Human Resources representative.

_____

Print Employee Name

_____ _____

Employee Signature Date