SAN DIEGO ASSOCIATION OF GOVERNMENTS
PART B1: OFFER BOOKLET

Solicitation Title:	Web ADA Compliance Project Assessment
Solicitation Number:	SOL1469413
Issued with:	☒ RFO ☐ Addendum No. _____

OFFEROR INFORMATION FORM

Name of Offeror: _____

Address: _____

Form of Business: _____

Tax ID Number: _____

License Number (if applicable): _____

License Type (if applicable): _____

Is your firm a DBE? ☐ Yes ☐ No

Is your firm a SB? ☐ Yes ☐ No

DIR Registration Number: _____

SAM Unique Entity ID Number: _____

Main point of contact regarding bid:

Name: _____

Title: _____

Email: _____

Phone Number: _____

The work to be done and referred to herein, shall be performed in accordance with all documents incorporated into this offer packet, including but not limited to the Request for Offers (RFO) and all documents incorporated therein.

Offers are to be submitted for the entire scope of work. The amount of the Offer for comparison purposes shall be the total of all offer items, including any options.

Utilizing Part B2: Price Sheet, the Offeror shall set forth for each item of work, in clearly legible figures, an item price for the item in the respective space provided for this purpose. In the case of unit basis items, the amount set forth under the "Total" column shall be the extension of the item prices Offer on the basis of the estimated quantity for the item. Offerors must bid on every item unless otherwise stated in the Price Sheet in order to be deemed responsive.

In case of discrepancy between the item price and the total set forth for the item, the item price shall prevail, provided however, if the amount set forth as an item price is ambiguous, unintelligible or uncertain for any cause, or is omitted, or in the case of unit basis items, is the same amount as the entry in the "Total" column, then the amount set forth in the "Total" column for the item shall prevail in accordance with the following:

A. As to lump sum item prices, the amount set forth in the "Total" column shall be the item price.
B. As to the unit basis items, the amount set forth in the "Total" column shall be divided by the estimated quantity for the item and the price thus obtained shall be the item price.

Per Section 2-III of the Request for Offers (RFO):

"An offer shall be considered responsive when it is in full compliance with all material terms of the RFO, including but not limited to the full completion, execution and, where appropriate, signature of the forms located in the Offer Booklet and Price Sheet. Failure of an Offeror to fully complete, execute, or return a form located in the Offer Booklet may render the offer non-responsive.

SANDAG reserves the right to waive any immaterial irregularity that is the basis of an offer's non-responsiveness if it does not impact the competitive process, in the sole determination of SANDAG."

Authorized person[1] to sign Agreement/Purchase Order:

Name: _____

Title: _____

Email: _____

Phone Number: _____

By execution of this Offer, the Offeror certifies conformance with the requirements and conditions of the terms and conditions referenced in the Request for Offers (RFO).

Offeror Signature: _____ Dated: _____

[1] If Offeror is a corporation, the legal name of the corporation shall be set forth above together with the signature of the officer or officers authorized to sign contracts on behalf of the corporation. If Offeror is a copartnership, the true name of the firm shall be set forth above together with the signature of the partner or partners authorized to sign contracts on behalf of the copartnership. If Offeror is an individual, their signature shall be placed above. If signature is by an agent, other than an officer of a corporation or a member of a partnership, a Power of Attorney must be on file with SANDAG prior to the Deadline for Offer Submittal or submitted with the Offer; otherwise, the Offer will be disregarded as irregular and unauthorized.

BIDDERS LIST

SOL1469413

Proposer | RFO No.

The United States DOT requires SANDAG to create and maintain a Bidders List containing information about all firms (DBEs and non-DBEs) that bid, propose, or quote on the SANDAG contracts in accordance with 49 CFR 26.11. The Proposer is to complete all requested information for every firm that submitted a bid, proposal, or quote, including the Proposer itself and any proposed subconsultants. The Bidders List form shall be submitted with the proposal. SANDAG will utilize this information to assist in the Overall Annual DBE Goal Setting process. The Bidders List content will not be considered in evaluating the Offer or determining award of an Agreement.

<table>
<tr><th colspan="2">Proposer's Information</th></tr>
<tr><td>Name of Prime's Firm:</td><td>Phone: ( ) -</td></tr>
<tr><td>Firm Address:</td><td>Fax: ( ) -</td></tr>
<tr><td>City: ST: ZIP:</td><td rowspan="2">Type of work/services/materials provided:</td></tr>
<tr><td>Number of years in business:</td></tr>
<tr><td>Contact Person:</td><td>Title:</td></tr>
<tr><td>Is the firm currently certified as a DBE under 49 CFR 26? ☐ Yes ☐ No

Proposer has DBE Certification for the firm's majority owner in the following categories (place an "X"):
☐ African American ☐ Asian Pacific American
☐ Native American ☐ Woman
☐ Hispanic American ☐ Subcontinent Asian American
☐ Other

Gender of Majority Owner: ☐ Male ☐ Female</td><td>Check the box below for your firm's annual gross receipts last year:
☐ Less than $1 million
☐ Less than $5 million
☐ Less than $10 million
☐ Less than $15 million
☐ More than $15 million</td></tr>
<tr><td colspan="2">List all NAICS code(s) applicable to each scope of work the firm is seeking to perform in its bid:</td></tr>
</table>

BIDDERS LIST (CONT'D)

Note: Each proposed subconsultant must complete this form and it must be submitted with the Offer.

<table>
<tr><th colspan="2">Subconsultant's Information</th></tr>
<tr><td>Name of Subconsultant's Firm:</td><td>Phone: ( ) -</td></tr>
<tr><td>Firm Address:</td><td>Fax: ( ) -</td></tr>
<tr><td>City: ST: ZIP:</td><td rowspan="2">Type of work/services/materials provided:</td></tr>
<tr><td>Number of years in business:</td></tr>
<tr><td>Contact Person:</td><td>Title:</td></tr>
<tr><td>Is the firm currently certified as a DBE under 49 CFR 26? ☐ Yes ☐ No

Proposer has DBE Certification in the following categories for the firm's majority owner (place an "X"):
☐ African American ☐ Asian Pacific American
☐ Native American ☐ Woman
☐ Hispanic American ☐ Subcontinent Asian American
☐ Other

Gender of Majority Owner: ☐ Male ☐ Female</td><td>Check the box below for your firm's annual gross receipts last year:
☐ Less than $1 million
☐ Less than $5 million
☐ Less than $10 million
☐ Less than $15 million
☐ More than $15 million</td></tr>
<tr><td colspan="2">List all NAICS code(s) applicable to each scope of work the firm is seeking to perform in its bid:</td></tr>
</table>

If necessary, this Bidders List form can be duplicated to include all firms (DBEs and non-DBEs) that have submitted a bid, proposal, or quote on this DOT-assisted Project, whether successful or unsuccessful in their attempt to obtain a contract.

Failure to submit the required Bidders List form may cause SANDAG to deem the proposal for award of an Agreement non-responsive.

WORKERS' COMPENSATION CERTIFICATE

I am aware of the provisions of Section 3700 of the Labor Code which require every employer to be insured against liability for worker's compensation or to undertake self-insurance in accordance with the provisions of that code and I will comply with such provisions before commencing the performance of the work of this RFO.

Executed this _____ day of _____, 20_____.

_____

Official, legal name of Offeror (Type or Print)

Print Name: _____

Title: _____

Signature: _____ Date: _____

PUBLIC RECORDS ACT INDEMNIFICATION CERTIFICATE

I, _____ hereby agree, on behalf of

(Type or Print name)

_____ :

Official, legal name of Offeror (Type or Print)

To indemnify and defend SANDAG in the event SANDAG withholds production of any records submitted in response to this RFO that Offeror has marked "Confidential" "Trade Secret" "Proprietary", or similar designations, in response to a Public Records Act request pursuant to California Government Code section 6250 or a Freedom of Information Act request; and

That all communications and information provided to SANDAG become public records as the property of SANDAG. As such, they may be subject to public review. I have read SANDAG's Board Policy No. 015: Records Management Policy, which is available at www.sandag.org/legal, for additional information; and

That records of Offeror related to SANDAG projects are subject to review and audit by SANDAG and its representatives.

_____

Official, legal name of Offeror (Type or Print)

Print Name: _____

Title: _____

Signature: _____ Date: _____

FALSE CLAIMS CERTIFICATION

OFFEROR'S CERTIFICATION OF COMPLIANCE WITH LAWS RELATING TO FALSE CLAIMS

I hereby certify that if awarded the Agreement or Purchase Order of which this certificate shall be made a part of, I will ensure that Offeror does not violate any provisions of the False Claims Act or any other applicable federal or state laws and regulations relating to the filing of false claims against a public agency, including laws and regulations hereinafter enacted. I additionally certify that in the event it is determined that Offeror or one of its subcontractors has violated the False Claims Act, that such violation shall be grounds for, among other things, debarment pursuant to the policies established by Federal, State, or local law.

_____

Official, legal name of Offeror (Type or Print)

Print Name: _____

Title: _____

Signature: _____ Date: _____

PUBLIC CONTRACT CODE SECTION 10162 QUESTIONNAIRE

In accordance with Public Contract Code Section 10162, the Offeror shall complete, under penalty of perjury, the following questionnaire:

Has the Offeror, any officer of the Offeror, or any employee of the Offeror who has a proprietary interest in the Offeror, ever been disqualified, removed, or otherwise prevented from bidding or proposing on, or completing a federal, state, or local government project because of a violation of law or a safety regulation?

☐ Yes ☐ No

If the answer is yes, explain the circumstances in the space below.

Official, legal name of Offeror (Type or Print)

Print Name: _____

Title: _____

Signature: _____ Date: _____

PUBLIC CONTRACT CODE SECTION STATEMENTS

PUBLIC CONTRACT CODE SECTION 10232 STATEMENT

In conformance with Public Contract Code Section 10232, the Offeror, hereby states under penalty of perjury, that no more than one final unappealable finding of contempt of court by a federal court has been issued against the Offeror within the immediately preceding two year period because of the Offeror's failure to comply with an order of a federal court which ordered the Offeror to comply with an order of the National Labor Relations Board.

PUBLIC CONTRACT CODE SECTION 10285.1 STATEMENT

In conformance with Public Contract Code Section 10285.1 (Chapter 376, Stats. 1985), the Offeror hereby declares under penalty of perjury under the laws of the State of California that the Offeror

☐ has ☐ has not

(Must Check One)

been convicted within the preceding three years of any offenses referred to in that section, including any charge of fraud, bribery, collusion, conspiracy, or any other act in violation of any state or federal antitrust law in connection with the bidding upon, award of, or performance of, any public works contract, as defined in Public Contract Code Section 1101, with any public entity, as defined in Public Contract Code Section 1100, including the Regents of the University of California or the Trustees of the California State University. The term "Offeror" is understood to include any partner, member, officer, director, responsible managing officer, or responsible managing employee thereof, as referred to in Section 10285.1 (reference to "Offeror").

The above statement is part of the offer. Signing the offer on the signature portion thereof shall also constitute signature of this statement. Offerors are cautioned that making a false certification may subject the certifier to criminal prosecution.

_____

Official, legal name of Offeror (Type or Print)

Print Name: _____

Title: _____

Signature: _____ Date: _____

ELIGIBILITY CERTIFICATION FOR FEDERALLY FUNDED CONTRACTS

The award of the Agreement or Purchase Order is subject to a financial assistance contract between the San Diego Association of Governments (SANDAG) and the U.S. Department of Transportation or another federal agency. Any name appearing on the Comptroller General's list of ineligible contractors for federally financed or assisted contracts is not eligible for the Agreement or Purchase Order.

Offeror hereby certifies that neither the Offeror nor any of its officers or holders of a controlling interest are on the U.S. Comptroller General's list of ineligible contractors for federally funded and assisted contracts. In the event the Offeror or any of its subcontractors are included on such a list during the performance of this Project, Offeror shall promptly inform SANDAG of this fact.

_____

Official, legal name of Offeror (Type or Print)

Print Name: _____

Title: _____

Signature: _____ Date: _____

SUBCONTRACTOR'S STATEMENT OF ELIGIBILITY

(To be filled out by each proposed subcontractor and submitted with the Offer.)

_____ certifies that neither it nor its
(Type or Print name)

principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in any federal project by any federal department or agency.

Where the subcontractor is unable to certify any of the statements in the certification, such subcontractor shall attach an explanation with this form.

The subcontractor certifies or affirms the truthfulness and accuracy of the contents of the statements submitted on or with this certification and understands that the provisions of 31 USC 3801, et seq., are applicable.

_____

Official, legal name of Offeror (Type or Print)

Print Name: _____

Title: _____

Signature: _____ Date: _____

NONCOLLUSION AFFIDAVIT/DECLARATION

(Title 23 United States Code Section 112 and Public Contract Code Section 7106)

In accordance with Title 23, United States Code Section 112, and Public Contract Code 7106, the Offeror declares that the Offer is not made in the interest of, or on behalf of, any undisclosed person, partnership, company, association, organization, or corporation; that the offer is genuine and not collusive or sham; that the Offeror has not, directly or indirectly, induced or solicited any other Offeror to put in a false or sham Offer; and has not, directly or indirectly, colluded, conspired, connived, or agreed with any Offeror or anyone else to put in a sham offer, or that anyone shall refrain from offering; that the Offeror has not in any manner, directly or indirectly, sought by agreement, communication, or conference with anyone to fix the offer price of the offeror or any other Offeror, or to fix any overhead, profit, or cost element of the offer price, or of that of any other Offeror, or to secure any advantage against the public body awarding the Agreement or Purchase Order of anyone interested in the proposed Agreement or Purchase Order; that all statements contained in the offer are true; and, further, that the Offeror has not, directly or indirectly, submitted his or her offer price or any breakdown thereof, or the contents thereof, or divulged information or data relative thereto, or paid, and will not pay, any fee to any corporation, partnership, company, association, organization, offer depository, or to any member or agent thereof to effectuate a collusive or sham offer.

Offerors are cautioned that making a false certification may subject the certifier to criminal prosecution.

Any person executing this declaration on behalf of a Offeror that is a corporation, partnership, joint venture, limited liability company, limited liability partnership, or any other entity, hereby represents that he or she has full power to execute, and does execute, this declaration on behalf of the Offeror.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct and that this declaration is executed on

_____ at _____, _____.

Date City State

_____

Official, legal name of Offeror (Type or Print)

Print Name: _____

Title: _____

Signature: _____ Date: _____

DEBARMENT AND SUSPENSION CERTIFICATE

Title 49, Code of Federal Regulations, Part 29

Offeror, under penalty of perjury, certifies that, except as noted below, he/she or any other person associated therewith in the capacity of owner, partner, director, officer, manager:

- is not currently under suspension, debarment, voluntary exclusion, or determination of ineligibility by any federal agency;
- has not been suspended, debarred, voluntarily excluded or determined ineligible by any federal agency within the past three (3) years;
- does not have a proposed debarment pending; and
- has not been indicted, convicted, or had a civil judgment rendered against it by a court of competent jurisdiction in any matter involving fraud or official misconduct within the past three (3) years.

If there are any exceptions to this certification, insert the exceptions in the following space.

For any exception noted above, indicate below to whom it applies, initiating agency, and dates of action.

_____

Official, legal name of Offeror (Type or Print)

Print Name: _____

Title: _____

Signature: _____ Date: _____

EQUAL EMPLOYMENT OPPORTUNITY CERTIFICATE

Offeror hereby certifies that it will comply with the provisions of the San Diego Association of Governments (SANDAG) Equal Employment Opportunity Program (SANDAG Board Policy No. 007), and rules and regulations adopted pursuant thereto, Title VI of the Civil Rights Act of 1964, the California Fair Employment Practices Act, and any other applicable federal and state laws and regulations relating to equal employment opportunity, including laws and regulations hereinafter enacted.

Furthermore, Offeror hereby certifies that it

☐ has ☐ has not

(Must Check One)

been found, adjudicated, or determined to have violated any laws of Executive Orders relating to employment discrimination or affirmative action including, but not limited to, Title VII of the Civil Rights Act of 1964, as amended, (42 U.S.C. 2000(e) et seq.); the Equal Pay Act (29 U.S.C. 206(d)); Executive Order (EO) 10925 (Kennedy, 1961), EO 11114 (Kennedy, 1963), or EO 11246 (Johnson, 1965); or the California Fair Employment and Housing Act (Government Code 12460 et seq.); by any federal or California court or agency, including but not limited to the Equal Employment Opportunity Commission, the Office of Federal Contract Compliance Programs, and the California Fair Employment and Housing Commission.

If the “has” box is marked above, please explain the circumstance.

_____

Official, legal name of Offeror (Type or Print)

Print Name: _____

Title: _____

Signature: _____ Date: _____

TECHNOLOGY AND ELECTRONIC REQUEST PACKET FOR SANDAG "NON-EMPLOYEES"

Technology and Electronic Request Packet
for SANDAG "non-employees"

STEP 1: This form is to be completed and signed by the SANDAG Project Manager (PM) requesting SANDAG's technology and electronic resources to be provided to a non-employee.
STEP 2: The non-employee must read, understand, and sign the policy "Technology and Electronic Resources policy" before these resources will be provided.
STEP 3: After review, the requested resources will be provided.

Non- Employee Information

Name:	
Company Name:	
Company Phone:	
Company Email:	
SANDAG project/s:	
Duration of the Project/s:	
Office location:	
SANDAG Project Manager:	
CIP/OWP Number:	

STEP 1 Resources Requested

SANDAG PM Please list the SANDAG resources needed and a brief description of why the resource(s) is/are needed. Please provide any additional details or notes. A BITS member may contact you if needed for clarification.

SANDAG PM : _____

SANDAG Title: _____

Signature: _____ Date: _____

STEP 2 Non-Employee Acknowledgement.

I have read SANDAG's Use of Technology & Electronic Resources policy and will comply with all of the terms and conditions set forth therein, avoiding activities described in the " Unacceptable Uses" section and will ensure that my use of SANDAG technology resources complies with the policy. Questions regarding the policy or reports of abnormalities or misuse should be reported to the SANDAG Principal Technology Program Manager.

Print Name: _____ Title/Employer: _____

Signature: _____ Date: _____

STEP 3 SANDAG Requested Resources Reviewed and Assigned by: _____ Date: _____

Policy: Technology and Electronic Resources Policy 1

Technology and Electronic Resources Policy

The policy is intended to apply to all technology and electronic resources used for SANDAG business. This policy applies to all users of technology and electronic resources to conduct SANDAG business, whether or not they are employees or independent contractors; whether or not they are using SANDAG technology or resources during or after work hours; or whether they access the technology or resources from SANDAG premises or some other location.

Definitions

The following terms, as defined below, are used in this policy:

- **Communication device** includes, but is not limited to, computers, telephones, mobile devices such as cell phones, smart phones, or tablets, and other similar devices. Communication devices may be owned by SANDAG or may be the personal property of an employee.
- **Computing resources** includes all SANDAG owned, licensed, or managed hardware and software, and use of the SANDAG network via a physical or wireless connection regardless of ownership of the computer or device connected to the network.
- **SANDAG business**: for purposes of this policy and cross-references to this policy, includes, but is not limited to any agency-related activity undertaken either on a mandatory or voluntary basis. It includes actions or activities that either in whole or in part, concern agency matters.
- **SANDAG business record** means a writing that is prepared, owned, used, or retained by the agency because it contains information related to SANDAG business.
- **SANDAG technology and electronic resource** includes, but is not limited to, computing resources, cloud storage services, file and print services, portable electronic storage devices, communication devices, Internet services, Intranet, telephone and voicemail systems, facsimile machines, and photocopiers. SANDAG licenses cloud-based storage, software, and systems which are all considered SANDAG resources. These include, but are not limited to: Microsoft Office 365 applications, SharePoint and OneDrive cloud storage, Team's communications and files; Zoom and other video conferencing systems; YouTube storage, video editing, and broadcasting, and Yammer and digit/social media accounts. Communication devices paid for, in whole or in part (including reimbursement of expenses), by SANDAG are considered SANDAG resources as they are used to prepare and transmit SANDAG business records. (See definitions of *Computing Resources* and *Communication Device* above for more information).

No Expectation of Privacy

Users should not expect that the information placed on or through SANDAG electronic resources is private. By using SANDAG technology and electronic resources, users consent to the monitoring discussed in this policy, without any additional notice. SANDAG employees have no right or expectation of privacy or confidentiality in any message created, sent, received, deleted, or stored using SANDAG technology or electronic resources. All SANDAG business records are the property of SANDAG and may be accessed by authorized staff, regardless of whether they are located on a SANDAG technology and electronic resource or personal resource (personal resources include but are not limited to personal devices or personal accounts). SANDAG electronic communications may be monitored as allowed by the Electronic Communications Privacy Act, the federal Stored Communications Act, and other any applicable federal or state laws. Most communications among SANDAG employees are not confidential communications. Certain communications such as attorney-client communications may be confidential or contain confidential information. Questions about whether communications are confidential, and how they are to be preserved, should be discussed with the Office of General Counsel.

SANDAG 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 SANDAG 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 SANDAG-issued electronic device. SANDAG may, however, require an employee to conduct a reasonable search of personal accounts for SANDAG business records that may be considered public records and disclosable consistent with the California Public Records Act and the SANDAG Public Records Management policy.

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 SANDAG technology and electronic resources are not misused, SANDAG may monitor or investigate computer files, electronic messages, voicemail, Internet use, and all other information kept or accessed by users on its technology or electronic resources (collectively referred to as 'information') to determine whether a user has misused these resources. Users should not expect information stored on or accessed from SANDAG electronic resources to be private, even if passwords, account codes, or other security measures are utilized. Information may be monitored regardless of its origin or content.
- Any information retained on or accessed from SANDAG 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 or former user's computer or voicemail.
- Data scans by law enforcement agencies and SANDAG Information Systems (IS) staff are made on an ongoing basis to check for malware, viruses or other illegal access or use of SANDAG information or equipment that may have been initiated by persons inside or outside SANDAG.

Unacceptable Use

The use of SANDAG technology and electronic resources is a privilege that may be revoked at any time. SANDAG 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 SANDAG technology or electronic resources.
- Violation of the federal Communications Decency Act or any other federal or state law applicable to computer and/or telecommunications systems.
- Obtaining, downloading, viewing, or otherwise gaining access to information or 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 SANDAG policies or applicable laws.
- Use of SANDAG technology or electronic resources for personal gain, commercial purpose outside of SANDAG's business purpose, or political or religious activity. This includes messages in support of or in opposition to campaigns for candidates for an elected office or for a ballot measure and messages of a religious nature, including messages promoting or opposing religious beliefs.
- Use of SANDAG 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 SANDAG 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 SANDAG, 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 permission 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 SANDAG owned logos or trademarks without approval from the Director of Strategic Communications.
- Disclosing confidential, sensitive, or proprietary information/data or allowing or facilitating unauthorized access to such information/data or SANDAG systems in any form.
- 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, Instagram, or Linked-In, or other Internet blogging sites during work hours for non-SANDAG business is forbidden if the time taken to do so or the content of the posting could be disruptive to SANDAG business. Use of social networking sites for SANDAG 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 SANDAG. Employees are expected to be respectful of SANDAG, its employees, member agencies, and the public. If an employee represents

himself/herself/themself on the Internet as a SANDAG employee, he/she/they is expected to ensure the page content complies with professional standards of conduct. Employees are prohibited from accessing, posting, or placing any content using SANDAG property that associates SANDAG with illegal, unethical, or unprofessional activity.

- Establishing Internet or other external network connections that could allow unauthorized persons to gain access to SANDAG 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 SANDAG 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 SANDAG office supplies.

Guidelines for Use of Text Messages and Emails to Conduct SANDAG Business

SANDAG employees who use text messages in performing their job duties should apply the agency's usual standards of professional and personal courtesy and conduct when drafting messages. Like other SANDAG communication, text messages are a reflection of SANDAG business practices.

Similar to emails, text messages should be easy to read and understand. Spelling and grammar should be correct. Avoid group texts and avoid using abbreviations that can be misunderstood or taken out of context.

SANDAG employees are expected to remember that any electronic communication sent from SANDAG accounts are a representation of SANDAG. Employees should apply the agency's usual standards of professional and personal courtesy and conduct when drafting electronic messages. Electronic messages should be drafted with the same care and in the same manner as any communication printed on SANDAG letterhead. Like other SANDAG communication, electronic messages are a reflection of SANDAG business practices.

All messages transmitted over the SANDAG systems should be limited to those which involve SANDAG business activities or contain information essential to SANDAG staff for the accomplishment of SANDAG-related tasks. Use of the SANDAG email system for personal communication must be kept to a minimum.

"Spam" email can be harmful to the computer system. Spam email is electronic junk mail, usually unsolicited commercial and non-commercial messages transmitted as a mass mailing to a number of recipients. Spam should be identified as junk email and deleted immediately. Examples include jokes, thoughts for the day, "chain" type email messages, etc. If an email message is not a SANDAG business

record needed for future use or reference, it is considered "housekeeping" consistent with the Public Records Management Policy and should be deleted from an employee's email account immediately.

Employees may determine that certain SANDAG business records are not needed for future use or reference. Examples may include but are not limited to email and text messages.

- Records that are not needed for future use or reference, and are not required to be kept in accordance with the Records Retention Schedule, may be disposed of if they have been retained for less than 60 days.
- Records that are kept for use or reference for more than 60 days must be kept for a minimum of two years.

Messages should be sent to smaller rather than larger audiences where appropriate. Email should not be used for broadcast purposes, unless the message is of interest to all SANDAG employees.

Remember that while emails, chat messages, and text messages often take a less formal tone, they may be subject to disclosure later; avoid humor, sarcasm, and anger vetting, and avoid use of emoticons and other symbols which can backfire or be misunderstood if disclosure is later required to a broader audience.

Use of Technology While Operating a Vehicle

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

Disclosure of SANDAG Information or Data

SANDAG employees who transfer or copy information or data from SANDAG technology or electronic resources to devices that are not owned or controlled by SANDAG must exercise caution to prevent SANDAG information or data from being hacked or otherwise disclosed. In the event any SANDAG information or data is disclosed to unauthorized persons, or electronic resources containing SANDAG information or data is hacked, lost or stolen, an employee must notify the SANDAG Information Systems Manager within 24 hours.

Consequences of Violating this Policy

The consequences for violating this policy include, but are not limited to, disciplinary action up to and including termination of employment, termination of a user's contract with or services for SANDAG, 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 Information Systems Manager immediately (within 24 hours). 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 their Director or the Manager of Human Resources immediately. The user should not show the misuse or offending material to other users or discuss these matters with anyone other than their Director or the Manager of Human Resources.

For Further Information

Some frequently asked questions and answers (FAQs) are below. For additional guidance on the use of technology and electronic resources at SANDAG, please consult with a member of the Information Technology team.

Amended February 2022

FREQUENTLY ASKED QUESTIONS (FAQs) RELATED TO THE TECHNOLOGY AND ELECTRONIC RESOURCES POLICY

Question 1:
What types of electronic information does the SANDAG Information Technology (IT) Team have access to?

Answer:
The IT Team may inspect, review, and/or monitor electronic media, data, and network traffic stored on or sent through the SANDAG network. Electronic media includes items such as hard drives, thumb drives, and DVD disks. Data refers to email, files, and pictures. Network traffic refers to the various websites that are visited. While the IS Team does not routinely monitor websites that employees visit or examine employee emails, documents, or pictures, they may do so in the course of troubleshooting or as part of an investigation.

Question 2:
Why does the IT Team have access to electronic information?

Answer:
In support of agency business, the IT Team has been granted permission to inspect, review, or access media and data in order to resolve system and network problems, to provide technical support, and to configure, replace, or repair hardware and software. For example, if the SANDAG email system is not working, the IT Team must find out why. Or, if an employee loses media or data during a power failure, access to his or her data/media is required in order to restore what was lost. Monitoring also allows the IS Team to proactively protect SANDAG by detecting, stopping, and removing malicious programs. We also gather statistics from monitoring that are used to plan for future growth.

Question 3:
Who may authorize a search and review of electronic media and under what circumstances?

Answer:
Requests may come from the Office of General Counsel or the Manager of Human Resources. For example, the Office of General Counsel frequently requires the IS Team to search electronic media in order to fulfill a California Public Records Act request or to support discovery efforts during litigation. In addition, the Manager of Human Resources may request a search as part of an internal investigation or as part of an employee relations matter.

Question 4:
Is data stored on my computer's local hard drive private?

Answer:
The local hard drive should not be used for anything but temporary storage of files and data. Local hard drives are not immediately accessible to respond to Public Record Requests and are not backed up by IT and the information and data may not be recoverable if there is a technical failure.

The local hard drive on an employee's computer is considered 'private' in that it cannot be accessed by other employees except as described in this policy The IT Team does have the ability to access files stored on an employee's local hard drive as described in Questions 2, 3 and 4 above, however, would

only do so if specifically instructed to do so by the Office of General Counsel, a Deputy CEO or the CFO, or Manager of Human Resources, or if access is required to provide technical support or to configure/replace/repair hardware or software.

Question 5:
What records are kept as a result of inspecting, reviewing, or monitoring electronic information?

Answer:
The IT Team keeps Internet and network traffic logs that summarize which technology resources are being used and how frequently. This information is kept for a maximum of 45 days and helps the IT Team identify trends and plan for additional resources. For example, while monitoring traffic the IT Team may observe a significant increase in the number of employees using the Internet and not enough Internet bandwidth to meet this need. These logs would justify the purchase of additional Internet bandwidth. Traffic logs also can help the IT Team identify causes behind issues that arise. Traffic logs and use data may also be gathered during an investigation, or in relation to a response to a records request or subpoena.

Question 6:
Who has authority to insert postings on and access SANDAG social media accounts?

Answer:
SANDAG has Facebook, Twitter and other social media accounts that it owns, operates and controls. Only authorized SANDAG staff are permitted to set up, access the account settings, or place new material on these accounts on behalf of SANDAG. Employees who are authorized to set up and manage social media accounts on behalf of SANDAG are required to provide username, password and account information to the IS Team upon request.

Question 7:
I use my personal cell phone, iPad, and/or home computer to access the SANDAG network. Does SANDAG have the right to inspect any of these devices? If so, what would happen to any personal information stored on the device/s?

Answer:
Any device used to access SANDAG electronic resources to conduct SANDAG business – the email system, shared network, etc.- is potentially subject to inspection by the IT Team or the Office of General Counsel in order to respond to a public records request, subpoena, or as part of an internal investigation or employee relations matter. Data stored on SANDAG servers will be subject to disclosure even if a personal device was used, and if SANDAG either purchased or helped finance the purchase of a device or pays the employee a stipend related to the device, SANDAG may be obligated by law to capture data on the device itself. The Office of General Counsel or the Manager of Human Resources would provide direction to the IT Team in such circumstances. Any information found that is pertinent to the requested search would be copied from the employee's device. An employee's personal information from the device may be reviewed by the Office of General Counsel or Human Resources as part of the search process, however, this information would not be divulged if it was not responsive to a legal request for SANDAG records or was exempt by law from disclosure.

Question 8:
I have been provided with a SANDAG cell phone, iPad, laptop, or other communication device and use this to access my personal email account. Can SANDAG view my personal messages?

Answer:
Any information accessed or stored on SANDAG electronic resources is subject to inspection, review, and/or monitoring. This includes personal information such as email messages.

Question 9:
I use my SANDAG email account to send occasional messages to family and friends. Can SANDAG access and view these messages?

Answer:
All messages sent using the SANDAG email system are subject to review and search by authorized agency personnel (Office of General Counsel, Human Resources, IT staff) even if they do not pertain to agency business. Employees should consider the consequences of using the SANDAG email system for personal matters. Although the personal matters may not be considered public records, authorized SANDAG persons may need to review a wide variety of records to determine which ones are personal versus public.

Question 10:
I access my personal email account (Gmail, Yahoo, Hotmail, etc.) from my work computer. Can SANDAG access my personal account?

Answer:
The IT Team may know which email websites an employee has visited, but does not have any detail about messages that were received or sent from the account. Users should note, however, that law enforcement or court actions may lead to use of forensic experts who may be able to obtain detailed information regarding the content of messages even if they are obtained from personal email accounts.