**Exhibit 11**

**special terms and conditions for**

**confidential information and personal information**

These special terms and conditions set forth information privacy and security requirements **[Contractor/Recipient]** must follow when Confidential Information or Personal Information as defined herein is disclosed to **[Contractor/Recipient]**, or is collected, created, maintained, stored, transmitted, or otherwise used by **[Contractor/Recipient]** in the performance of this Agreement. **[Contractor/Recipient]** must ensure that all individuals and entities participating in any way with this Agreement, including but not limited to its officers, employees, agents, subcontractors, subawardees, vendors, and other project partners, comply with these special terms and conditions.

1. ***Order of Precedence***

These special terms and conditions take precedence over any conflicting terms or conditions in any other part of this Agreement.

1. ***Definitions***
	* + 1. “Confidential Information” means information CEC has designated as confidential pursuant to Title 20 of the California Code of Regulations, Section 2505 et seq., information CEC has otherwise deemed or stated to be confidential, and other information exempt from Disclosure under the Public Records Act or any other applicable state or federal laws. **[Recipient/Contractor]** may obtain confidential information from CEC or third parties on behalf of the CEC for the performance of this Agreement.
			2. “Disclose” or Disclosure” refers to the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information.
			3. “Personal Information” means information that meets the definition of “personal information” in California Civil Code Section 1798.3(a) or one of the data elements set forth in California Civil Code Section 1798.29(g)(1) or (g)(2). **Personal information is a type of confidential information and is therefore subject to all requirements for Confidential Information provided in this Agreement and applicable law.** However, there are additional requirements specific to personal information.
			4. “Security Incident” means the theft, loss, damage, unauthorized destruction, unauthorized modification, or any intentional, unintentional, negligent, inappropriate or unauthorized release of any Confidential Information, data classified as confidential, sensitive, or personal, including critical infrastructure information.
2. ***Labeling***

Confidential Information and Personal Information shared by CEC will be provided as follows:

* 1. List Describing Confidential Information and Personal Information. A description of Confidential Information and Personal Information that CEC anticipates it will provide to Recipient is included in Section 19 below. If CEC needs to add items after execution of this Agreement, CEC will update the list and provide a copy to **[Contractor/Recipient]**; and
	2. Identification of Confidential Information. Each individual item of Confidential Information and Personal Information will be visibly identifiable, regardless of file type, before CEC provides access to **[Contractor/Recipient]**. The Confidential Information and Personal Information could be identified as a separate folder, workbook, document, field, electronic tag, etc.
1. ***Use and Disclosure Restrictions***

**[Contractor/Recipient]** and all individuals and entities participating in any way with this Agreement must:

* 1. Protect all Confidential Information and Personal Information from unauthorized Disclosure. This includes but is not limited to implementing administrative, physical, and technical safeguards that reasonably and appropriately protect the privacy, confidentiality, security, integrity, and availability of Confidential Information, including electronic or computerized Confidential Information.
	2. Promptly transmit to CEC’s CAM all requests for Disclosure of any Confidential Information or Personal Information unless prohibited from doing so by applicable state or federal law.
	3. Not use any Confidential Information or Personal Information for any purpose other than performing **[Contractor's/Recipient’s]** work under this Agreement.
	4. Not Disclose, except as otherwise specifically permitted by this Agreement, any Confidential Information or Personal Information to anyone other than CEC without prior written authorization from CEC’s CAM, except when Disclosure is required by State or Federal law.
1. ***Information Security Program Plan.***
	1. Attestation and Review. Before **[Contractor/Recipient]** is provided access to Confidential Information or Personal Information, **[Contractor/Recipient]** must attest, using a form provided by CEC, it has in place an Information Security Program Plan (ISPP) that meets or exceeds the minimum requirements as stated in the California State Administrative Manual Chapter 5300, Information Security (https://www.dgs.ca.gov/Resources/SAM), and any other applicable law. Further, CEC may, at its discretion, also request a copy of **[Contractor’s/Recipient’s]** ISPP for review. After CEC’s review, CEC may choose whether to direct **[Contractor/Recipient]** to perform work that involves Confidential Information or Personal Information.
	2. Content. **[Contractor's/Recipient’s]** ISPP can be represented in a single document or a compilation of documents.
	3. Implementation. **[Contractor/Recipient]** must implement and maintain appropriate procedural safeguards to secure Confidential Information and Personal Information from Security Incidents and unauthorized use for the term of this Agreement. **[Contractor/Recipient]** is responsible for the security and confidentiality of the Confidential Information and Personal Information under its control and the control of its employees, agents, subcontractors, and other project partners and follow the requirements of its ISPP.
2. ***Encryption***

All Confidential information and Personal Information accessed by **[Contractor/Recipient]** must be encrypted in transit and at rest.

1. ***Computer Security Updates***

**[Contractor/Recipient]** must use computer, software and network systems that are updated with the latest security patches, upgrades, and virus software at all times **[Contractor/Recipient]** has access to Confidential Information or Personal Information.

1. ***Nondisclosure Agreements***
	1. Need to Access Confidential Information or Personal Information. **[Contractor/Recipient]** agrees to release Confidential Information and Personal Information only to the individuals who need to access such information to complete work under the Agreement. **[Contractor/Recipient]** must ensure individuals properly handle and secure Confidential Information and Personal Information from unauthorized use or Disclosure, including signed nondisclosure agreements and security awareness training as described in this Section and Section 9, Security Awareness Training, below.
	2. Maintain Current List of Individual Employees. **[Contractor/Recipient]** must maintain a current list, and keep past versions of it, of all individuals who have access to Confidential Information or Personal Information and the dates each individual has access. **[Contractor/Recipient]** must remove individuals who are no longer employed or no longer have access to Confidential Information or Personal Information and add individuals who are subsequently granted access.
2. Nondisclosure Agreement. **[Contractor/Recipient]** must ensure all individuals who will have access to Confidential Information or Personal Information are provided a copy of, and comply with, these special terms and conditions. **[Contractor/Recipient]** must ensure that individuals sign a nondisclosure agreement provided by CEC before being provided access to Confidential Information or Personal Information. The nondisclosure agreement includes maintaining the security of Confidential Information and Personal Information; not disclosing Confidential Information or Personal Information to others; using Confidential Information and Personal Information only for the scope of work in support of the Agreement; providing written notification of any unauthorized release of Confidential Information or Personal Information; destruction of Confidential Information and Personal Information; etc.
3. Copy of Nondisclosure Agreement. **[Contractor/Recipient]** mustprovide a copy of each signed nondisclosure agreement to CEC’s CAM.
4. ***Security Awareness Training***

**[Contractor/Recipient]** must ensure that all individuals who will have access to Confidential Information or Personal Information take security awareness training before being given access to Confidential Information or Personal Information and then annually thereafter until this Agreement ends for any reason, including termination, or the individual no longer has access, possession, use, or control of Confidential Information or Personal Information. The training must include, at a minimum, the following topics: password protection; malware, social engineering, phishing, social media, privacy awareness, acceptable use, and data protection (data collection, storage, transmission, use, disclosure and destruction). Before **[Contractor/Recipient]** allows any individual access to Confidential Information or Personal Information, **[Contractor/Recipient]** must provide to the CAM a copy of that individual’s training certificate.

1. ***Security Incident***
	1. Reporting of Security Incident. If **[Contractor/Recipient]** becomes aware of a potential Security Incident that might affect Confidential Information in this Agreement, **[Contractor/Recipient]** must notify CAM in writing immediately, but no later than 48 hours, after the **[Contractor/Recipient]** first learns of the potential Security Incident. **[Contractor/Recipient]** must promptly provide communications to CAM in writing as new information becomes available during the Security Incident response process.
	2. Prompt Action. **[Contractor/Recipient]** must take prompt corrective action to mitigate any risks or damages involved with the Security Incident and to protect the operating environment, and any action pertaining to a Security Incident required by applicable federal and state laws.
	3. Investigation. **[Contractor/Recipient]** must immediately investigate a Security Incident and provide a written report to CEC as soon as practicable. The report must describe the extent of the Security Incident and **[Contractor’s/Recipient’s]** corrective action to contain the Security Incident and prevent any recurrence. CEC has the right to participate in any investigation of a Security Incident. In addition, CEC has the right to conduct its own independent investigation. **[Contractor/Recipient]** must fully cooperate in all investigations related to the Security Incident. **[Contractor/Recipient]** is responsible for its expenses for conducting its own investigation or participating in the investigation by CEC or other entity selected by CEC.
	4. Notification. If there is a Security Incident that results in the loss of Confidential Information in **[Contractor’s/Recipient’s]** possession, **[Contractor/Recipient]** must comply with any notice requirement under applicable state or federal law. **[Contractor/Recipient]** must, at its sole expense, provide required notices and any other mitigation efforts, with CEC written approval. CEC reserves the right to provide the required notices and any other mitigation efforts.
	5. Costs. In addition to any other rights and remedies available to CEC, **[Contractor/Recipient]** is responsible for, and must promptly pay to CEC, all costs, fees, and any other type of expense incurred by CEC due to a Security Incident resulting from the failure of **[Contractor/Recipient]** to perform, or the intentional, unintentional, negligent, inappropriate or unauthorized acts of **[Contractor’s/Recipient’s]** personnel, that results in an unauthorized Disclosure, release, access, review, or destruction; or loss, theft or misuse of Confidential Information provided to **[Contractor/Recipient]**. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the Security Incident causing loss of Confidential Information. **[Contractor/Recipient]** is also responsible for all costs incurred by CEC due to a Security Incident resulting from the same failure of a subcontractor, lower tier of subcontractor, project partner, match funder or any other entity or person who received Confidential Information under this Agreement.
	6. Subcontracts and Others with Access to Confidential Information. In order that all subcontractors, subawardees, vendors, project partners, and others with access to Confidential information are liable to CEC for costs as detailed in subsection 10.E above, **[Contractor/Recipient]** must include a provision indicating CEC is a third-party beneficiary to all such agreements.
2. ***Additional Requirements for Personal Information***
	1. Possession, Handling, or Use of Personal Information. If **[Contractor/Recipient]** possesses, handles or uses Personal Information during the course of this Agreement, **[Contractor/Recipient]** agrees to comply with the provisions of the Information Practices Act in Civil Code Section 1798 et seq., the California State Administrative Manual chapter 5300 as if **[Contractor/Recipient]** were an “agency” for its work under the Agreement, and any other applicable law. This includes but is not limited to complying with the following:
		1. Maintaining only Personal Information relevant and necessary for the purposes of this Agreement in accordance with Civil Code Section 1798.14.
		2. Maintaining the source or sources of Personal Information in accordance with Civil Code Section 1798.16.
		3. Providing notice on or with any form used to collect personal information from individuals in accordance with Civil Code Section 1798.17.
		4. Establishing appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the Information Practices Act, to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury in accordance with Civil Code Section 1798.21.
	2. Notification. If there is a Security Incident that results in the loss of Personal Information in **[Contractor’s/Recipient’s]** possession, **[Contractor/Recipient]** must comply with the notice requirements in Civil Code Section 1798.29 and California State Administrative Manual chapter 5300. **[Contractor/Recipient]** must, at its sole expense, provide required notices and any other mitigation efforts, with CEC written approval. CEC reserves the right to provide the required notices and any other mitigation efforts.
	3. Rights. **[Contractor/Recipient]** has no ownership, license, or other rights in Personal Information or in any form in which it is used (e.g., Products). In this regard, the Personal Information is not treated like Data, Products, Intellectual Property, or other provisions in the Agreement that may indicate **[Contractor/Recipient]** has ownership, license, or other rights.
	4. Costs. In addition to any other rights and remedies available to CEC, **[Contractor/Recipient]** is responsible for, and must promptly pay to CEC, all costs, fees, and any other type of expense incurred by CEC due to a Security Incident resulting from the failure of **[Contractor/Recipient]** to perform, or the intentional, unintentional, negligent, inappropriate or unauthorized acts of **[Contractor’s/Recipient’s]** personnel, that results in an unauthorized Disclosure, release, access, review, or destruction; or loss, theft or misuse of Personal Information provided to **[Contractor/Recipient]**. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the Security Incident causing loss of Personal Information. **[Contractor/Recipient]** is also responsible for all costs incurred by CEC due to a Security Incident resulting from the same failure of a subcontractor, lower tier of subcontractor, project partner, match funder or any other entity or person who received Personal Information under this Agreement.
	5. Subcontracts and Others with Access to Personal Information. In order that subcontractors, subawardees, vendors, project partners, and others with access to Personal information are liable to CEC for costs as detailed in subsection 11.D above, **[Contractor/Recipient]** must include a provision indicating CEC is a third-party beneficiary to all such agreements.
3. ***End of the Agreement***

When this Agreement ends for any reason, including termination, or sooner if **[Contractor’s/Recipient’s]** work with the Confidential Information or Personal Information has concluded, **[Contractor/Recipient]** must securely destroy all Confidential Information and Personal Information and ensure that each entity with individuals that received Confidential Information or Personal Information does the same. **[Contractor/Recipient]** must not attempt to reuse or distribute Confidential Information or Personal Information after destruction. **[Contractor/Recipient]** must provide written verification to CEC that all Confidential Information and Personal Information has been properly destroyed, including the date and method of destruction.

1. ***Audit***

**[Contractor/Recipient]** must maintain books, records, documents, and other evidence, sufficient to reflect that **[Contractor/Recipient]** properly followed all requirements related to these special terms and conditions for a minimum of three years after final payment, unless a longer period of records retention is stipulated. CEC, other state agencies, and agents designated by CEC have the right to review, copy and audit **[Contractor’s/Recipient’s]** records related to Confidential Information and Personal Information at all reasonable times, with prior notice by CEC. **[Contractor/Recipient]** agrees to provide auditors access to such records during normal business hours and to allow interviews of any individual employees who might reasonably have information related to such records.

1. ***Public Records Act Request***

**[Contractor/Recipient]** must work cooperatively with CEC to respond timely and accurately to Public Records Act requests CEC receives about **[Contractor’s/Recipient’s]** activities and related Confidential Information or Personal Information under this Agreement.

1. ***Termination***

**[Contractor/Recipient]** understands and agrees that in addition to any other rights and remedies available to CEC, any unauthorized release of Confidential Information or Personal Information, or disregard for appropriate security protocols that could result in Confidential Information or Personal Information being released may result in CEC’s termination of this Agreement.

1. ***Survival***

These special terms and conditions will remain in full force and effect in perpetuity.

1. ***Amendment***

**[Contractor/Recipient]** and CEC acknowledge that federal and state laws regarding information security and privacy rapidly evolves and that amendment of these special terms and conditions may be required to provide for procedures to ensure compliance with such laws. **[Contractor/Recipient]** and CEC specifically agree to take such action as is necessary to implement new standards and requirements imposed by regulations and other applicable laws relating to the security or privacy of Confidential Information and Personal Information.

1. ***Flow-down***

**[Contractor/Recipient]** must flow-down these special terms and conditions to all subcontractors, subawardees, vendors, project partners, and other individual or entity participating in any way with this Agreement, including match funding, that will have access to Confidential Information or Personal Information before the individual or entity has access to any such information. **[Contractor/Recipient]** must also require all individuals and entities to flow down all terms in this Exhibit to any lower tier subcontractors, subawardees, vendors, project partners, and other individual or entity participating in any way with this Agreement that will have access to Confidential Information or Personal Information before the individual or entity has access to any such information.

1. ***List of Confidential Information and Personal Information***

The following is a description of Confidential Information and Personal Information that CEC anticipates it will provide to **[Contractor/Recipient]**:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_