

CalSAWS

AMENDED, RESTATED, AND REVISED LEADER REPLACEMENT SYSTEM AGREEMENT

Exhibit Y (Work To Be Performed in GDN – Security, Access and Technology Requirements)

**CalSAWS Consortium,
a California Joint Powers Authority**

1. INTRODUCTION AND OVERVIEW

This Exhibit Y sets forth, the security, access and technology requirements for the performance of Work under the Agreement in CONTRACTOR's Global Delivery Network ("GDN"). The CONSORTIUM agrees and acknowledges that the Work expressly designated in Section 4 of this Exhibit Y will be performed offshore at facilities which are a part of CONTRACTOR's GDN. All Work will be conducted in accordance with all data privacy and security requirements included in the Agreement, including but not limited to, the requirement that all Work performed by GDN personnel must take place within a secure bay dedicated to the Work ("Secure Bay").

2. DEFINITIONS

Terms not otherwise defined in this Exhibit Y shall have the meanings set forth in the Agreement.

A. **Personally Identifiable Information ("PII"):** PII is information that can be used alone or with other information to identify, contact, or locate a single person, or to identify them in context. It includes: (1) A first and last name; (2) A home or other physical address, including street name and name of a city or town; (3) An e-mail address; (4) A telephone number; (5) A social security number; and (6) any other identifier that permits the physical or online contacting of a specific individual. PII also includes information defined as Personal Information in California Civil Code section 1798.3 and section 1798.29(g)-(h).

B. **Protected Health Information ("PHI"):** PHI is, as defined by 45 CFR 160.103, information transmitted or maintained by a covered entity or its business associates in any form or medium. It includes an individual's past, present, or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

C. **Production Data:** The term "Production Data" includes all data falling within the definition of "Program Data," which is defined as all federal, state, county, and/or other data and information: (i) which is (a) stored online, stored off-line, or computed, and used or accessed by CONTRACTOR for providing services under this Base Agreement and all

backups of such data and information, and/or (b) placed into, used within, or resulting from the use of, the CalSAWS Software and all backups of such data and information and (ii) which is not System Data. The term “Production Data” also includes any data containing PII or PHI and also includes any and all case data.

3. ADDITIONAL TERMS

In addition to all of the obligations applicable to CONTRACTOR under the Agreement, CONTRACTOR will provide the following additional controls with respect to Work performed in CONTRACTOR’s GDN. The details regarding these additional controls are set forth in the PCD Deliverable, which is incorporated herein by reference.

A. Secure Bay Requirements

CONTRACTOR will perform all Work within a Secured Bay environment, which will adhere to the following requirements:

- 1) The Secured Bay will be a physically segregated space that is clearly demarked from other common areas by walls and doors capable of supporting both magnetic and key locks.
- 2) Access to the Secured Bay must be controlled and audited via electronic badge system. Individuals may not share badges.
- 3) Only CONTRACTOR staff required for performing Work for CONSORTIUM, and other supporting activities (IT Admin., etc.) will be allowed to access the Secured Bay.
- 4) Security guards must be posted at all entrances of each facility that houses a Secured Bay.
- 5) CONTRACTOR will not authorize copying of any data from the Windows Virtual Desktop Instances (VDIs) to a local computer via copy/paste, screen capture, camera picture, or otherwise under any circumstance.
- 6) All devices such as mobile phones, USB storage devices, other external storage devices, and any other media recording devices will be prohibited. Any exceptions must be explicitly approved by the CONSORTIUM Executive Director.

- 7) All computers in the Secured Bay must be locked down to not allow the use of any external ports and devices including, but not limited to, USB ports, serial ports, and CD/DVD Drives, except when required to deliver the Work (e.g., monitor, keyboard, mouse, network connectivity).
- 8) The use of paper, pens, pencils and printed material may be allowed in the Secured Bay, however, no CONSORTIUM documents or printed materials may be taken out of the Secured Bay by CONTRACTOR staff under any circumstance. Paper must be shredded before discarding. Print capabilities will be restricted to supervisors or other senior management.

B. Virus Protection

- 1) CONTRACTOR's workstations in the Secured Bay will have Symantec Antivirus, IDS Proventia, and PointSec Encryption or substantially similar protections.
- 2) CONTRACTOR will update, operate, and maintain such virus protection and malware prevention software.

C. Workstations

- 1) CONTRACTOR personnel will use the standard CONSORTIUM workstation image build with access to CONSORTIUM's environment.
- 2) CONTRACTOR will limit administrative rights to workstations.
- 3) The workstation environment will meet agreed-upon security requirements (e.g. desktop encryption; updated anti-virus definitions; patch management processes).
- 4) CONTRACTOR will centrally manage operating software patching of workstations. Security patches released by Microsoft will be pushed to workstations and monitored.

D. Security

- 1) CONTRACTOR's personnel located in the Secure Bay will (i) undergo annual information security compliance training, HIPAA awareness sessions, and CONSORTIUM data protection training in order to protect (i) Production Data as defined in Section 2.C of this Exhibit Y and (ii) Program Data and System Data as defined in the Agreement,

from unauthorized use, disclosure or access; and (ii) document attendance at, or completion of, same.

- 2) CONSORTIUM supplied access such as security certificates will be periodically reconciled and inventoried.

E. Reporting and Access

- 1) CONTRACTOR's information security unit will enforce and monitor the Secure Bay and report upon its compliance with the controls to the project team.
- 2) CONTRACTOR will provide reasonable access to its GDN facilities, and equipment by, and make its books and other records pertaining to the Work available to CONSORTIUM to access, inspect, evaluate and audit books and other records pertaining to any aspect of the Work being performed in CONTRACTOR's GDN.
- 3) CONTRACTOR shall provide the CONSORTIUM with rights of access to materials, facilities and persons that the CONSORTIUM may reasonably request in order to monitor on an on-going basis CONTRACTOR's compliance with the requirements described and referenced in this Exhibit Y.

4. WORK TO BE PERFORMED IN THE GDN

A. Subject to the limitations herein and Section 4.1 of the Agreement, CONTRACTOR is authorized to perform Application Development, Application Build and Application Test (including unit, assembly, system, and automated regression testing) activities in GDN locations. This authorization explicitly does not apply to the aspects of such activities addressing the business rules engine, generation of State reports and User Acceptance Testing.

B. In addition to the requirements stated in subparagraph A above, CONTRACTOR must first mask or otherwise obfuscate any Production Data that may reside in any of the test environments described in Subparagraph A above that are accessible from the Secured Bays at any of CONTRACTOR's GDN locations.

C. CONTRACTOR shall comply with, implement, adhere to, align with all applicable State, Federal, and CalSAWS standards, regulations, guidelines and requirements in place as of April 1, 2019. These include, but are not limited to, Social Security Administration

(Technical System Security Requirements), NIST, ADA, and California SIMM / SAM) requirements.

D. The Parties may, at any time, mutually agree in writing (without necessity of an Amendment) to expand the (a) scope of Work performed or (b) data accessed offshore in CONTRACTOR's GDN locations.