

SERVICE AGREEMENT

This Service Agreement ("Agreement") is dated March 11, 2025 and is between Johnson Controls, Inc., a Wisconsin corporation ("Contractor"), and the County of Fresno, a political subdivision of the State of California ("County").

Recitals

A. The County previously purchased Metasys hardware ("Metasys"), a building automation system, and Application and Data Server software ("ADS"), a component of Metasys that collects trend and system configuration data, event messages, and operator transactions, to automate climate control, monitor system performance device failures, and provide notifications to engineering staff.

B. The County's Purchasing Manual allows the County to utilize contracts that have been competitively bid by other government agencies and cooperative purchasing groups, including OMNIA Partners.

C. The Contractor was awarded Agreement No. 2023003491 by The Regents of the University of California ("UC") in California, which has been made available by OMNIA Partners and is based upon the Contractor's response to the competitive bid No. 002815. The Contractor was the most responsive and responsible bidder based on the requirements issued in the bid.

D. The Contractor agrees to provide pricing to the County equivalent or better to the pricing offered under the OMNIA Partner's contract and both parties agree to abide by the terms as set forth within the OMNIA Partner's Agreement No. 2023003491 for the entirety of this Agreement.

E. The County desires to utilize the Contractor's services and pricing, and believes it is in the best interest of the County to contract for necessary building automation system hardware and software.

The parties therefore agree as follows:

Article 1

Contractor's Responsibilities

1.1 **Scope of Services.** The Contractor shall perform all of the services provided in Exhibit A to this Agreement, titled "Scope of Services."

1.2 **Representation.** The Contractor represents that it is qualified, ready, willing, and able to perform all of the services provided in this Agreement.

1.3 **Compliance with Laws.** The Contractor shall, at its own cost, comply with all applicable federal, state, and local laws and regulations in the performance of its obligations under this Agreement, including but not limited to workers compensation, labor, and confidentiality laws and regulations.

1.4 **Confidentiality of Inmates/Wards/Patients/Clients Identity.** Some of the work to be performed under this Agreement may occur in secured facilities or facilities that require confidentiality. The Contractor shall alert and inform its employees and agents that State law requires that the identities of inmates/wards/patients/clients be kept confidential. Revealing the identities of inmates/wards/patients/clients is punishable by law.

1.5 **Security.** Security is of great concern to the County. Failure to comply with the security requirements listed below will be considered a breach of contract and may result in termination of this Agreement. The Contractor's personnel shall cooperate with all County security personnel at all times, and shall be subject to and conform to County security rules and regulations, including, but not limited to the County's security rules and procedures, as detailed in Exhibits E through I. Any violations or disregard of these rules may be cause for denial of access to County property. The background checks required, and policies listed below, may change throughout the life of this Agreement. It is the Contractor's responsibility to request updates from the County. All of the Contractor's employees, agents, and subcontractors must read the policies listed below.

- Exhibit E – Probation Juvenile Detention Facilities – No Hostage Policy
- Exhibit F – Probation Juvenile Detention Facilities – Campus Manual – Vendors, Visitors and Student Interns
- Exhibit G – Fresno Sheriff – Coroner's Office (FSCO) Jail Detention Facilities – No Hostage Policy
- Exhibit H – The Prison Rape Elimination Act
- Exhibit I – Background Investigations & Identification (ID) Badges

1 (A) Security provisions will be strictly enforced. All parties who are required to
2 perform their individual services at the site shall be limited to the area required to complete the
3 services. Such access shall be obtained by notification to the Facility Services Manager or their
4 designee, of the time and place, prior to commencing services.

5 (B) All keys used during construction shall be numbered. Each key issued shall be
6 recorded, and its prompt return shall be strictly enforced. Duplication of any keys issued is
7 strictly prohibited. These keys shall be returned to the County's representative at the end of
8 each working day, when required.

9 (C) Some of the services to be done under this Agreement may be in secured
10 facilities such as jails. Prior to commencement of services, the Contractor, including all
11 subcontractor and contractors, shall obtain security clearances for all employees that will be
12 working or making deliveries to the sites.

13 (D) When services are performed in secured facilities, it is incumbent upon the
14 Contractor to alert all workmen of the necessity for extreme care in accounting for, and keeping
15 all areas free of any and all types of hand tools, power tools, small parts, scrap material, and all
16 other materials which might be concealed upon the person of an inmate/ward/patient, at all
17 times when such tools and materials are not used for the task at hand.

18 (E) Each service area shall be kept clean and in order both during working hours and at
19 the completion of the working day.

20 **Article 2**

21 **County's Responsibilities**

22 2.1 **County Representative.** The County shall provide a County representative to
23 represent the County, who will work with the Contractor to carry out the Contractor's obligations
24 under this Agreement. The County representative will be the County's Facility Services
25 Manager, and/or their designees. The Contractor shall provide a contact person to the County
26 Representative upon execution of this Agreement.

27 2.2 **Modifications of Services.** The Director of Internal Services/Chief Information
28 Officer (Director) or other authorized County staff member acting in the same capacity, or his or

her designee, reserves the right at any time during the term of this Agreement to modify services and/or service levels. The Contractor understands that any increases and/or decreases of service hours will affect the compensation paid or time of performance; however, no additions or removals of service will cause the maximum compensation amount to be exceeded, pursuant to Article 3 of this Agreement.

Article 3

Compensation, Invoices, and Payments

3.1 The County agrees to pay, and the Contractor agrees to receive, compensation for the performance of its services under this Agreement as described in Exhibit B to this Agreement, titled "Compensation."

3.2 **Maximum Compensation.** The maximum compensation payable to the Contractor under this Agreement is \$1,750,000 for the initial three-year term of this Agreement. In the event this Agreement is extended for its first optional one-year extension ("Year 4"), the total compensation payable to the Contractor under this Agreement is \$2,500,000. In the event this Agreement is extended for its final one-year extension ("Year 5"), the total compensation payable to the Contractor under this Agreement is \$3,250,000. In the event the total maximum compensation amount in the Initial Term, Year 4, and/or Year 5 is not fully expended, the remaining unspent funding amounts shall roll over to each subsequent term's established maximum compensation.

The Contractor acknowledges that the County is a local government entity, and does so with notice that the County's powers are limited by the California Constitution and by State law, and with notice that the Contractor may receive compensation under this Agreement only for services performed according to the terms of this Agreement and while this Agreement is in effect, and subject to the maximum amount payable under this section. The Contractor further acknowledges that County employees have no authority to pay the Contractor except as expressly provided in this Agreement.

3.3 **Invoices.** The Contractor shall submit monthly invoices referencing the provided agreement number to the County of Fresno, Facility Services, Attention: Manager, 4590 E.

Cesar Chavez Blvd., Fresno, CA 93702, ISDFacilitiesAP@fresnocountyca.gov. Each invoice shall reference this agreement number, the FAMIS (the County's computerized maintenance management system) work order number, the OMNIA Partners contract number, the date of service, arrival and departure time, address of serviced building, specific area where work was performed, description of services provided, number of service hours and hourly rates for services provided, materials used and cost of materials, notice that warranty of any new material installed was provided, the printed name of the County representative who authorized the work, and the name of the vendor and vendor technician that provided the service. The Contractor shall submit each invoice within 60 days after the month in which the Contractor performs services and in any case within 60 days after the end of the term or termination of this Agreement.

3.4 Payment. The County shall pay each correctly completed and timely submitted invoice within 45 days after receipt. The County shall remit any payment to the Contractor's address specified in the invoice.

3.5 Incidental Expenses. The Contractor is solely responsible for all of its costs and expenses that are not specified as payable by the County under this Agreement.

Article 4

Term of Agreement

4.1 Term. This Agreement is effective upon execution, and terminates three years from the effective date ("Initial Term"), except as provided in section 4.2, "Extension," or Article 6, "Termination and Suspension," below.

4.2 Extension. The term of this Agreement may be extended for no more than two, one-year periods only upon written approval of both parties at least 30 days before the first day of the next one-year extension period. The Director of Internal Services/Chief Information Officer, or other authorized County staff member acting in the same capacity, or his or her designee is authorized to sign the written approval on behalf of the County based on the Contractor's satisfactory performance. The Contractor will provide the County with notice of any adjustments in the Service Agreement price applicable to any renewal period no later than forty-five (45)

1 calendar days prior to the commencement of that renewal period. The extension of this
2 Agreement by the Parties is not a waiver or compromise of any default or breach of this
3 Agreement by the breaching Party existing at the time of the extension whether or not known to
4 the affected Party.

5 **Article 5**

6 **Notices**

7 5.1 **Contact Information.** The persons and their addresses having authority to give and
8 receive notices provided for or permitted under this Agreement include the following:

9 **For the County:**

10 Director of General Services
11 County of Fresno
12 333 W. Pontiac Way
13 Clovis, CA 93612
14 isdcontracts@fresnocountyca.gov

15 **For the Contractor:**

16 Andrew Konkle, HVAC TB Service Manager
17 Johnson Controls, Inc.
18 3451 W. Ashlan Avenue
19 Fresno, CA 93722
20 andrew.konkle@jci.com

21 5.2 **Change of Contact Information.** Either party may change the information in section
22 5.1 by giving notice as provided in section 5.3.

23 5.3 **Method of Delivery.** Each notice between the County and the Contractor provided
24 for or permitted under this Agreement must be in writing, state that it is a notice provided under
25 this Agreement, and be delivered either by personal service, by first-class United States mail, by
26 an overnight commercial courier service, or by Portable Document Format (PDF) document
27 attached to an email.

28 (A) A notice delivered by personal service is effective upon service to the recipient.

(B) A notice delivered by first-class United States mail is effective three County
business days after deposit in the United States mail, postage prepaid, addressed to the
recipient.

(C) A notice delivered by an overnight commercial courier service is effective one
County business day after deposit with the overnight commercial courier service,

1 delivery fees prepaid, with delivery instructions given for next day delivery, addressed to
2 the recipient.

3 (D) A notice delivered by PDF document attached to an email is effective when
4 transmission to the recipient is completed (but, if such transmission is completed outside
5 of County business hours, then such delivery is deemed to be effective at the next
6 beginning of a County business day), provided that the sender maintains a machine
7 record of the completed transmission.

8 **5.4 Claims Presentation.** For all claims arising from or related to this Agreement,
9 nothing in this Agreement establishes, waives, or modifies any claims presentation
10 requirements or procedures provided by law, including the Government Claims Act (Division 3.6
11 of Title 1 of the Government Code, beginning with section 810).

12 **Article 6**

13 **Termination and Suspension**

14 **6.1 Termination for Non-Allocation of Funds.** The terms of this Agreement are
15 contingent on the approval of funds by the appropriating government agency. If sufficient funds
16 are not allocated, then the County, upon at least 30 days' advance written notice to the
17 Contractor, may:

18 (A) Modify the services provided by the Contractor under this Agreement; or

19 (B) Terminate this Agreement.

20 **6.2 Termination for Breach.**

21 (A) Upon determining that a breach (as defined in paragraph (C) below) has
22 occurred, the affected Party may give written notice of the breach to the breaching Party.
23 The written notice may suspend performance under this Agreement, and must provide at
24 least 30 days for the breaching Party to cure the breach.

25 (B) If the breaching Party fails to cure the breach to the affected Party's satisfaction
26 within the time stated in the written notice, the affected Party may terminate this
27 Agreement immediately.
28

(C) For purposes of this section, a breach occurs when, in the determination of the affected Party, the breaching Party has:

- (1) Obtained or used funds illegally or improperly;
- (2) Failed to comply with any part of this Agreement;
- (3) Submitted a substantially incorrect or incomplete report to the County; or
- (4) Improperly performed any of its obligations under this Agreement.

6.3 Termination without Cause. In circumstances other than those set forth above, either Party may terminate this Agreement by giving at least 30 days advance written notice to the other Party.

6.4 No Penalty or Further Obligation. Any termination of this Agreement by a Party under this Article 6 is without penalty to or further obligation of such Party.

6.5 County's Rights upon Termination. Upon termination for breach under this Article 6, the County may demand repayment by the Contractor of any monies disbursed to the Contractor under this Agreement that were not expended in compliance with this Agreement. The Contractor shall promptly refund all such monies upon demand. This section survives the termination of this Agreement.

Article 7

Independent Contractor

7.1 Status. In performing under this Agreement, the Contractor, including its officers, agents, employees, and volunteers, is at all times acting and performing as an independent contractor, in an independent capacity, and not as an officer, agent, servant, employee, joint venturer, partner, or associate of the County.

7.2 Verifying Performance. The County has no right to control, supervise, or direct the manner or method of the Contractor's performance under this Agreement, but the County may verify that the Contractor is performing according to the terms of this Agreement.

7.3 Benefits. Because of its status as an independent contractor, the Contractor has no right to employment rights or benefits available to County employees. The Contractor is solely responsible for providing to its own employees all employee benefits required by law. The

Contractor shall save the County harmless from all matters relating to the payment of the Contractor's employees, including compliance with Social Security withholding and all related regulations that are Contractor's responsibility.

7.4 **Services to Others.** The parties acknowledge that, during the term of this Agreement, the Contractor may provide services to others unrelated to the County.

Article 8

Indemnity and Defense

8.1 **Indemnity.** The Contractor shall indemnify and defend the County (including its officers, agents, employees, and volunteers) against claims for damages, reasonable costs and expenses (including attorney fees and costs), and liabilities of any kind to the County regarding personal injury, including death, or tangible property damage but only to the extent such damages, liabilities and expenses are caused by the negligent acts or willful misconduct of the Contractor under this Agreement. The County may conduct or participate in its own defense without affecting the Contractor's obligation to indemnify or defend the County.

8.2 **Survival.** This Article 8 survives the termination of this Agreement.

8.3 No parties shall be liable in any way for any, incidental, indirect, consequential, exemplary, punitive, or reliance damages, even if such party is advised of the possibility of such damages. Contractor's liability to county arising out of this agreement shall not exceed amounts paid or payable under this agreement.

Article 9

Insurance

9.1 The Contractor shall comply with all the insurance requirements in Exhibit D to this Agreement.

Article 10

Confidentiality & Data Security

10.1 **Confidentiality.** The County and the Contractor may have access to information that the other considers to be a trade secret as defined in California Government Code section 7924.510(f).

1 10.2 Each party shall use the other's Information only to perform its obligations under, and
2 for the purposes of, the Agreement. Neither party shall use the Information of the other Party for
3 the benefit of a third party. Each Party shall maintain the confidentiality of all Information in the
4 same manner in which it protects its own information of like kind, but in no event shall either
5 Party take less than reasonable precautions to prevent the unauthorized disclosure or use of the
6 Information.

7 10.3 Neither Party shall disclose the discloser's data except to any third parties as
8 necessary to operate the Contractor Products and Services (provided that the discloser hereby
9 grants to the recipient, at no additional cost, a non-perpetual, noncancelable, worldwide,
10 nonexclusive license to utilize any data, on an anonymous or aggregate basis only, that arises
11 from the use of the Contractor Products and Services to improve the functionality of the
12 Contractor Products and Services and any other legitimate business purpose, subject to all legal
13 restrictions regarding the use and disclosure of such information).

14 10.4 Upon termination of the Agreement, or upon a Party's request, each Party shall
15 return to the other all Information of the other in its possession. All provisions of the Agreement
16 relating to confidentiality, ownership, and limitations of liability shall survive the termination of
17 the Agreement.

18 10.5 All services performed by the Contractor shall be in strict conformance with all
19 applicable Federal, State of California, and/or local laws and regulations relating to
20 confidentiality, including but not limited to, California Civil Code, California Welfare and
21 Institutions Code, California Health and Safety Code, California Code of Regulations, and the
22 Code of Federal Regulations.

23 10.6 **Data Security.** Both Parties understand that The Contractor only has access to
24 equipment information retrieved by the Metasys system. In no way does Contractor has access
25 to, stores or process any confidential or personal information; however, in the event Contractor
26 has access to such information, both parties agree to be bound by Exhibit J, entitled
27 "Information Security Rider." County is solely responsible for the establishment, operation,
28 maintenance, access, security and other aspects of its computer network, together with those

1 networks of its other third-party vendors (collectively, the “Network”), and shall supply
2 Contractor secure Network access for providing its services. Products networked, connected to
3 the internet, or otherwise connected to computers or other devices must be appropriately
4 protected by County and/or end user against unauthorized access.

5 **Article 11**

6 **Inspections, Audits, and Public Records**

7 **11.1 Inspection of Documents.** Subject to limitations under applicable law, the
8 Contractor shall make available to the County, and the County may examine during business
9 hours that does not disrupt business operations, prior thirty (30) days of written notice, and as
10 often as the County deems necessary, all of the Contractor’s records and data with respect to
11 the matters covered by this Agreement, excluding attorney-client privileged communications.
12 The Contractor shall, upon prior notice and request by the County, permit the County to audit
13 and inspect all of such records and data to ensure the Contractor’s compliance with the terms of
14 this Agreement.

15 **11.2 State Audit Requirements.** If the compensation to be paid by the County under this
16 Agreement exceeds \$10,000, the Contractor is subject to the examination and audit of the
17 California State Auditor, as provided in Government Code section 8546.7, for a period of three
18 years after final payment under this Agreement. This section survives the termination of this
19 Agreement.

20 **11.3 Public Records.** Subject to limitations under applicable law, the County might not be
21 limited in any manner with respect to its public disclosure of this Agreement or any record or
22 data that the Contractor may provide to the County. The County’s public disclosure of this
23 Agreement or any record or data that the Contractor may provide to the County may include but
24 is not limited to the following:

25 (A) The County may voluntarily, or upon request by any member of the public or
26 governmental agency, disclose this Agreement to the public or such governmental
27 agency.
28

1 (B) The County may voluntarily, or upon request by any member of the public or
2 governmental agency, disclose to the public or such governmental agency any record or
3 data that the Contractor may provide to the County, unless such disclosure is prohibited
4 by court order.

5 (C) This Agreement, and any record or data that the Contractor may provide to the
6 County, is subject to public disclosure under the Ralph M. Brown Act (California
7 Government Code, Title 5, Division 2, Part 1, Chapter 9, beginning with section 54950).

8 (D) This Agreement, and any record or data that the Contractor may provide to the
9 County, is subject to public disclosure as a public record under the California Public
10 Records Act (California Government Code, Title 1, Division 10, Chapter 3, beginning
11 with section 7920.200) ("CPRA").

12 (E) This Agreement, and any record or data that the Contractor may provide to the
13 County, is subject to public disclosure as information concerning the conduct of the
14 people's business of the State of California under California Constitution, Article 1,
15 section 3, subdivision (b).

16 (F) Any marking of confidentiality or restricted access upon or otherwise made with
17 respect to any record or data that the Contractor may provide to the County shall be
18 disregarded and have no effect on the County's right or duty to disclose to the public or
19 governmental agency any such record or data.

20 **11.4 Public Records Act Requests.** If the County receives a written or oral request
21 under the CPRA to publicly disclose any record that is in the Contractor's possession or control,
22 and which the County has a right, under any provision of this Agreement or applicable law, to
23 possess or control, then the County may demand, in writing, that the Contractor deliver to the
24 County, for purposes of public disclosure, the requested records that may be in the possession
25 or control of the Contractor. Within five business days after the County's demand, the
26 Contractor shall (a) deliver to the County all of the requested records that are in the Contractor's
27 possession or control, together with a written statement that the Contractor, after conducting a
28 diligent search, has produced all requested records that are in the Contractor's possession or

1 control, or (b) provide to the County a written statement that the Contractor, after conducting a
2 diligent search, does not possess or control any of the requested records. The Contractor shall
3 cooperate with the County with respect to any County demand for such records. If the
4 Contractor wishes to assert that any specific record or data is exempt from disclosure under the
5 CPRA or other applicable law, it must deliver the record or data to the County and assert the
6 exemption by citation to specific legal authority within the written statement that it provides to
7 the County under this section. The Contractor's assertion of any exemption from disclosure is
8 not binding on the County, but the County will give at least 10 days' advance written notice to
9 the Contractor before disclosing any record subject to the Contractor's assertion of exemption
10 from disclosure. The Contractor shall be responsible to the County for any court-ordered award
11 of costs or attorney's fees under the CPRA that results from the Contractor's delay, claim of
12 exemption, failure to produce any such records, or failure to cooperate with the County with
13 respect to any County demand for any such records.

14 **Article 12**

15 **Disclosure of Self-Dealing Transactions**

16 12.1 **Applicability.** This Article 12 applies if the Contractor is operating as a corporation,
17 or changes its status to operate as a corporation.

18 12.2 **Duty to Disclose.** If any member of the Contractor's board of directors is party to a
19 self-dealing transaction, he or she shall disclose the transaction by completing and signing a
20 "Self-Dealing Transaction Disclosure Form" (Exhibit C to this Agreement) and submitting it to
21 the County before commencing the transaction or immediately after.

22 12.3 **Definition.** "Self-dealing transaction" means a transaction to which the Contractor is
23 a party and in which one or more of its directors, as an individual, has a material financial
24 interest.

25 **Article 13**

26 **General Terms**

27 13.1 **Modification.** Except as provided in Article 6, "Termination and Suspension," this
28 Agreement may not be modified, and no waiver is effective, except by written agreement signed

by both parties. The Contractor acknowledges that County employees have no authority to modify this Agreement except as expressly provided in this Agreement.

13.2 **Non-Assignment.** Neither party may assign its rights or delegate its obligations under this Agreement without the prior written consent of the other party.

13.3 **Governing Law.** The laws of the State of California govern all matters arising from or related to this Agreement.

13.4 **Jurisdiction and Venue.** This Agreement is signed and performed in Fresno County, California. The Contractor consents to California jurisdiction for actions arising from or related to this Agreement, and, subject to the Government Claims Act, all such actions must be brought and maintained in Fresno County.

13.5 **Construction.** The final form of this Agreement is the result of the parties' combined efforts. If anything in this Agreement is found by a court of competent jurisdiction to be ambiguous, that ambiguity shall not be resolved by construing the terms of this Agreement against either party.

13.6 **Days.** Unless otherwise specified, "days" means calendar days.

13.7 **Headings.** The headings and section titles in this Agreement are for convenience only and are not part of this Agreement.

13.8 **Severability.** If anything in this Agreement is found by a court of competent jurisdiction to be unlawful or otherwise unenforceable, the balance of this Agreement remains in effect, and the parties shall make best efforts to replace the unlawful or unenforceable part of this Agreement with lawful and enforceable terms intended to accomplish the parties' original intent.

13.9 **Nondiscrimination.** During the performance of this Agreement, the Contractor shall not unlawfully discriminate against any employee or applicant for employment, or recipient of services, because of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, military status or veteran status pursuant to all applicable State of California and federal statutes and regulation.

1 13.10 **No Waiver.** Payment, waiver, or discharge by either Party of any liability or obligation
2 of the other Party under this Agreement on any one or more occasions is not a waiver of
3 performance of any continuing or other obligation of the other Party and does not prohibit
4 enforcement by the affected Party of any obligation on any other occasion.

5 13.11 **Entire Agreement.** Both Parties agree that OMNIA's UC Agreement No.
6 2023003491, this Service Agreement from the County and Contractor's Terms and Conditions
7 found in proposal, along with their exhibits, constitute the entire agreement between the
8 Contractor and the County with respect to the subject matter of this Agreement, and it
9 supersedes all previous negotiations, proposals, commitments, writings, advertisements,
10 publications, and understandings of any nature unless those things are expressly included in
11 this Agreement. If there is any inconsistency or conflict between the terms of the documents
12 listed in this section , then the inconsistency or conflict will be resolved by giving the following
13 precedence order: (1) the text of this Agreement, excluding Exhibits A through I; (2) the text of
14 OMNIA Agreement #2023003491, located at [https://www.omniapartners.com/suppliers/johnson-](https://www.omniapartners.com/suppliers/johnson-controls/public-sector/contract-documents#contract-379)
15 [controls/public-sector/contract-documents#contract-379](https://www.omniapartners.com/suppliers/johnson-controls/public-sector/contract-documents#contract-379); (3) Contractor's Terms and Conditions
16 found in proposal and (4) Exhibits A through I.

17 13.12 **No Third-Party Beneficiaries.** This Agreement does not and is not intended to
18 create any rights or obligations for any person or entity except for the parties.

19 13.13 **Agent for Service of Process.** The Contractor represents to County that the
20 Contractor's agent for service of process in California, and that such agent's address for
21 receiving such service of process in California, which information the Contractor shall maintain
22 with the office of the California Secretary of State, is as follows:

23 **1505 Corporation**

24 C T Corporation System

25 330 N. Brand Blvd.

26 Glendale, CA 91203

27 The Contractor further represents to the County that if the Contractor changes its agent for
28 service of process in California, or the Contractor's agent for service of process in California

1 changes its address for receiving such service of process in California, which changed
2 information the Contractor shall maintain with the office of the California Secretary of State, the
3 Contractor shall give the County written notice thereof within five calendar days thereof pursuant
4 to Article 5 of this Agreement.

5 **13.14 Authorized Signature.** The Contractor represents and warrants to the County that:

6 (A) The Contractor is duly authorized and empowered to sign and perform its
7 obligations under this Agreement.

8 (B) The individual signing this Agreement on behalf of the Contractor is duly
9 authorized to do so and his or her signature on this Agreement legally binds the
10 Contractor to the terms of this Agreement.

11 **13.15 Electronic Signatures.** The parties agree that this Agreement may be executed by
12 electronic signature as provided in this section.

13 (A) An "electronic signature" means any symbol or process intended by an individual
14 signing this Agreement to represent their signature, including but not limited to (1) a
15 digital signature; (2) a faxed version of an original handwritten signature; or (3) an
16 electronically scanned and transmitted (for example by PDF document) version of an
17 original handwritten signature.

18 (B) Each electronic signature affixed or attached to this Agreement (1) is deemed
19 equivalent to a valid original handwritten signature of the person signing this Agreement
20 for all purposes, including but not limited to evidentiary proof in any administrative or
21 judicial proceeding, and (2) has the same force and effect as the valid original
22 handwritten signature of that person.

23 (C) The provisions of this section satisfy the requirements of Civil Code section
24 1633.5, subdivision (b), in the Uniform Electronic Transaction Act (Civil Code, Division 3,
25 Part 2, Title 2.5, beginning with section 1633.1).

26 (D) Each party using a digital signature represents that it has undertaken and
27 satisfied the requirements of Government Code section 16.5, subdivision (a),
28

1 paragraphs (1) through (5), and agrees that each other party may rely upon that
2 representation.

3 (E) This Agreement is not conditioned upon the parties conducting the transactions
4 under it by electronic means and either party may sign this Agreement with an original
5 handwritten signature.

6 13.16 **Counterparts.** This Agreement may be signed in counterparts, each of which is an
7 original, and all of which together constitute this Agreement.

8 [SIGNATURE PAGE FOLLOWS]

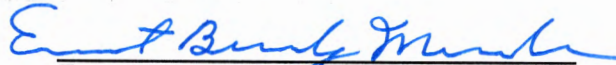
1 The parties are signing this Agreement on the date stated in the introductory clause.

2 JOHNSON CONTROLS, INC.

COUNTY OF FRESNO

3 Eric Franklin

Digitally signed by Eric Franklin
DN: cn=Eric Franklin c=US o=JCI BSNA
ou=JCI-Seattle e=eric.franklin@jci.com
Reason: I have reviewed this document
Location:
Date: 2025-02-25 16:23-08:00




4 Eric Franklin, Market General Manager

Ernest Buddy Mendes, Chairman of the
Board of Supervisors of the County of Fresno

5 3451 W. Ashlan Ave.
6 Fresno, CA 93722

7 **Attest:**
Bernice E. Seidel
8 Clerk of the Board of Supervisors
County of Fresno, State of California

9
10 By: 
Deputy

11 For accounting use only:

12 Org No.: 8935
13 Account No.: 7205
Fund No.: 1045
14 Subclass No.: 10000

Exhibit A

Scope of Services

A. DEFINITIONS

The following terms used throughout this Agreement shall be defined as follows:

- a. **"Acceptance Criteria"** means the performance and operating specifications which the System must meet at a minimum, as set out or referred to in this Agreement.
- b. **"Acceptance Test"** means the process of testing a specific function or functions to determine if the operation or operations are as stated in this Agreement.
- c. **"Basic Coverage"** means Scheduled Service Visits, plus Scheduled Service Materials. No parts, equipment, Repair Labor or Repair Materials are provided under Basic Coverage.
- d. **"Change Control Process"** means the process used by the Information Technology Division of the County's Internal Services Department (ISD) to inform staff of new or updated production use systems.
- e. **"County System Hardware"** means the central processing units owned or leased by the County, which are described in this Agreement, on which the County is licensed to use the System Software, any back-up equipment for such central processing units, and any peripheral hardware such as terminals, printers, and Personal Computers as described in this Agreement.
- f. **"County System Software"** means the operating system and database software installed on the County System Hardware.
- g. **"Covered Equipment"** means the equipment for which services are to be provided under this Agreement.
- h. **"Digital Enabled Services"** means services provided that employ the Contractor's software and/or related equipment installed by the County, and the Contractor's cloud-hosted software offerings and tools used to improve, develop, and enable such services. Digital Enabled Services include, but are not limited to:
 - i. Remote servicing and inspection
 - ii. Advanced equipment fault detection and diagnostics
 - iii. Data dashboard and health reporting
- i. **"Equipment Failure"** means the failure, under normal and expected working conditions, of moving, electric, or electronic components of Covered Equipment that are necessary for its operations.
- j. **"Final System Acceptance"** means when it is determined by the County that all necessary deliverables have been delivered, the data has been converted, the base Metasys and ADS software has been successfully installed and tested, and the Metasys and ADS performs all functions in accordance with its specifications.
- k. **"First Production Use"** means the date of first use of the system in a production environment.
- l. **"Hazardous Materials"** means any material or substance that, whether by its nature or use, is now or hereafter defined or regulated as a hazardous waste, hazardous substance, pollutant, or contaminant under any local, state, or federal law, regulation, or ordinance relating to or addressing public and employee health and safety and protection of the environment, or which is toxic, explosive, corrosive, flammable, radioactive, carcinogenic or otherwise hazardous or which is or contains petroleum, gasoline, diesel, fuel, another petroleum hydrocarbon product or polychlorinated biphenyls. "Hazardous Materials" specifically includes mold, lead-based paints, biohazards such as but not limited to Legionella and asbestos-containing materials ("ACM").

Exhibit A

- m. **"License"** means the rights and obligations that it creates under the laws of the United States of America and the State of California, including without limitation, copyright and intellectual property law.
- n. **"Monies", "Charges", "Price", and "Fees"** will be considered to be equivalent.
- o. **"Public Records"** includes any writing containing information relating to the conduct of the public's business that is prepared, owned, used, or retained by any state or local agency, regardless of physical form or characteristics.
- p. **"Remote Monitoring Services"** means remote monitoring of Covered Equipment and/or systems including building automation and HVAC equipment using a UL Certified Central Station.
- q. **"Remote Operations Center"** (ROC) is the Contractor's department that remotely monitors alarms and industrial, or HVAC, process signals.
- r. **"Repair Labor"** means the labor necessary to restore Covered Equipment to working condition following an Equipment Failure but does not include services relating to total equipment replacement due to obsolescence or unavailability of parts.
- s. **"Repair Materials"** means the parts and materials necessary to restore Covered Equipment to working condition following an Equipment Failure but excludes total equipment replacement due to obsolescence or unavailability of parts, unless excluded from the Agreement.
- t. **"Scheduled Service Materials"** means the materials required to perform Scheduled Service Visits on Covered Equipment, unless excluded from the Agreement.
- u. **"Scheduled Service Visits"** means the on-site labor visits required to perform Contractor recommended inspections and preventative maintenance on Covered Equipment.
- v. **"Services"** mean the work, materials, labor, service visits, and repairs to be provided by the Contractor pursuant to this Agreement except that the Services do not include the Connected Equipment Services or the provision of other software products or digital or cloud services.
- w. **"Supplier", "Vendor", and "Johnson Controls International, Inc."** all refer to the Contractor, and are considered to be equivalent throughout this Agreement.
- x. **"System"** means the System Software and System Documentation, collectively. Reference to the "System" shall include any component thereof. All modifications and enhancements to the System shall be deemed to be part of the System as defined herein and shall be subject to all terms and conditions set forth herein. The System consists of Metasys and ADS, which supports ISD – Facility Services, all interfaces, and third-party software required for the system to function.
- y. **"System Documentation"** means the documentation relating to the System Software, and all manuals, reports, brochures, sample runs, specifications and other materials comprising such documentation provided by the Contractor in connection with the System Software pursuant to this Agreement.
- z. **"System Operation"** means the general operation of the County's hardware and all software including, but not limited to, system restarts, configuration and operation of system peripherals (such as printers, modems, and terminals), installation of new software releases, and other related activities.
- aa. **"System Installation"** means all software has been delivered, has been physically loaded on a computer, and the County has successfully executed program sessions.

Exhibit A

- bb. **"System Software"** means Metasys and ADS, that certain computer software described in this Agreement provided by the Contractor, and all interfaces, coding, tapes, disks, modules and similar materials comprising such software or on which it is stored. System Software shall not include operating system software, or any other Third-Party Software.
- cc. **"User", "Customer" and "Licensee"** all refer to the County and are considered to be equivalent throughout this Agreement.

B. SOFTWARE LICENSE

I. EULA

County shall use any intellectual property embedded or embodied in products solely for the purposes of installing, commissioning, operating, repairing, and servicing instances of the products received from the Contractor. Nothing in this Agreement supersedes any terms of service or end-user-license agreements which may accompany software (including software provided as a service). The County is responsible for reviewing and agreeing to such terms separately. Continued use of or access to software provided as a service may be subject to payment of recurring fees (such as subscription fees). The County shall be responsible for these payments, subject to their budgeting and financial approval process.

II. OWNERSHIP

The parties acknowledge and agree that, as between the Contractor and the County, title and full ownership of all rights in and to the System Software, System Documentation, and all other materials provided to the County by the Contractor under the terms of this Agreement shall remain with the Contractor. The County will take reasonable steps to protect trade secrets of the System Software and System Documentation. Ownership of all copies is retained by the Contractor. The County may not disclose or make available to third parties the System Software or System Documentation or any portion thereof. The Contractor shall own all right, title and interest in and to all corrections, modifications, enhancements, programs, and work product conceived, created or developed, alone or with the County or others, as a result of or related to the performance of this Agreement, including all proprietary rights therein and based thereon. Except and to the extent expressly provided herein, the Contractor does not grant to the County any right or license, express or implied, in or to the System Software and System Documentation or any of the foregoing. The parties acknowledge and agree that, as between the Contractor and the County, full ownership of all rights in and to all County data given to Contractor, whether in magnetic or paper form, are the exclusive property of the County.

III. TRANSFER OF SOFTWARE

The County shall not rent, lease, license, distribute, sell, transfer, or assign this License, the System Software, or the System Documentation, or any of the information contained therein other than County data, to any other person or entity, whether on a permanent or temporary basis, and any attempt to do so will constitute a breach of this Agreement. No right or license is granted under this Agreement for the use or other utilization of the licensed programs, directly or indirectly, for the benefit of any other person or entity, except as provided in this Agreement.

IV. POSSESSION AND USE OF SOURCE CODE

Source code and other material that results from custom programming by the Contractor released to the County under this License shall be deemed the Contractor's software, subject to all of the terms and conditions of the software License set forth in this Agreement. The scope of the County's permitted use of the custom source code under this License shall be limited to maintenance and support of the System Software. For purposes of this section, the term "maintenance and support" means correction of System Software errors and preparation of System Software modifications and enhancements. If the County creates derivative work from the System Software, the copyright to such derivative work shall be owned by the Contractor,

Exhibit A

and the County's rights to use such derivative work shall be limited to those granted with respect to the System Software in this Agreement.

V. RESTRICTIONS ON USE

The County shall not (i) license, sublicense, sell, resell, transfer, assign, distribute or otherwise commercially exploit or make available to any third party the System Software or the System Documentation in any way; (ii) modify or make derivative works based upon the System Software or the System Documentation; (iii) create Internet "links" to the System Software or "frame" or "mirror" any System Documentation on any other server or wireless or Internet-based device; (iv) send spam or otherwise duplicative or unsolicited messages in violation of applicable law; (v) send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material harmful to children or violative of third party privacy rights; (iv) send or store material containing software viruses, worms, Trojan horses or other harmful computer code, files, scripts, agents or programs; (vii) interfere with or disrupt the integrity or performance of the System Software or the data contained therein, including but not limited to County Data; (viii) attempt to gain unauthorized access to the System Software or its related systems or networks; (ix) reverse engineer or access the System Software in order to (a) build a competitive product or service, (b) build a product using similar ideas, features, functions or graphics of the System Software, or (c) copy any ideas, features, functions or graphics of the System Software.

VI. INTELLECTUAL PROPERTY, TRADEMARK, AND COPYRIGHT

The Contractor retains ownership of the System Software, any portions or copies thereof, and all rights therein. The Contractor reserves all rights not expressly granted to the County. This License does not grant the County any rights in connection with any trademarks or service marks of the Contractor, its suppliers or licensors. All right, title, interest and copyrights in and to the System Software and the accompanying System Software Documentation and any copies of the System Software are owned by the Contractor, its suppliers or licensors. All title and intellectual property rights in and to the content which may be accessed through use of the System Software are the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This License grants the County no rights to use such content.

C. SERVICES TO BE PROVIDED BY CONTRACTOR TO COUNTY

I. SERVICES

The Contractor will provide Basic Coverage for the County's facilities. The Contractor will provide preventative maintenance services at County facilities. The Contractor will check for operational deficiencies, perform scheduled block hour tasks, complete required maintenance checklists, and provide County with observations. Preventative maintenance includes, but is not limited to:

- i. validating the configuration and functionality of alarms, trend logs, and automatic reports
- ii. assessing equipment functionality and compiling a status report on operational conditions
- iii. identifying deficiencies, document issues, and formulating of a remediation plan
- iv. performing server backups
- v. confirming software and engines are upgraded to latest revisions.

II. DOCUMENTATION

The Contractor shall provide to the County Metasys and ADS System Documentation, which shall consist of electronic media files. The electronic media files must be printable using PC software normally available at the County. The Contractor shall provide new System Documentation corresponding to all new Software Upgrades. The County may print additional

Exhibit A

copies of all documentation. All System Documentation is to be used by the County only for the purposes identified within this Agreement.

III. OUT OF SCOPE SERVICES

If, during any Service Visit, the Contractor detects a defect in any of the County's equipment that is not Covered Equipment under this Agreement (an "Out of Scope Defect"), the Contractor may (but shall have no obligation to) notify the County of such Out of Scope Defect. If the County elects for the Contractor to repair such Out of Scope Defect, or if the Contractor otherwise performs any Services or provides any materials, parts, or equipment outside the scope of the Services (collectively, "Out of Scope Services"), the County shall direct the Contractor to perform such Out of Scope Services in writing, and the County shall pay for such Out of Scope Services at the rates defined in Exhibit B of this Agreement.

D. SYSTEM MAINTENANCE AND SUPPORT BY CONTRACTOR

System maintenance and support includes System Updates as they are released by the Contractor, including updates as required as a result of Federal Regulatory Changes. The first day of production use will be identified by the County and communicated to the Contractor. The Contractor will support day-to-day operation of the System as follows:

I. SUPPORT HOURS/SCOPE:

Provide unlimited technical assistance by phone during normal coverage hours (7:30 a.m. to 4:30 p.m. Pacific Standard Time (PST), Monday through Friday, except County holidays), toll-free telephone assistance to keep the System in, or restored to, normal operating condition. The object of this support will be to answer specific questions related to the System Software and the application thereof. If the Contractor's technical phone assistance does not solve the County's issue within 30 minutes, the Contractor may, upon the County's approval, provide on-site support, which shall be billable at the Contractor's rates as listed in Exhibit B of this Agreement. Support provided under this Agreement does not include training of new personnel (after initial staff is trained), operation of hardware, or solving other hardware/software problems unrelated to the System Software.

II. SUPPORT RESPONSE:

During the term of this Agreement, the Contractor shall (a) correct any error or malfunctions in the System that prevent the System from operating in conformance with the specifications set forth in this Agreement, or (b) provide a commercially reasonable alternative that will conform to the specifications set forth in this Agreement.

If analysis by the Contractor indicates a reported problem is caused by a reproducible error or malfunction in the then-current release of the System Software as supplied and maintained by the Contractor, that significantly impacts effective use of the System by the County, the Contractor shall, if the System is inoperable, as reported by the County, provide continuous effort to correct the error or to resolve the problem by providing a circumvention.

In such cases, the Contractor will provide the County with corrective information, such as corrective documentation and/or program code. The Contractor will endeavor to respond to the County's service request no later than four business hours from the time a call has been received by the Contractor. In the event that a person with the necessary expertise is not available when the call is received, the Contractor will endeavor to respond to the service request no later than within one business day.

III. REMOTE VIRTUAL PRIVATE NETWORK (VPN) DIAGNOSTICS

Remote VPN Diagnostics Support includes:

- a. Diagnostic or corrective actions necessary to restore proper Metasys and ADS operation;
- b. Diagnostic actions which attempt to identify the cause of system problem;
- c. Correction of data file problem; and
- d. Product modifications

Exhibit A

The Contractor product specialists will provide diagnostics via VPN on Metasys and ADS. The County will provide any required hardware and equipment necessary at the County for the Contractor's VPN support.

IV. ERROR CORRECTION PROCESS

If during the term of this Agreement the County determines that software error(s) exist, the County will first follow the error procedures specified in the System Documentation. If following the error procedures does not correct the software error, the County shall immediately notify the Contractor, setting forth the defects noted with specificity. Upon notification of a reported software error, the Contractor shall have five days to determine if any actual software error exists and, if so, endeavor to correct such software errors. At the Contractor's request, additional time to solve difficult problems will not be unreasonably withheld. Within 15 days of correction, the County shall retest the System Software, and report any other software errors.

V. WARRANTIES

The Contractor warrants its Services will be provided in a good and workmanlike manner for 90 days from the date of Services. If the Contractor receives written notice of a breach of this warranty prior to the end of this warranty period, the Contractor will re-perform any non-conforming Services at no additional charge within a commercially reasonable time of the notification.

If the Contractor installs or furnishes a piece of equipment under this Agreement, the Contractor warrants that equipment labeled the Contractor shall be free from defects in material and workmanship arising from normal usage for a period of 90 days. No warranty is provided for third-party products and equipment installed or furnished by the Contractor. Such products and equipment are provided with the third-party manufacturer's warranty to the extent available, and the Contractor will transfer the benefits, together with all limitations, of that manufacturer's warranty to the County. All transportation charges incurred in connection with the warranty for equipment and/or materials not covered under this Agreement shall be borne by the County. Except as provided herein, if the Contractor receives written notice of a breach of this warranty prior to the end of this warranty period, the Contractor will repair or replace (at the Contractor's option) the defective equipment.

VI. EXCLUSIONS

The Contractor's Services and warranty obligations expressly exclude:

- i. the repair or replacement of ductwork, casings, cabinets, structural supports, tower fill/slats/basin, hydronic and pneumatic piping, and vessels, gaskets, and piping not normally replaced or maintained on a scheduled basis, and removal of oil from pneumatic piping;
- ii. disposal of hazardous wastes (except as otherwise expressly provided herein);
- iii. disinfecting of chiller condenser water systems and other components for biohazards, such as but not limited to, Legionella unless explicitly set forth in the scope of services between the parties. Unless explicitly provide for within the scope of services, this is Out of Scope Services and the County's exclusive responsibility to make arrangements for such services with a provider other than the Contractor. Mentions of chiller tube cleaning, condenser cleaning, cooling tower cleaning or boiler tube cleaning in any scope of services, only involve work to remove normal buildup of debris and scale using tube brush cleaning pressure washing or acid flushing. Reference to such cleaning does not include chemical cleaning, disinfection or chemical water treatment required to eliminate, control or disinfect against biohazards such as but not limited to Legionella;
- iv. refrigerant; supplies, accessories, or any items normally consumed during the use of Covered Equipment, such as ribbons, bulbs and paper;
- v. the furnishing of materials and supplies for painting or refinishing equipment;

Exhibit A

- vi. the repair or replacement of wire in conduit, buried cable/transmission lines, or the like, if not normally replaced or maintained on a scheduled basis;
- vii. replacement of obsolete parts; and
- viii. damages of any kind, including but not limited to personal injury, death, property damage, and the costs of repairs or service resulting from:
 - a. abuse, misuse, alterations, adjustments, attachments, combinations, modifications, or repairs to Covered Equipment not performed, provided, or approved in writing by the Contractor;
 - b. equipment not covered by this Agreement or attachments made to Covered Equipment;
 - c. acts or omissions of the County, including but not limited to the failure of the County to fulfill the County Obligations and Commitments to the Contractor as described in this Agreement, operator error, the County's failure to conduct preventive maintenance, issues resulting from the County's previous denial of the Contractor access to the Covered Equipment, and the County's failure to keep the site clean and free of dust, sand, or other particles or debris, unless such conditions are previously expressly acknowledged by the Contractor in writing;
 - d. use of the Covered Equipment in a manner or environment, or for any purpose, for which it was not designed by the manufacturer;
 - e. site-related and environmental conditions, including but not limited to power failures and fluctuations in electrical current (or "power surges") and biohazards such as but not limited to Legionella associated with condenser water, cooling tower systems and subcomponent systems;
 - f. the effects of erosion, corrosion, acid cleaning, or damage from unexpected or especially severe freezing weather;
 - g. issues or failures not specifically covered by this Agreement; or
 - h. occurrences beyond the Contractor's reasonable control and without the Contractor's fault or negligence.

THESE WARRANTIES ARE CONTRACTOR'S SOLE WARRANTIES AND TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THOSE OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

VII. TECHNICAL INFORMATION

The Contractor will provide technical information to the County from time to time. Such information may cover areas such as Metasys and ADS usage, third-party software, and other matters considered relevant to the County by the Contractor. Technical information will be provided at the discretion of the Contractor but will not be unreasonably withheld.

E. ADDITIONAL SYSTEM MAINTENANCE SERVICES BY CONTRACTOR

The Contractor may provide additional maintenance services ("Additional Maintenance and Support Services" or "Additional Maintenance Services") at an additional charge. Charges will be as identified in Exhibit B of this Agreement; or, if not included in this Agreement, charges will be at current prices in effect at the time goods or services are provided. Any Additional Maintenance and Support Services requested by the County and determined by the Contractor to be billable by the Contractor must be identified as a chargeable service prior to the service being performed and must be approved in writing in advance by the County Representative. All charges pursuant to this Section will be subject to the maximum compensation amount in the Agreement at Section 3.2. Additional Maintenance Services include, but are not limited to, the following:

I. ADDITIONAL TRAINING

Exhibit A

The Contractor shall provide quarterly training to the County's ISD-Facility Services staff as follows:

- i. Eight hours of quarterly on-site training for ISD-Facility Services staff assigned to specific County locations, with trainings for each location rotated on a quarterly basis.

II. DATA AND SYSTEM CORRECTIONS

Data and System Corrections include any corrective actions accomplished by the Contractor on-site or via VPN which are necessary due to the County errors or unauthorized source code or data access by the County. Unauthorized access to the data is defined as any the County editing of data through other than normal system usage, as defined in System Documentation. Unauthorized access to source code is defined as any County access whatsoever to system source code. Services provided by the Contractor are not billable when they result from errors caused by Metasys and ADS or instruction provided by the Contractor.

III. CUSTOMER SITE VISITS

Site visits to County sites, as may be requested using the Contractor's automated service management system, by the County and that are within the scope of the project services, are available for reasons such as, but not limited to, (1) additional system training on hardware or software usage; (2) resolution of system difficulties not resulting from actions by, or otherwise the responsibility of the Contractor (as determined by mutual agreement between the Contractor and the County); (3) installation of Software Releases; and (4) assistance in equipment maintenance, movement or diagnosis. Site visits outside of the scope of project services will be reviewed by the Contractor and must be requested in writing in advance by the County Representative. Charges will be at rates identified in this Agreement.

IV. EMERGENCY SERVICES

Emergency services can be provided seven days a week, 24 hours a day, 365 days a year. During normal business hours, emergency services will be coordinated by the Contractor's customer service agent. After hours, weekends, and holidays, the emergency service number transfers to the Contractor's after-hours call center and on-call technicians are dispatched as needed. Technicians are dispatched within hours of receiving request for emergency services.

V. CUSTOM PROGRAMMING

Requests for supplemental programming or customization of system features not covered under this Agreement are available to the County. Such requests will be reviewed by the Contractor and must be requested in writing in advance by the County Representative. Charges will be at rates identified in this Agreement.

F. CONTRACTOR PROJECT COORDINATOR

Upon execution of this Agreement, the Contractor shall appoint a Project Coordinator who will act as the primary contact person to interface with the County for implementation, maintenance and support of Metasys and ADS. All immediate service needs will funnel through the Contractor's 24 hour support line and the Contractor will direct calls to the technician who will be able to respond within the County's requested timeframe.

G. SYSTEM UPDATES AND NEW PRODUCTS

I. SYSTEM UPDATES

- a. POSSESSION, USE, AND UPDATE OF SOFTWARE

Exhibit A

The County agrees that the County will only use the System Software for its own internal purposes. The Contractor may, at reasonable times, inspect the County's premises and equipment to verify that all of the terms and conditions of this license are being observed. The Contractor may create, from time to time, updated versions of the System Software and System Documentation and the Contractor shall make such System Updates available to the County. All System Updates shall be licensed under the terms of this Agreement. The County agrees to follow the prescribed instructions for updating System Software and System Documentation provided to the County by the Contractor, included but not limited to the following:

The Contractor shall perform all System Updates after receiving the County's written approval. The Contractor shall provide a list of upgradeable hardware upon execution of this Agreement. The Contractor will provide most recent System Update allowed by the hardware and operating systems of the County's existing computers and servers for duration of this Agreement. System Updates shall include major software revisions (e.g. 10.0 to 11.0), not minor software revisions (e.g. 10.0 to 10.1).

If any hardware is updated during the term of this Agreement, the new hardware shall be installed with the County's current revision of software; however, it will not be included under the annual software upgrades listed in this Agreement.

The County must authorize all System Updates in writing.

b. From time to time, the Contractor will develop and provide System Updates to the County for the County's licensed Contractor software. System Updates shall be subject to the terms and conditions of this Agreement and shall be deemed licensed System Software hereunder and will be made available to the County at no additional charge to the County. System Updates will be made available to the County at the discretion of the Contractor but will not be unreasonably withheld.

II. NEW PRODUCTS

The Contractor may from time to time release new software with capabilities substantially different from or greater than the System Software ("New Products") and which therefore do not constitute System Updates. These New Products will be made available to the County at a cost not to exceed the Contractor's then standard rates for customers similarly situated.

H. OPERATING SYSTEM UPDATES

The application must run on an operating system (O/S) that is consistently and currently supported by the operating system vendor. Applications under maintenance are expected to always be within one year of current in regard to the O/S. Outdated or unsupported O/S will not be implemented on the production network.

The County will notify the Contractor when a critical security patch is released. The Contractor will have 30 days to ensure application can perform in the updated environment. With approval from the Contractor, the County will apply patches to both the operating system, and non-critical security subsystems as releases are available from operating system vendors. The application is expected to perform in this environment. The Contractor is expected to keep their software within one year of current in order to operate in this environment. These patches include critical O/S updates and security patches.

I. COUNTY OBLIGATIONS

The County agrees and warrants that, during the term of this Agreement, the County will:

Exhibit A

- a. operate the Covered Equipment according to manufacturer and/or the Contractor's recommendations;
- b. keep accurate and current work logs and information about the Covered Equipment as recommended by manufacturer and/or the Contractor;
- c. provide an adequate environment for Covered Equipment as recommended by manufacturer and/or the Contractor, including, but not limited to adequate space, electrical power, water supply, air conditioning, and humidity control;
- d. notify the Contractor immediately of any Covered Equipment malfunction, breakdown, or other condition affecting the operation of the Covered Equipment;
- e. provide the Contractor with safe access to its Premises and Covered Equipment at all reasonable and necessary times for the performance of the Services;
- f. allow the Contractor to start and stop, periodically turn off, or otherwise change or temporarily suspend equipment operations so that the Contractor can perform the Services required under this Agreement;
- g. as applicable, provide proper condenser, cooling tower and boiler water treatment for the proper functioning of Covered Equipment and protect against any environmental issues and instances of biohazards such as but not limited to Legionella;
- h. carefully and properly set and test the intrusion alarm system each night or at such other time as the County shall close the Premises;
- i. obtain all necessary licenses and permits required for and pay all taxes associated with the Services;
- j. properly maintain, repair, service, and assure the proper operation of any other property, system, equipment, or device of the County or others to which the Covered Equipment may be attached or connected, in accordance with manufacturer recommendations, insurance carrier requirements, or the requirements of any fire rating bureau, agency, or other authorities having jurisdiction thereof;
- k. not tamper with, alter, adjust, disturb, injure, remove, or otherwise interfere with any Covered Equipment (including any related software) and not permit the same to be done;
- l. refrain from causing false alarms, and reimburse the Contractor for any fine, penalty, or fee paid by or assessed against the Contractor by any governmental or municipal agency as a result thereof;
- m. be solely responsible for the establishment, operation, maintenance, access, security and other aspects of its computer network ("Network") and shall supply the Contractor with secure Network access for providing its services. Products networked, connected to the internet, or otherwise connected to computers or other devices must be appropriately protected by the County and/or end user against unauthorized access; and
- n. take appropriate measures, including performing back-ups, to protect information, including without limit data, software, or files (collectively "Data") prior to receiving the service or products.

The County acknowledges and understands that unless water treatment for biohazards (such as Legionella) is explicitly included in the services the Contractor is providing, it is the County's responsibility to provide such treatment. The County also acknowledges that its failure to meet the above obligations will relieve the Contractor of any responsibility for any Covered Equipment breakdown, or any necessary repair or replacement of any Covered Equipment. If

Exhibit A

the County breaches any of these obligations, the Contractor shall have the right, upon written notice to the County, to suspend its Services until the County cures such breach. In addition, the County shall be responsible for paying or reimbursing the Contractor for any costs associated with corrective work required as a result of the County's breach of these obligations.

J. ANTI-VIRUS MANAGEMENT

The County will actively run anti-virus management, where appropriate, on all application servers and PCs. The application is expected to perform adequately while anti-virus management is active.

K. ADHERE TO CHANGE CONTROL PROCESS

The Contractor must adhere to the County's Change Control Process, which shall be provided to the Contractor in writing. The County employs a procedure to implement updates, upgrades, and version releases to a system that is in production use. This forum allows ISD to inform staff (Help Desk, Network, Server, Database, Security, and Analysts) of upcoming changes to a production system. The Contractor must inform ISD a minimum of one week prior to any planned, non-emergency changes so that the Change Control Process may be followed.

L. HAZARDOUS MATERIALS

The Contractor will be responsible for removing or disposing of any Hazardous Materials that it uses in providing the Services (Contractor Hazardous Materials) and for the remediation of any areas affected by the release of Contractor Hazardous Materials. For other Hazardous Materials that may be present at its facilities (Non-Contractor Hazardous Materials), the County shall supply the Contractor with any information in its possession relating to the presence of Hazardous Materials if their presence may affect the Contractor's performance of the Services. If either the County or the Contractor becomes aware of or suspects the presence of Non-Contractor Hazardous Materials that may interfere with the Contractor's Services, it shall immediately stop the Services in the affected area and notify the other party. As between the County and the Contractor, the County shall be responsible at its sole expense for removing and disposing of Non-Contractor Hazardous Materials from its facilities and for the remediation of any areas impacted by the release of the Non-Contractor Hazardous Materials and must provide a certificate of abatement before the Contractor will be obligated to perform or continue its Services, unless the Contractor had actual knowledge that Non-Contractor Hazardous Materials were present and acted in disregard of that knowledge, in which case (i) the Contractor shall be responsible at its sole expense for the remediation of any areas impacted by its release of such Hazardous Materials, and (ii) the County shall remain responsible at its sole expense for the removal of Hazardous Materials that have not been released and for releases not resulting from the Contractor's performance of the Services.

M. OTHER

Unless otherwise specified, for third-party software, the Contractor shall provide standard documentation in electronic form (via the Internet or File Transfer Protocol (FTP)).

Refrigerant is not included under this Agreement and will be billed separately to the County by the Contractor.

The system being provided runs in a Local Area Network and Web environment. As such, the performance of the system is directly related to, among other things: available network bandwidth, and the performance of other applications. For this reason, the Contractor makes no guarantees as to system response time.

Exhibit B

Compensation

The Contractor will be compensated for performance of its services under this Agreement (subject to the maximum compensation amount per Section 3.2) as provided in this Exhibit B. The Contractor is not entitled to any compensation except as expressly provided in this Exhibit B.

Year	Scheduled Labor Hours	Scheduled Labor Subtotal	Training Hours	Training Subtotal	Software Total	Mileage & Travel Subtotal	Annual Known-Cost Sub-Totals	Additional Maintenance Service Term Subtotals*
1	16 hrs/wk	\$224,192.44	8 hrs/qtr	\$9,093.12	\$7,940.00	\$697.44	\$241,923.00	\$824,905.00
2	20 hrs/wk	\$288,897.77	8 hrs/qtr	\$9,365.91	\$8,178.20	\$698.33	\$307,140.00	
3	24 hrs/wk	\$357,260.64	8 hrs/qtr	\$9,646.89	\$8,423.54	\$700.93	\$376,032.00	
4	28 hrs/wk	\$429,466.98	8 hrs/qtr	\$9,936.30	\$8,676.25	\$701.47	\$448,781.00	\$301,219.00
5	32 hrs/wk	\$505,682.36	8 hrs/qtr	\$10,234.10	\$8,936.54	\$703.00	\$525,556.00	\$224,444.00
Initial Term Maximum Compensation								\$1,750,000.00
Optional Year 4 Maximum Compensation								\$2,500,000.00
Optional Year 5 Maximum Compensation								\$3,250,000.00

* An average of \$275,000 is available, annually, for Additional Maintenance Services.

Exhibit C

Self-Dealing Transaction Disclosure Form

In order to conduct business with the County of Fresno ("County"), members of a contractor's board of directors ("County Contractor"), must disclose any self-dealing transactions that they are a party to while providing goods, performing services, or both for the County. A self-dealing transaction is defined below:

"A self-dealing transaction means a transaction to which the corporation is a party and in which one or more of its directors has a material financial interest."

The definition above will be used for purposes of completing this disclosure form.

Instructions

- (1) Enter board member's name, job title (if applicable), and date this disclosure is being made.
- (2) Enter the board member's company/agency name and address.
- (3) Describe in detail the nature of the self-dealing transaction that is being disclosed to the County. At a minimum, include a description of the following:
 - a. The name of the agency/company with which the corporation has the transaction; and
 - b. The nature of the material financial interest in the Corporation's transaction that the board member has.
- (4) Describe in detail why the self-dealing transaction is appropriate based on applicable provisions of the Corporations Code.

The form must be signed by the board member that is involved in the self-dealing transaction described in Sections (3) and (4).

Exhibit C

(1) Company Board Member Information:			
Name:		Date:	
Job Title:			
(2) Company/Agency Name and Address:			
(3) Disclosure (Please describe the nature of the self-dealing transaction you are a party to)			
(4) Explain why this self-dealing transaction is consistent with the requirements of Corporations Code § 5233 (a)			
(5) Authorized Signature			
Signature:		Date:	

Exhibit D

Insurance Requirements

1. Required Policies

Contractor, at its sole expense, shall maintain in full force and effect the following insurance policies throughout the term of this Agreement.

- (A) **Commercial General Liability.** Commercial general liability insurance with limits of One Million Dollars (\$1,000,000) per occurrence and an annual aggregate of Two Million Dollars (\$2,000,000). This policy must be issued on a per occurrence basis. Coverage must include products, completed operations, property damage, bodily injury, personal injury, and advertising injury. The Contractor shall obtain an endorsement to this policy naming the County of Fresno, its officers, agents, employees, and volunteers, individually and collectively, as additional insureds, but only insofar as the operations under this Agreement are concerned. Such coverage for additional insureds will apply as primary insurance and any other insurance, or self-insurance, maintained by the County is excess only and not contributing with insurance provided under the Contractor's policy.
- (B) **Automobile Liability.** Automobile liability insurance with limits of One Million Dollars (\$1,000,000) combined single limit for bodily injury and for property damages. Coverage must include any auto used in connection with this Agreement.
- (C) **Workers Compensation.** Workers compensation insurance as required by the laws of the State of California with statutory limits.
- (D) **Employer's Liability.** Employer's liability insurance with limits of One Million Dollars (\$1,000,000) per occurrence for bodily injury and for disease.
- (E) **Professional Liability.** Professional liability insurance with limits of Million Dollars (\$1,000,000) per occurrence and an annual aggregate of Two Million Dollars (\$2,000,000). If this is a claims-made policy, then (1) the retroactive date must be prior to the date on which services began under this Agreement; (2) the Contractor shall maintain the policy and provide to the County annual evidence of insurance for three years after completion of services under this Agreement; and (3) if the policy is canceled or not renewed, and not replaced with another claims-made policy with a retroactive date prior to the date on which services begin under this Agreement, then the Contractor shall purchase extended reporting coverage on its claims-made policy for three years after completion of services under this Agreement.
- (F) **Molestation Liability.** Sexual abuse / molestation liability insurance with limits of One Million Dollars (\$1,000,000) per occurrence, with an annual aggregate of Two Million Dollars (\$2,000,000). This policy must be issued on a per occurrence basis.
- (G) **Technology Professional Liability (Errors and Omissions).** Technology professional liability (errors and omissions) insurance with limits of not less than Two Million Dollars (\$2,000,000) per claim and in the aggregate. Coverage must encompass all of the Contractor's obligations under this Agreement, including but not limited to claims involving Cyber Risks.

Exhibit D

- (H) **Cyber Liability.** Cyber liability insurance with limits of Two Million Dollars (\$2,000,000) per claim and in the aggregate. Coverage must include claims involving Cyber Risks. The cyber liability policy must be endorsed to cover the full replacement value of damage to, alteration of, loss of, or destruction of intangible property (including but not limited to information or data) that is in the care or custody of the Contractor.

2. Additional Requirements

- (A) **Verification of Coverage.** Within 30 days after the Contractor signs this Agreement, and at any time during the term of this Agreement as requested by the County's Risk Manager or the County Administrative Office, the Contractor shall deliver, or cause its broker or producer to deliver, to the County Risk Manager, at 2220 Tulare Street, 16th Floor, Fresno, California 93721, or HRRiskManagement@fresnocountyca.gov, and by mail or email to the person identified to receive notices under this Agreement, Accord certificates of insurance and endorsements required by contract for all of the coverages required under this Agreement.

- (i) Each insurance certificate must evidence that: (1) the insurance coverage has been obtained and is in full force; (2); and the Contractor has waived its right to recover from the County, its officers, agents, employees, and volunteers any amounts paid under any insurance policy required by this Agreement and that waiver does not invalidate the insurance policy.
- (ii) The commercial general liability insurance certificate must also state, and include an endorsement, that the County of Fresno, its officers, agents, employees, and volunteers, individually and collectively, are additional insureds insofar as the operations under this Agreement are concerned. The commercial general liability insurance certificate must also state that the coverage shall apply as primary insurance and any other insurance, or self-insurance, maintained by the County shall be excess only and not contributing with insurance provided under the Contractor's policy.
- (iii) The automobile liability insurance certificate must state that the policy covers any auto used in connection with this Agreement.

The professional liability insurance certificate, if it is a claims-made policy, must also state the retroactive date of the policy, which must be prior to the date on which services began under this Agreement.

- (B) **Acceptability of Insurers.** All insurance policies required under this Agreement must be issued by admitted insurers licensed to do business in the State of California and possessing at all times during the term of this Agreement an A.M. Best, Inc. rating of no less than A: VII.
- (C) **Notice of Cancellation or Change.** For each insurance policy required under this Agreement, the Contractor shall provide to the County, or ensure that the policy requires the insurer to provide to the County, electronic notice of any cancellation or change in material policy as required in this paragraph. For cancellation of the policy for

Exhibit D

nonpayment of premium, the Contractor shall, or shall cause the insurer to, provide electronic notice to the County not less than 30 days in advance of cancellation..

- (D) **County's Entitlement to Greater Coverage.** If the Contractor has or obtains insurance with broader coverage, higher limits, or both, than what is required under this Agreement, then the County requires and is entitled to the broader coverage, higher limits, or both.
- (E) **Waiver of Subrogation.** The Contractor waives any right to recover from the County, its officers, agents, employees, and volunteers any amounts paid under the policy of worker's compensation insurance required by this Agreement. The Contractor is solely responsible to obtain any policy endorsement that may be necessary to accomplish that waiver, but the Contractor's waiver of subrogation under this paragraph is effective whether or not the Contractor obtains such an endorsement.
- (F) **County's Remedy for Contractor's Failure to Maintain.** If the Contractor fails to keep in effect at all times any insurance coverage required under this Agreement, the County may, in addition to any other remedies it may have, suspend or terminate this Agreement upon Contractor's failure to remedy lack of insurance within 30 days of written notice from County, or purchase such insurance coverage, and charge the cost of that coverage to the Contractor. The County may offset such charges against any amounts owed by the County to the Contractor under this Agreement.
- (G) **Subcontractors.** The Contractor shall require and verify that all subcontractors used by the Contractor to provide services under this Agreement maintain insurance meeting all insurance requirements provided in this Agreement. This paragraph does not authorize the Contractor to provide services under this Agreement using subcontractors.

Exhibit E



Subject: Hostage Situations
Policy Number: 326.0
Page: 1 of 2
Date Originated: April 1, 2004
Date Revised: February 1, 2008
Authority: Title 15; Section 1327;
California Code of Regulations

It is imperative for the safety and security of all persons within Juvenile Justice Campus (JJC) facilities, as well as for those in the community, that minors are not allowed to leave the secure confines of the facilities by the taking of a hostage(s). If successful in securing a release through these means minors would be much more likely in the future to use this practice again in an attempt to escape the confines of the facilities. This would put those visiting and working at the JJC at higher level of risk and would jeopardize the safety of the community if the minor was in fact successful in securing his/her release.

The JJC is a "no-hostage" facility. This means that minors will not be released from custody under any circumstances due to the taking of a hostage(s). Any staff person taken hostage, no matter what their rank or status, immediately loses their authority and any orders issued by that person will not be followed.

I. HOSTAGE SITUATION PROCEDURES

- A. If any minor(s) and/or other person(s) in the facility attempt to hold any person hostage, and they do not respond to verbal commands to stop staff will immediately notify the Watch Commander. He/she will respond to the location and assess the situation. If a hostage situation is in progress the Watch Commander will:
 1. Summon assistance from other officers as required.
 2. Establish a secure perimeter around the hostage takers and allow no one to pass into it for any reason without authorization. Risks should not be taken that might allow the taking of additional hostages.
 3. Evacuate all non-essential persons at the scene to a safe location or any housing pod that is not directly involved in the incident.
 4. Direct officers to place minors in uninvolved housing pods in their rooms and have them remain there until directed otherwise. Minors outside of housing pods will remain in place under officer supervision until it is safe to return to their respective housing pods or any housing pod that is not directly involved in the incident.
 5. Immediately notify the Director or the Probation Services Manager/Assistant Director in his/her absence and confer with higher authority as to action to be taken. Administration in turn will notify the Chief.
- B. The Fresno Sheriff's Dispatch Center (488-3111) will be notified immediately and a request for a trained hostage negotiator and other emergency personnel will be made as needed. Prior to the arrival of the Sheriff Department's hostage negotiator the Watch Commander will attempt to ascertain:

Exhibit E

Subject: Hostage Situation Policy #:326.0

1. The number and identity of both the hostages and hostage takers;
 2. Any known weapons possessed by the hostage takers;
 3. The demands of the hostage takers.
- C. The Watch Commander will retain and direct departing custody officers, as well as, available Probation peace officer staff to assist with security and safety needs, as necessary. Additional Juvenile Correctional Officers should be called in as may be needed to insure the safe and secure operation of the facility.
- D. The Watch Commander will coordinate with the Sheriff's Department all activities taken to resolve the hostage situation, including the use of appropriate force, and will maintain control of the facility until relieved of that duty by the presence of a Probation Services Manager/Assistant Director, Director, or the Chief Probation Officer.
- E. Once the hostage situation has been resolved the minors involved should be housed in the most secure setting available and all appropriate charges should be filed.
- F. Each officer and/or non-sworn staff member who was involved or observed the incident will complete an incident report and if required, the appropriate critical incident evaluation report(s) regarding the details of the incident prior to the end of his/her shift. (See Incident Report, located in JAS Probation View, under "Word Templates".)
- G. The Watch Commander will prepare a Critical Incident Investigation Report, using the Critical Incident Evaluation Report - Page 2 report form and the critical incident evaluation report(s) completed by the reporting persons at the time of the incident.

II. PARENTAL AND MEDIA INFORMATION

- A. Attempts will be made at the direction of Administration to reach the families of the hostages to advise them of the situation. Notification will also be made to the parents of the hostage takers as deemed appropriate.
- B. All media inquiries will be referred to the Chief's office per departmental policy.

III. SECURITY AND OPERATIONAL REVIEW

Once the incident has been resolved a team will be established to conduct a security and operational review of the incident. The review will be conducted within 2 days of the resolution of the incident. The review team will be comprised of the facility administrator and/or facility Director, Probation Services Manager/Assistant Director and Supervising Juvenile Correctional Officers who are relevant to the incident. The team will review the circumstances leading up to the incident and any necessary corrective action necessary to ensure that such an incident does not repeat itself.

Fresno County Probation Department

Vendors, Volunteers and Student Interns

Vendors, Volunteers and Student Interns

308.1 PURPOSE AND SCOPE

This policy establishes guidelines for using Juvenile Justice Campus vendors, volunteers, and student interns, to supplement and assist Department personnel in their duties. Vendors and volunteers are members who can augment Department personnel and help complete various tasks.

308.1.1 DEFINITIONS

Definitions related to this policy include:

Student intern - A college, university, or graduate student gaining practical experience in a chosen field while performing services for the Department under supervision.

Vendor - An individual representing a company, outside agency, or non-profit organization, who is assigned to one of our facilities, performs a service for the Department, and may receive compensation for services rendered.

Volunteer - An individual who performs a service for the Department without promise, expectation, or receipt of compensation for services rendered. This may include unpaid chaplains and student interns.

308.2 POLICY

The Fresno County Probation Department shall ensure that vendors, volunteers and student interns are properly appointed, trained, and supervised to carry out specified tasks and duties in order to create an efficient Department and improve services to the community.

308.3 ELIGIBILITY

Requirements for participation as a vendor, volunteer or student intern for the Department may include but are not limited to:

- (a) Being at least 18 years of age.
- (b) Possession of liability insurance for any personally owned equipment, vehicles, or animals utilized during volunteer or student intern work.
- (c) No conviction of a felony, any crime of a sexual nature or against children, any crime related to assault or violence, any crime related to dishonesty, or any crime related to impersonating a law enforcement officer.
- (d) Ability to meet physical requirements reasonably appropriate to the assignment.
- (e) A background history and character suitable for a person representing the Department, as validated by a background investigation.

The Chief Probation Officer or the authorized designee may allow exceptions to these eligibility requirements based on organizational needs and the qualifications of the individual.

Fresno County Probation Department

Vendors, Volunteers and Student Interns

308.4 RECRUITMENT, SELECTION, AND APPOINTMENT

The Fresno County Probation Department shall endeavor to recruit and appoint only those applicants who meet the high ethical, moral, and professional standards set forth by this Department.

308.4.1 RECRUITMENT

Volunteers and student interns are recruited on a continuous basis consistent with Department policy on equal opportunity, nondiscriminatory employment terms. A primary qualification for participation in the application process should be an interest in and an ability to assist the Department in serving the public.

Requests for volunteers and student interns should be submitted in writing by interested Department members to the Personnel Unit through the requester's immediate supervisor. A complete description of the volunteer's or intern's duties and a requested time frame should be included in the request. All Department members should understand that the recruitment of volunteers and student interns is enhanced by creative and interesting assignments.

Vendors are recruited/selected in accordance with the Fresno County Purchasing Office contract/agreement process.

308.4.2 SELECTION

Vendor, volunteer and student intern candidates shall successfully complete this process before appointment:

- (a) Submit the appropriate written application.
- (b) Current TB skin test (completed within the last 6 months).
- (c) Successfully complete an appropriate-level background investigation, which may include fingerprinting, and/or obtaining information from local, state, federal and Department of Motor Vehicle databases.

308.4.3 APPOINTMENT

Volunteers and student interns shall be placed only in assignments or programs consistent with their knowledge, skills, and abilities and the needs of the Department. Volunteers' and student interns' interests will be considered when placed in assignments.

Volunteers and student interns serve at the discretion of the Chief Probation Officer.

Vendors are appointed and placed in accordance with the Fresno County Purchasing Office contract/agreement.

308.5 IDENTIFICATION

As representatives of the Department, vendors, volunteers and student interns are responsible for presenting a professional image to the community. Vendors, volunteers and student interns shall dress appropriately for the conditions and performance of their duties, in compliance with Personal Appearance Standards and Uniform and Non-Uniform attire policies unless excluded by the Department.

Fresno County Probation Department

Vendors, Volunteers and Student Interns

Vendors, volunteers and student interns will be issued Fresno County Probation Department identification cards, which must be carried at all times while on-duty. The identification cards will be the standard Fresno County Probation Department identification cards, except that "Volunteer" or "Student Intern" will be indicated on the cards.

308.6 PERSONNEL WORKING AS STUDENT INTERNS

Qualified regular Department personnel, when authorized, may also serve as student interns. However, this Department shall not utilize the services of student interns in such a way that it would violate employment laws or collective bargaining agreements or memorandums of understanding (e.g., a Juvenile Correctional Officer participating as a student intern for reduced or no pay). Therefore, members shall consult with the Personnel Unit prior to allowing regular department personnel to serve in a student intern capacity (29 CFR 553.30).

308.7 PERSONNEL UNIT

The function of the Personnel Unit is to provide a central coordinating point for effective volunteer management within the Department, and to direct and assist efforts to jointly provide more productive volunteer services.

The responsibilities of the Personnel Unit include but are not limited to:

- (a) Recruiting and selecting qualified volunteers and student interns.
- (b) Maintaining records for each vendor, volunteer and student intern.
- (c) Completing and disseminating, as appropriate, all necessary paperwork and information.
- (d) Maintaining a liaison with colleges and universities that provide student interns to promote the intern program with both students and the educational system.
- (e) Maintaining volunteer and student intern orientation and training materials and outlining expectations, policies, and responsibilities for all volunteers and student interns.

308.8 DUTIES AND RESPONSIBILITIES

Volunteers assist department personnel as needed. Assignments of volunteers may be to any division within the Department, as needed. Volunteers should be placed only in assignments or programs consistent with their knowledge, skills, interests, abilities and the needs of the Department. Student interns should be assigned to areas that meet the needs of both their educational program and the Department. Vendors will be assigned per the contract/agreement.

308.8.1 COMPLIANCE

Vendors, volunteers and student interns shall be required to adhere to all Department policies and procedures. Policies and procedures are available on the Department website and will be made available to each vendor, volunteer, and student intern upon appointment. The vendor, volunteer

Fresno County Probation Department

Vendors, Volunteers and Student Interns

and student intern shall become thoroughly familiar with these policies as directed by the Chief Probation Officer or the authorized designee.

Whenever a rule, regulation, or guideline in this Custody Manual refers to regular Department personnel, it shall also apply to vendors, volunteers and student interns, unless by its nature it is inapplicable.

Vendors, volunteers and student interns are required by this Department to meet Department-approved training requirements as applicable to their assignments.

308.9 TASK SPECIFIC TRAINING

Task-specific training is intended to provide the required instruction and practice for vendors, volunteers and student interns to properly and safely perform their assigned duties. Training should correspond to the assignment.

Vendors, volunteers and student interns shall be provided with the policies of the Department and procedures applicable to their assignments.

Vendors, volunteers and student interns shall receive position-specific training to ensure they have adequate knowledge and skills to complete the required tasks and should receive ongoing training as deemed appropriate by their supervisors or the authorized designee.

Training should reinforce to vendors, volunteers and student interns that they shall not intentionally represent themselves as, or by omission give the impression that they are, Juvenile Correctional Officers or other full-time members of the Department. They shall always represent themselves as vendors, volunteers or student interns.

All vendors, volunteers and student interns shall comply with the standards of conduct and with all applicable orders and directives, either oral or written, issued by the Department.

308.9.1 STATE REQUIREMENTS

The vendor, volunteer and student intern initial orientation shall include the following: safety and security issues and anti-discrimination policies.

308.10 SUPERVISION

Each vendor, volunteer and student intern must have a clearly identified supervisor who is responsible for direct management of that individual. This supervisor will be responsible for day-to-day management and guidance of the work of the vendor, volunteer or student intern and should be available for consultation and assistance.

Functional supervision of vendors, volunteers and student interns is the responsibility of the supervisor or the authorized designee in charge of their assigned duties. The following are some considerations that supervisors or the authorized designee should keep in mind while supervising vendors, volunteers and student interns:

- (a) Take the time to introduce vendors, volunteers and student interns to members on all levels.

Fresno County Probation Department

Vendors, Volunteers and Student Interns

- (b) Ensure vendors, volunteers and student interns have work space and necessary office supplies.
- (c) Make sure the work is challenging. Do not hesitate to give vendors, volunteers and student interns assignments or tasks that will utilize these valuable resources.
- (d) Ensure the work for student interns meets the needs of their educational program, while also meeting the needs of the Department.

308.10.1 EVALUATIONS

Student interns may need evaluations as a requirement of their educational program.

308.10.2 FITNESS FOR DUTY

No vendor, volunteer or student intern shall report for work or be at work when the individual's judgment or physical condition has been impaired due to illness or injury, or by the use of alcohol or drugs, whether legal or illegal.

Vendors, volunteers and student interns shall report to their supervisors any change in status that may affect their ability to fulfill their duties. This includes but is not limited to:

- (a) Driver's license.
- (b) Arrests.
- (c) Criminal investigations.
- (d) All law enforcement contacts.

308.11 INFORMATION ACCESS

Volunteers and student interns should not have access to or be in the vicinity of criminal histories, investigative files, or information portals. Unless otherwise directed by a supervisor, the duties of the position, or Department policy, all such information shall be considered confidential. Only that information specifically identified and approved by authorized members shall be released. Confidential information shall be given only to persons who have a need and a right to know as determined by Department policy and supervisory personnel.

A vendor, volunteer or student intern whose assignment requires the use of, or access to, confidential information will be required to be fingerprinted and have the fingerprints submitted to the California Department of Justice to obtain clearance. Vendors, volunteers and student interns working this type of assignment shall receive training in data practices and shall be required to sign a CLETS Employee/Volunteer Statement before being given an assignment with the Department. Subsequent unauthorized disclosure of any confidential information verbally, in writing, or by any other means by the vendor, volunteer, or student intern is grounds for immediate dismissal and possible criminal prosecution.

Vendors, volunteers and student interns shall not address public gatherings, appear on radio or television, prepare any article for publication, act as correspondents to newspapers or other periodicals, release or divulge any information concerning the activities of the Department, or

Exhibit F

Fresno County Probation Department

Vendors, Volunteers and Student Interns

maintain that they represent the Department in such matters without permission from the proper Department personnel.

308.11.1 RADIO AND DATABASE ACCESS USAGE

The supervisor or the authorized designee shall ensure that radio and database access training is provided for vendors, volunteers, and student interns whenever necessary.

308.12 EQUIPMENT

Any property or equipment issued by the Department shall be for official and authorized use only. Any property or equipment issued to a vendor, volunteer or student intern shall remain the property of the Department and shall be returned at the termination of service.

308.13 TERMINATION OF SERVICES

If a vendor or volunteer is the subject of a personnel complaint or becomes involved in an internal investigation, the matter shall be investigated in compliance with the Personnel Complaints Policy. If a student intern is the subject of or is involved in an internal investigation, the coordinator of the educational program that sponsors the intern should be notified.

Vendors and volunteers are considered at-will and may be removed from service at the discretion of the Chief Probation Officer or the authorized designee, with or without cause. Vendors and volunteers shall have no property interest in their continued appointments. Vendors and volunteers may resign from service with the Department at any time. It is requested that vendors and volunteers who intend to resign provide advance notice and a reason for their decision.

308.14 ISSUED DATE

- 02/18/2022

Exhibit G

FRESNO COUNTY SHERIFF'S OFFICE JAIL DIVISION POLICIES AND PROCEDURES

TITLE: HOSTAGE SITUATIONS
FILE: HOSTAGE

NO: B-130

EFFECTIVE DATE: 12-18-89
96, 09-01-99,

REVISED: 08-06-90, 12-25-94, 05-06-
12-01-10

AUTHORITY: Sheriff M. Mims

APPROVED BY: Assistant Sheriff T. Gattie

REFERENCE: California Code of Regulations, Title 15, Section 1029(a)(7)(B) and
Penal Code Section 236.

PURPOSE:

The purpose of this policy is to establish procedures which provide for the resolution of a hostage-taking incident while preserving the safety of staff, public, inmates, and hostages, and maintaining facility security.

POLICY:

The Fresno County Sheriff's Office Jail Division maintains a **NO HOSTAGE FACILITY** and will not consider bargaining with hostage takers for ANY reason.

It is the policy of the Fresno County Sheriffs Office Jail Division that once any staff member is taken hostage, they immediately lose their authority and any orders issued by that person will not be followed regardless of their rank or status.

It is the policy of the Fresno County Sheriffs Office Jail Division that the primary responsibility of all staff members in a hostage situation is to protect every person involved, if possible, from serious injury or death.

PROCEDURES:

I. DEFINITION

HOSTAGE SITUATION: any staff member, citizen or inmate held against their will by another person for the purpose of escape, monetary gain or any reason which may place an individual in danger of losing life or suffering serious injury.

II. NOTIFICATIONS. CONTAINMENT AND CONTROL OF THE SITUATION

A. Emergency procedures and notifications shall be implemented as per Emergency Planning procedures (B-101/FILE: EMERGENCY).

Exhibit G

FRESNO COUNTY SHERIFF'S OFFICE JAIL DIVISION POLICIES AND PROCEDURES

TITLE: HOSTAGE SITUATIONS
FILE: HOSTAGE

NO: B-130

- B. The Watch Commander will notify the Patrol Watch Commander and apprise them of the incident. The Patrol Watch Commander may be requested to activate the Crisis Negotiations Team (CNT), outside support agencies, equipment, personnel, and dispatch a detective to the scene for the crime report.

III. DURING NEGOTIATIONS

- A. While at the scene, the CNT members will conduct all verbal or written communications between the hostage taker(s) and the Incident Commander. CNT will immediately notify the Incident Commander of any changes in the following situations:
 - 1. Hostage status
 - 2. Incident changes and developments
 - 3. Hostage taker demands
 - 4. Any and all pertinent information concerning the incident
- B. Staff members at the scene not actively involved with negotiations will not act or speak out to the hostage taker(s) or hostages.
- C. The Tactical Commander will formulate a plan to take the necessary actions, using the appropriate force, to terminate the hostage situation in the event negotiations fail. Hostage safety will be of paramount concern.

IV. HOSTAGE SURVIVAL STRATEGIES

- A. If taken hostage, it is important to make the transition from being a victim to being a survivor. The following are not strict rules that must be rigidly followed, but rather general guidelines. There will always be exceptions.
 - 1. Regain/maintain composure. Try to be calm, focused and clear-headed at all times. Do not stand out from other hostages. Drawing unnecessary attention increases the chance of being singled out and victimized.
 - 2. Maintain a low-key, unprovocative posture. Overt resistance is usually counterproductive in a hostage situation.
 - a. Remain calm and follow instructions. Comply with the hostage takers when at all possible.
 - b. Be stoic. Maintain an outward face of acceptance of adversity with dignity. Avoid open displays of cowardice and fear. Inmates will view frailty and feebleness as weakness, which may lead to victimization.

Exhibit G

FRESNO COUNTY SHERIFF'S OFFICE JAIL DIVISION POLICIES AND PROCEDURES

TITLE: HOSTAGE SITUATIONS
FILE: HOSTAGE

NO: B-130

- c. Do not antagonize, threaten or aggravate the hostage takers. Avoid saying "no", or arguing with the hostage takers. Do not act authoritative. The hostage takers must make it known that they are in charge.
 - d. Eye contact may be regarded as a challenge; make eye contact with the hostage takers sparingly.
 - e. Fight off basic instincts, such as anger and hostility. Be polite and remain alert. Speak normally and don't complain.
- 3. Hostages should try to establish a level of rapport or communication with their captors in attempt to get the captors to recognize them as human beings.
- 4.
 - a. Find a mutual ground, an association with the hostage takers. Foster communication on non-threatening topics (e.g., family, hobbies, sports, interests).
 - b. Use the captors' first names, if known. However, if hostage takers are attempting to conceal their identity, do not give any indication that they are recognized.
 - c. Listen actively to the captors' feelings and concerns, but never praise, participate in, or debate their "cause". If they want to talk about their cause, act interested in their viewpoints. Avoid being overly solicitous, which may be viewed as patronizing or insincere.
 - d. Do not befriend the inmates; such an attempt will likely result in exploitation.
 - e. Try asking for items that will increase personal comfort. Make requests in a reasonable, low-key manner.
- 5. Be prepared to be isolated and disoriented.
 - a. Do not talk to other hostages. The hostage takers may think a plot is being formed.
 - b. Develop mind games to stimulate thinking and maintain mental alertness.
- 6. Be tolerant of fellow hostages. Just as each person has different reactions to stress, each individual will have different methods of coping as a hostage. Some methods are not effective and may endanger the group, or be annoying to other hostages (e.g., constant talking). Try to help these people cope in other ways.
- 7. Gather intelligence. Hostages should take in and store as much detail, about their captors as possible without drawing attention to their efforts. Make mental notes

Exhibit G

FRESNO COUNTY SHERIFF'S OFFICE JAIL DIVISION POLICIES AND PROCEDURES

TITLE: HOSTAGE SITUATIONS
FILE: HOSTAGE

NO: B-130

and attempt to gather the following information: identification of the ring leader, the number of hostage takers, the type of weapons they are using, their tactics, location within the area, etc.

8. Maintain hope. Depending on the circumstances, resolution of hostage situations can be a lengthy process.
- B. Stay away from doors and windows through which rescue teams may enter or shoot. If a rescue is attempted, drop to the floor and keep hands in view.
- C. If there is a chance to escape, the hostage should be certain of their success.
 1. Balance the likely payoff of any behavior with the possible consequences. Hostage takers may use violence or death to teach a lesson.
 2. Realize that Central Control will not open any doors for anyone.

Hostages should be aware of the "Stockholm Syndrome", whereby hostages begin to show sympathy toward their captors. Hostages who develop Stockholm Syndrome often view the captor as giving life by simply not taking it. Such hostages often misinterpret a lack of abuse as kindness and may develop feelings of appreciation for the perceived benevolence

Exhibit H

THE PRISON RAPE ELIMINATION (PREA) ACT

All contractors must comply with the Prison Rape Elimination (PREA) Act as stated below:

The Contractor shall comply with all Prison Rape Elimination (PREA) Act standards for juvenile correctional facilities. Training will be provided by Probation at no charge to the Contractor. The Contractor will ensure that all staff assigned to work at the Juvenile Justice Campus (JJC) undergo a pre-employment Live Scan and criminal background security clearance by the Probation Department at no charge to the Contractor. No alcoholic beverages/drugs will be brought into any facility. Nor will anyone under the influence of alcoholic beverages or drugs be allowed inside. In the event of any disturbance inside the facilities, the Contractor's employees will immediately follow the orders of the Facility Administrator or his/her designees.

The Contractor shall comply with all Probation Department Policies and Procedures. In the event of a dispute involving the County staff and the contract employee, the on-duty Facility Administrator will have the final decision." **INFORMATION ON THE PRISON RAPE ELIMINATION ACT CAN BE FOUND HERE:** <http://www.prearesourcecenter.org/>

BACKGROUND INVESTIGATIONS AND IDENTIFICATION (ID) BADGES

Background Investigations

Prior to the beginning of any services, one (1) background check may be required for every member of the Contractor's personnel providing services to a building location for the life of the agreement. The background check may be required before access is given to any County facility/property. Clearance will only be granted after a successful background check, completed by the County of Fresno Sheriff's Department. Background checks provided by any agency other than the County of Fresno Sheriff's Department will not be accepted.

The current cost of a background check is \$52 per person. This cost will be incurred by the Contractor. One check covering the cost of background checks for all employees shall be made payable to: Sheriff, County of Fresno. The Contractor will be notified regarding the result of background checks. Those that are accepted will report to County of Fresno Security to have their photo taken and ID badge issued.

Background checks are done on a first-come, first serve basis between the hours of 7:00 a.m and 12:00 noon. Monday through Friday. The process takes approximately 20 minutes time. The amount of time it takes to receive the result of background checks varies from one day to a month (or longer), dependent upon the individual's history.

Individuals who are cleared through this process are entered into the Department of Justice database. Their records are flagged and the County of Fresno Sheriff's Department is notified if the person is ever arrested in the future.

When required by County, applicants' background checks must be approved prior to entering any County facility. Approval will not be granted to any individual possessing any of the following circumstances:

1. They have been convicted of a felony, or any crime involving moral turpitude, or carrying or possessing a dangerous weapon.
2. They have ever been charged with a felony or are currently under investigation for a felony.
3. They are charged with or convicted of any crime committed in or at a correctional institution.
4. They are currently on parole or probation or are a sentenced inmate at any correctional facility.
5. They have been refused a license as a private investigator or had such license revoked.
6. They have fraudulently represented themselves, their credentials, their employment or their criminal or arrest record on their application.
7. Make omissions or false statements on their application.
8. They have no valid reason for entering a facility.
9. Their admission into a facility could represents a threat to security, staff or inmate safety.
10. Further information regarding the criteria for background check clearance, including an appeal for process for someone who may be denied clearance is available upon request.

Exhibit I

Identification (ID) Badges

The Contractor's employees will be issued a badge that must be worn and be visible at all times during performance of work in any County building to identify the wearer as an individual who is authorized to enter County facilities.

1. ID badges will be given only after successfully completing the background investigation. ID badges will be issued when the photo is taken. If electronic access to any County facility is required, activation of the badge may take an additional 48 hours to complete.
2. The wearer will not escort or bring any other individuals into any County facilities. County issued ID badges are for the exclusive use of the individual named and pictured on the badge.
3. All ID badges will remain the property of the County and are returnable upon demand or upon the expiration of the contract. The Contractor will be responsible for collecting all ID badges issued and turning them in to the County Security Office when a contract ends or when an employee leaves employment. The Contractor will assume all responsibility for their employee's use of and the return of the County ID badges.

The ID badges will only be issued to individuals passing the Background check. Each individual will need to present themselves in person with a valid, clean, and legible copy of a Driver's license or State issued Identification Card to receive an ID badge.

Exhibit J

INFORMATION SECURITY RIDER

This Information Security Rider ("Rider") supplements the agreement for the purchase of Products and/or Services (each as defined below) ("Agreement") in effect between the customer set forth therein ("Customer") and the Johnson Controls affiliate set forth therein ("Johnson Controls"). In the event of conflict or inconsistency between this Rider and the Agreement, this Rider shall control.

1. **Scope**. This Rider describes the information security measures that Johnson Controls has implemented and maintains with respect to the Products and Services purchased, licensed or subscribed to by Customer under the Agreement and Johnson Controls' Support Infrastructure, as well as certain related obligations of Customer. This Rider is effective on the date of last signature below ("Effective Date") and continues until the Agreement is terminated or expires.

2. **Definitions**. Capitalized terms have the definitions set forth below or elsewhere in this Rider:

"Cloud Services" means Johnson Controls' software-as-a-service offering subscribed to by the Customer and which hosts Customer Data.

"Confidential Information" means Customer's confidential or proprietary information that is subject to a confidentiality agreement in effect between Johnson Controls and Customer ("Confidentiality Agreement"), and the public disclosure of which would be harmful to Customer's business or personnel.

"Customer's Assets" means Customer's devices (e.g., desktops or laptops), software and platforms accessed by Johnson Controls during the performance of Services.

"Customer Data" means the Personal Data and/or Confidential Information of Customer that is accessible to Johnson Controls during its performance under the Agreement.

"Customer's Network" means the Customer's internal information technology network which includes certain hardware, software, communication systems, infrastructure, network architecture, equipment and electronic devices.

"Cyber Resources Website" is found at <https://www.johnsoncontrols.com/trust-center>.

"EOL Products" means Products that Johnson Controls has announced are "end of life", "end of support" or a similar designation, or which contain Installed Software that is older than the current version or one immediate version prior.

"Hardware" means connected hardware manufactured by Johnson Controls that processes Customer Data.

"Installed Software" means Johnson Controls-owned software included with Hardware (including firmware pre-installed on Hardware) and any other Johnson Controls software provided for installation on premises at the Customer's location, but excluding Third-Party Products and Cloud Services.

"Malware" means viruses, Trojan horses, backdoors, worms, spyware and other malware that enable unauthorized access, disabling, or modification to software, systems, devices or networks.

"Personal Data" means information relating to an identified or identifiable natural person that is regulated by applicable privacy or data protection laws ("Data Protection Laws").

"Products" means Hardware, Installed Software, and Cloud Services.

"Services" means professional services (e.g., installation, implementation, support, maintenance) performed by Johnson Controls or its subcontractors.

Exhibit J

“Support Infrastructure” means Johnson Controls’ (a) enterprise information technology network(s) that includes certain hardware, software, communications systems, infrastructure, network architecture, equipment and electronic devices, (b) service technician laptops, desktops or other devices provided by Johnson Controls and used to connect to the Customer’s Network (“JCI Laptops”), and (c) service or business support centers. “Support Infrastructure” does not include Products, Customer’s Assets, Customer’s Network, or Third-Party Products.

“Third-Party Products” means (a) hardware, software, cloud services or other products manufactured or licensed by a third party, and/or (b) professional services performed by a third party that is not a Johnson Controls subcontractor, even if such hardware, software, cloud services, products or professional services are re-sold or sublicensed by Johnson Controls to Customer.

3. General Information Security.

- a. **Confidentiality.** Johnson Controls’ employees and subcontractors with access to Customer Data, Customer’s Network, Customer’s Assets, or Customer’s premises are subject to an obligation of confidentiality by statute or a contract containing industry standard confidentiality provisions (or more stringent confidentiality obligations if required in the Agreement).
- b. **Dedicated Security Organizations.** Johnson Controls maintains dedicated, global, enterprise product security and information security organizations (respectively, its “Global Product Security” and “Global Cybersecurity” organizations), that collaborate on security initiatives within the organization. Johnson Controls also maintains dedicated privacy and physical enterprise security departments within the organization.
- c. **Vendor Management.** Johnson Controls maintains a vendor management program and subcontractors with access to Customer Data, Customer’s Network, Customer’s Assets or Customer’s premises are required to execute confidentiality, privacy and security terms with Johnson Controls commensurate with the nature of such vendor’s access.
- d. **Training.** Johnson Controls maintains a Cybersecurity Training and Awareness Policy that requires all employees and contingent workers with Johnson Controls login credentials to participate in mandatory cybersecurity training. Johnson Controls also maintains a Global Information Security Awareness Program that delivers end user information security and policy awareness education and content commensurate with the user’s role and regulatory requirements. Johnson Controls maintains a privacy training program that requires all employees and contingent workers with Johnson Controls login credentials to participate in mandatory privacy training. Advanced training may be required for certain business functions, roles or responsibilities, such as regulatory compliance trainings (e.g., for PCI DSS).
- e. **Reporting Hotline.** Johnson Controls maintains an anonymous ethics reporting hotline where employees can report security concerns or incidents, among other ethics-related concerns. Johnson Controls’ employees receive training on use of the ethics reporting hotline.
- f. **Background Checks.** Johnson Controls’ employees who access Customer Data, Customer’s Network, Customer’s Assets or Customer’s premises in the course of their job duties must undergo an industry standard, pre-employment, background check unless prohibited by applicable laws. It is Johnson Controls’ policy to contractually require its subcontractors who have access to Customer Data, Customer’s Network, Customer’s Assets or Customer’s premises to also undergo industry standard background checks.
- g. **Third-Party Certifications and Audits.** Johnson Controls’ internal, enterprise, information technology infrastructure and all Johnson Controls’ Cloud Services align to the International Organization for Standardization (ISO) 27001, or a materially similar standard recognized within the industry. Select Products may be reported or certified to comply under SSAE 18 SOC 2 Type I, SSAE 18 SOC 2 Type II, ISO 27001 (or their successor standards), or other similar standards. Such standards and related reports (or summaries thereof) may be found at the Cyber Resources Website, which may be updated from time-to-time. Customer should coordinate with its account manager to learn more about the current reporting or compliance status for any given Product.

Exhibit J

- h. **Security Testing of Products.** As part of Johnson Controls' Product release process, Johnson Controls performs security testing, such as vulnerability scans and internal/external penetration testing, each as appropriate and applicable.
 - i. **Disaster Recovery.** Johnson Controls has implemented and maintains disaster recovery policies and procedures with regard to its Support Infrastructure and Cloud Services.
4. **Support Infrastructure Security.** Johnson Controls has implemented and maintains (i) an information security policy and (ii) reasonable physical, technical and organizational measures designed to protect against unauthorized or unlawful access, modification or damage to Johnson Controls' Support Infrastructure.
- a. **Attack Monitoring and Prevention.** Johnson Controls performs continuous monitoring of its Support Infrastructure, including its network traffic, with the goal of identifying and preventing potential vulnerabilities or threats to the Support Infrastructure. Johnson Controls' internal Global Cybersecurity organization has implemented policies regarding Johnson Controls-managed endpoint device protections, including policies addressing anti-malware, data loss prevention, vulnerability detection, and privilege access management.
 - b. **Password Reset Policy.** Johnson Controls has implemented and enforces an internal password reset policy.
 - c. **Multi-Factor Authentication (MFA).** Johnson Controls' administrators with access to its Support Infrastructure components are required to use Multi-Factor Authentication ("MFA").
 - d. **Identity and Access Management.** Johnson Controls has implemented and maintains identity and access management policies, procedures and technologies designed to limit access to its Support Infrastructure and facilities where Customer Data or systems that process Customer Data are accessible or stored, to those with a need-to-know pertaining to their job duties for Johnson Controls. Access rights are assigned according to least privileged principles. Johnson Controls maintains a dedicated enterprise security function that addresses physical and environmental security at Johnson Controls' locations.
 - e. **Acceptable Use Policy.** Johnson Controls has implemented an industry standard acceptable use policy regarding the access and use of its Support Infrastructure and assets that it requires its employees and subcontractors to comply with. The acceptable use policy is published annually and Johnson Controls mandates that its employees provide attestations of compliance relating to such policy.
 - f. **Mobile Device Management.** Johnson Controls has implemented and maintains a mobile device management policy ("MDM Policy") that requires encryption for Johnson Controls'-managed mobile devices. Any personal devices that process Johnson Controls' or a customer's information are subject to the MDM Policy and must be enrolled in Johnson Controls' mobile device management platform. Personal devices that are not managed by Johnson Controls are prohibited from connecting to Johnson Controls' or its customers' networks.
 - g. **Business Continuity Plan.** Johnson Controls has implemented and maintains a business continuity plan ("BCP") for its Support Infrastructure designed with the goal of preventing and promptly responding to cyber attacks and other threats to the security of its Support Infrastructure.
 - h. **Encryption.** Johnson Controls' internal network traffic is encrypted.
5. **Access to Customer's Network, Customer's Assets and Customer's Premises.**
- a. **Customer Policies.** Johnson Controls will make commercially reasonable efforts to comply with Customer's reasonable security and access policies with respect to Johnson Controls' access and use of Customer's Network, Customer's Assets,

Exhibit J

and Customer's premises, so long as such policies are provided to Johnson Controls in advance of beginning work under the Agreement and do no conflict with the Agreement.

- b. **Limited Access and Use.** Johnson Controls' employees and contractors shall only access and use Customer's Assets, Customer's Network, and the data accessible therein as necessary to perform its obligations under the Agreement
- c. **Restriction or Revocation.** Johnson Controls understands and agrees that its access to Customer's Assets, Customer's Network and Customer's premises may be restricted or revoked by Customer at any time (although Johnson Controls is not liable for its inability to perform under the Agreement due to such restricted or revoked access).
- d. **Confidentiality.** Johnson Controls will treat any data and information accessible to it via the Customer's Network and Customer's Assets as Customer's confidential and proprietary information.
- e. **JCI Laptops.** While on Customer's premises, Johnson Controls will not connect hardware (physically or via a wireless connection) to Customer's Network unless reasonably required for Johnson Controls to perform the Services. If Johnson Controls uses JCI Laptops to connect to Customer's Network, such JCI Laptops will be managed by Johnson Controls, have end-point protection and response, undergo regular patching, are configured with Bitlocker encryption (or an equivalent), and will be protected by up-to-date security agents. Upon reasonable request by Customer, Johnson Controls will permit Customer to visually inspect the JCI Laptops, under the supervision of Johnson Controls' security personnel, for the sole purpose of verifying compliance with the security measures described in this Rider, so long as Johnson Controls has reasonably determined that such inspection will not breach any confidentiality obligation it has to other customers.

6. Installed Software.

- a. **Security By Design.** Johnson Controls has achieved and will maintain a certification under ISASecure Secure Development Lifecycle Assurance ("SDLA"), in conformance with ISA/IEC 62443-4-1 (or its successor or materially similar standard) for all Johnson Controls' Installed Software, which requires Johnson Controls to follow industry standard (or better) requirements pertaining to "security by design." Product development teams consider security at every stage in the development process.
- b. **Patching.** Johnson Controls will use commercially reasonable efforts to make patches available for Installed Software according to the patching policies set forth in its hardening guides available on the Cyber Resources Website for the then-current version of the Installed Software and the immediate version prior ("JCI Patching Policies"). Unless separately provided for in a planned services agreement with Johnson Controls, Johnson Controls will not conduct the patching (i.e., the installation of the patch), and it is Customer's responsibility to identify and install available patches. Customer may sign-up for patch notifications at the Cyber Resources Website. Unless otherwise specified, Johnson Controls will not make security patches available for EOL Products. If applicable law or regulation require a change in any of the timelines set forth in the JCI Patching Policies, Johnson Controls shall satisfy such timelines as required under applicable law or regulation. Johnson Controls, in coordination with CISA (Cybersecurity and Infrastructure Security Agency), periodically publishes product security vulnerability information on its Cyber Resources Website.

7. Cloud Services.

- a. **Information Security.** Johnson Controls has implemented and maintains reasonable physical, technical and organizational measures designed to protect the confidentiality, security and integrity of Customer Data in Johnson Controls' possession or control or that is otherwise processed in the Cloud Services. Johnson Controls (or its subcontractors) performs continuous monitoring of its Cloud Services with the goal of identifying and preventing potential vulnerabilities or threats to the Cloud Services.
- b. **Security By Design.** Johnson Controls has achieved and will maintain a certification under ISASecure Secure Development Lifecycle Assurance ("SDLA"), in conformance with ISA/IEC 62443-4-1 (or its successor or materially similar standard) for all Johnson Controls' Cloud Services, which requires Johnson Controls to follow industry standard (or better) requirements

Exhibit J

pertaining to “security by design.” Product development teams consider security at every stage in the development process.

- c. **Encryption.** Customer Data stored or processed in the Cloud Services is encrypted in transit and Johnson Controls’ OpenBlue offerings are also encrypted at rest.
 - d. **Penetration Testing.** As a part of its software development process, Johnson Controls conducts penetration testing on Cloud Services that process Customer Data with the purpose of identifying and thereafter remediating security vulnerabilities in its Cloud Services.
 - e. **Hosting.** If Johnson Controls uses third-party vendors to host Cloud Services, Johnson Controls uses reputable third-party vendors who are recognized within the industry for the reliability and security of their services, such as Amazon Web Services (AWS) or Microsoft Azure. Johnson Controls is a global organization; therefore, unless the parties have expressly agreed to specific location requirements in the Agreement (which is not available for all Cloud Services), Johnson Controls may host and support Cloud Services on a worldwide basis.
 - f. **Intrusion Detection.** Johnson Controls uses industry standard intrusion detection and prevention systems with respect to the Cloud Services, that are designed to detect known Malware and intrusion. Johnson Controls will promptly install all relevant security patches released with respect to such programs as recommended by its security personnel.
 - g. **Business Continuity Plan.** Johnson Controls has implemented and maintains a BCP for its Cloud Services designed with the goal of preventing and promptly responding to cyber attacks and other threats to the security and availability of its Cloud Services.
 - h. **Logical Separation.** Customer Data stored or otherwise processed in the Cloud Services is logically separated from other customers’ data and any of Johnson Controls’ data.
 - i. **Access Controls.** Johnson Controls’ administrators with access to the Cloud Services are required to use MFA. Access rights are assigned according to least privileged principles.
8. **Third-Party Products.** Johnson Controls does not make any representations, warranties or commitments pertaining to Third-Party Products, including without limitation relating to their security, quality or functionality. However, Johnson Controls does commit that its installation and support of Third-Party Products (if purchased in the Agreement) will comply with the terms and conditions in this Rider, such as those terms pertaining to Johnson Controls’ access to the Customer’s Network and Customer Data. All terms and conditions pertaining to Third-Party Products are either between Customer and the applicable third-party supplier or Johnson Controls will make commercially reasonable efforts to pass-through to Customer any relevant third-party warranties to the extent applicable and available regarding Third-Party Products.

9. Customer Audits.

- a. **Process.** If required under applicable Data Protection Law, Cloud Services customers may audit Johnson Controls, no more than once per year during the term of the Agreement, for the sole purpose of confirming Johnson Controls’ compliance with this Rider or compliance with law, only using the following process and so long as Customer (or its independent auditor if applicable) is subject to a non-disclosure agreement reasonably acceptable to Johnson Controls:

Step 1: Upon Customer’s written request, Johnson Controls will provide to Customer a summary(ies) of third-party audits (e.g., SOC 2 Type II) performed or third-party certifications (e.g., ISO 27001) received pertaining to the relevant purchase (“Audit Report”) for Customer’s remote review (e.g., screen sharing) and consideration, and any such Audit Report will be deemed sufficient evidence of Johnson Controls’ compliance with the terms in this Rider.

Step 2: However, if Customer demonstrates by reasonable evidence that the information provided in *Step 1* does not show Johnson Controls’ compliance with this Rider or does not permit Customer to comply with Data Protection Laws, then

Exhibit J

Customer may either schedule a discussion with relevant Johnson Controls personnel via the Johnson Controls Trust Center at TrustCenter@jci.com to discuss its concerns pertaining to Johnson Controls' compliance with this Rider and/or Customer may send to Johnson Controls a security questionnaire that is tailored specifically to the purchases made in the Agreement. Johnson Controls will respond to such security questionnaire no more than once per year, and will only respond to questions that are relevant to the purchases made in the Agreement. Additional professional service fees may apply if responding to Customer's security questionnaire requires more than eight (8) hours for Johnson Controls to reasonably complete. Any security questionnaire must be limited to the scope of work provided by Johnson Controls in the Agreement and commensurate with the sensitivity of the Customer Data to which Johnson Controls has access.

- b. **Prohibitions.** Except as stated in Section 9(c), Johnson Controls does not permit audits of its facilities or physical testing of any kind. For example, Johnson Controls' policy is that its customers are prohibited from performing facility audits or penetration or other tests of its Support Infrastructure and Cloud Services. Johnson Controls does not permit over-the-shoulder testing. These limits are intended to keep Johnson Controls' facilities, Support Infrastructure and Cloud Services more secure and maintain the confidentiality of Johnson Controls' proprietary information and the confidential information of Johnson Controls' other customers.
 - c. **Exceptions Required by Law.** Notwithstanding Sections 9(a) and 9(b), if Customer cannot comply with Data Protection Laws without performing a broader or more in depth audit than described in such Sections, then Johnson Controls will reasonably cooperate with Customer in the performance of such audit, but Johnson Controls will only provide the minimum access necessary to its facilities, systems, Support Infrastructure, personnel, Cloud Services and documentation that is required in order for Customer to comply with such Data Protection Laws. If there is any method by which Customer can comply with Data Protection Laws that does not require access to Johnson Controls' facilities, systems, Support Infrastructure, or Cloud Services (or testing by Customer thereof), then Johnson Controls may decline to permit such access in its sole discretion.
 - d. **Additional Requirements.** Customer must provide at least thirty (30) days prior written notice of any requested audit, and such audit will occur at a time that minimizes business interruptions to Johnson Controls. Customer may use an independent auditor to perform the audit described in this provision, subject to Johnson Controls' prior written approval of such auditor, not to be unreasonably withheld. All individuals performing an audit or receiving information pertaining to the audit must be subject to a written confidentiality agreement that is reasonably acceptable to Johnson Controls. Additional hourly service charges may apply for any audit (including time spent preparing for the audit and responding to a security questionnaire) exceeding eight (8) hours.
10. **EOL Products.** This Rider, and Johnson Controls' commitments and obligations herein, do not apply to EOL Products. Security for EOL Products is solely Customer's responsibility.
 11. **Incident Response.** Johnson Controls maintains a dedicated, 24/7 security operations center. In the event of a confirmed, unauthorized or unlawful access, acquisition or disclosure of Personal Data in Johnson Controls' possession and control ("Incident"), Johnson Controls will notify Customer within 72 hours of confirmation, unless a shorter timeframe is required of Johnson Controls by Data Protection Law.
 12. **Liability.** Johnson Controls disclaims all liability, and Customer waives all claims against Johnson Controls, arising from or related to security incidents of any kind (including but not limited to Incidents) except to the extent an Incident is caused solely by Johnson Controls' breach of the security provisions in this Rider or negligent acts or omissions. Further, the limitations of liability and exclusions of damages set forth in the Agreement shall apply to all claims arising from or related to the subject matter of this Rider, except that (i) in no event shall Johnson Controls be liable for special, incidental, indirect, consequential or punitive damages related to or arising out of damages or losses related to a security incident of any kind (including an Incident) and/or a breach of the security provisions herein or in the Agreement ("Security Losses") and (ii) in the event that Security Losses are not subject to a monetary cap on Johnson Controls' liability in the Agreement, Johnson Controls' aggregate liability for any and all Security Losses shall be subject to an aggregate cap of the lesser of (i) payments made to Johnson Controls under the Agreement in the twelve month period preceding the date on which such claim arose and (ii) \$500,000.00 U.S.D.

Exhibit J

13. Customer Obligations.

- a. **Data Minimization.** Customer shall follow data minimization principles in compliance with industry standards and Data Protection Laws. Customer shall limit Johnson Controls' access to Customer Data to that which is required for Johnson Controls to perform its obligations under the Agreement. Unless expressly permitted in the relevant Product documentation or required in order for Johnson Controls to provide the Services, Customer shall not provide or make accessible to Johnson Controls any (a) Personal Data that is considered "sensitive personal data" or "special categories of personal data" (or the like) under Data Protection Laws or (b) Personal Data of minors under eighteen (18) years old. Customer shall not enter Personal Data into fields in the Cloud Services platforms that are not designed or intended for submitting Personal Data.
- b. **Customer's Network.** Unless purchased by Customer in a services agreement, any monitoring, testing or event logging related to Customer's Network or regarding devices/software which reside within Customer's Network are solely the responsibility of Customer (although Customer must also comply with any use restrictions pertaining to Installed Software that are set forth in the Agreement). Customer is solely responsible for establishing and maintaining (i) the Customer's Network, and (ii) physical, technical and organizational measures designed to protect the confidentiality, security and integrity of the Customer's Network, and all devices/software thereon, in compliance with industry standards and Data Protection Laws, which include, without limitation, using reputable, industry standard anti-virus / anti-malware programs, security patches and firewalls, and maintaining industry standard access control policies and procedures. Customer is solely responsible for maintaining disaster recovery policies and procedures and a business continuity plan for Customer's Network and the devices/software that reside thereon. Except as described in Section 5 above, Customer is solely responsible for any Customer Data that is stored or processed within Customer's Network, including processed on Hardware or Installed Software that is connected to Customer's Network. Customer understands and agrees that Johnson Controls' Services do not include providing security for Customer's Network or the devices/software that reside thereon.
- c. **Database Support.** If Customer sends or makes accessible to Johnson Controls a database for maintenance, support, inspection, repair or other similar purposes, Customer is solely responsible for ensuring that such database does not contain Customer Data and that all data thereon has been de-identified and anonymized.
- d. **Shared Responsibility for Hardening of Systems.** Cybersecurity is a shared responsibility between Johnson Controls and Customer. Johnson Controls publishes best practices and hardening guides at the Cyber Resources Website, and it is Customer's responsibility to review and implement such practices and guides.
- e. **Indemnity.** Customer will indemnify, defend and hold harmless Johnson Controls from and against any claims, actions, losses, liabilities, costs, expenses and settlements brought by any person or entity (including Customer's insurer) to the extent arising from Customer's breach of this Section 13.

14. **Analytics Data.** Nothing in this Rider shall be interpreted as prohibiting Johnson Controls from collecting, using and sharing systems usage data, analytics data, performance data or other similar data pertaining to or collected from the Products and performance of the Services, so long as such data does not contain Customer Data ("Analytics Data"). Johnson Controls is the sole and exclusive owner of Analytics Data.
15. **Privacy.** If Johnson Controls will process Personal Data under the Agreement, then the data processing addendum found at <https://www.johnsoncontrols.com/privacy-center/global-privacy-notice/johnson-controls-data-processing-addendum> ("DPA") shall apply as described therein, unless different privacy terms are stated in the Agreement. To the extent possible, this Rider and the DPA shall be interpreted as consistent and supplementary to each other, but in the event of conflict between this Rider and the DPA, the DPA shall control.
16. **Exclusions.** In addition to any exceptions or exclusions set forth elsewhere in this Rider, this Rider does not apply to Cloud Services or Installed Software that are pre-production, pre-GA, beta versions or that are provided on a evaluation or trial basis. This Rider does not apply to data or information that is neither Personal Data nor Confidential Information, such as utility data, non-confidential building data and building data that is publicly available, chiller vibration information, sensor point information, equipment performance data, and the like. This Rider does not apply to information that is or becomes publicly available through

Exhibit J

no breach by Johnson Controls of a Confidentiality Agreement or that is disclosed to Johnson Controls by a third party without an obligation of confidentiality.