GLOBAL SERVICES AGREEMENT

Effective Date: _____

This **GLOBAL SERVICES AGREEMENT** is made as of the Effective Date by and between Johnson Controls, Inc., 5757 North Green Bay Avenue, Milwaukee, Wisconsin 53209, for itself and on behalf of its Affiliates (collectively, "JCI"), and

Name: (the "Supplier"): _____

Street Address: _____

City, State, Zip: _____

1. BACKGROUND

Supplier has the know-how and expertise to provide JCI with certain services unique to Supplier. Supplier desires to provide to JCI, and JCI desires to obtain from Supplier, Services (as defined below) on the terms and conditions set forth herein.

2. DEFINITIONS

Unless otherwise specifically provided, and in addition to the other defined terms set forth herein, the following terms will have the meanings set forth below:

"Affiliates" means any JCI company or entity that has Johnson Controls International plc as its ultimate parent company, as well as any entity or joint venture in which JCI or a JCI Affiliate has any ownership. For avoidance of doubt, Johnson Controls International plc shall not be included in the definition of Affiliate for purposes of this Agreement. The liability of each Affiliate and JCI under this Agreement shall be several and not joint. Supplier shall bill each such JCI Affiliate separately for the Services it provides to such Affiliate. Each Affiliate shall only be liable for those obligations expressly set forth in the order for service to which it is a party. In no event will JCI be liable for any of the obligations or liabilities of any Affiliate pursuant to this Agreement.

"Agreement" means this Global Services Agreement, together with all schedules, exhibits, links, amendments, and other attachments hereto, all of which are incorporated into this Agreement by reference, as the same may be modified, amended, or supplemented from time to time.

"Confidential Information" means any information disclosed- regardless of the form of the disclosure- by or on behalf of the Discloser to the Recipient during the term of this Agreement, except information that Recipient can demonstrate:

(a) is or becomes generally available to the public other than as a result of disclosure by the Recipient;

(b) is already known by or in the possession of the Recipient at the time of disclosure by the Discloser as evidenced by written documentation in the Recipient's possession prior to receipt of the Confidential Information;

(c) is independently developed by the Recipient without use of or reference to the Confidential Information; or

(d) is obtained by the Recipient from a third party that has not breached any obligations of confidentiality.

JCI's Confidential Information includes, without limitation, JCI Data and Personal Data.

"Discloser" means the Party disclosing Confidential Information hereunder.

"Equipment" means any equipment, computer hardware, consumables, operating systems, software, firmware, and telecommunications, networking, routing, cabling, electrical or other infrastructure equipment that is owned, operated, or controlled by Supplier and used in connection with performance of the Services.

"Fees" means the agreed fees due to Supplier in consideration for the performance of the Services in accordance with the terms of an applicable SOW.

"Key Personnel" are those Supplier's employees identified on the SOW as necessary for Supplier's performance of its obligations hereunder. Supplier agrees not to reassign Key Personnel without the prior written consent of JCI, unless an individual leaves the employ of Supplier or becomes ill (in which event such individual's replacement will be subject to JCI's prior written approval). In any event, if Supplier makes any changes to its Key Personnel pursuant to this Agreement or SOW, then it shall provide thirty (30) days' prior written notice of the change, and Supplier shall replace such Key Personnel with minimal disruption to its performance of the Services hereunder and to JCI's overall business.

"Party" means JCI or Supplier individually, and collectively they are referred to herein as "Parties."

"Personnel" means Supplier's employees and, as and if permitted and approved by JCI pursuant to an applicable SOW, Supplier's subcontractors, agents, and representatives.

"Pricing Schedule" means the prices for Services set forth on Schedule A hereto.

"Project Manager" means those individuals designated as a "Project Manager" in an SOW.

"Recipient" means the Party receiving Confidential Information hereunder.

"Services" means any services to be performed and provided by Supplier on a non-exclusive basis under this Agreement and related SOW(s).

"SOW" means a transactional document (which may be entitled "Work Order", "Statement of Work" or the like, which in all cases shall be deemed an "SOW" for all purposes under this Agreement that is entered into pursuant to this Agreement by and between Supplier and JCI. Each SOW shall be substantially in the form of Schedule B hereof and shall automatically incorporate by reference the provisions of this Agreement as though such provisions were set forth therein in their entirety.

"JCI" means JCI and its Affiliates.

"JCI Networks" means collectively, computers, computer systems and networks of JCI.

3. SCOPE OF THE AGREEMENT

3.1 Scope of Services. Pursuant to the terms of this Agreement, and from time to time during the term of this Agreement, JCI may engage Supplier to perform Services. This Agreement sets forth the terms and conditions that will govern Supplier's performance of such Services to JCI. Such Services will be more fully described in an applicable SOW issued hereunder. Supplier acknowledges that until an applicable SOW and Purchase Order are issued by JCI, JCI is not required to order any Services hereunder by virtue of this Agreement alone.

3.2 Controlling Documents. In the event of a conflict between the terms and conditions of this Agreement and the terms and conditions of any mutually executed SOW, the terms and conditions of this Agreement will control. Any exceptions expressly agreed upon in writing by JCI and Supplier pursuant to a particular SOW will apply only for purposes of that SOW, and will not be deemed to in any way amend, modify, cancel, or waive the provisions of this Agreement or for any other SOW.

3.3 Issuance of SOW. In each instance when JCI desires to engage Supplier to perform Services, JCI and Supplier will develop and agree upon an SOW defining the Services to be provided by Supplier and such other details as the Parties deem appropriate, and Supplier will render Services in accordance with the schedule and standards described in the applicable SOWs and in this Agreement. Each SOW shall set forth: (i) a description of the Services or Deliverables to be furnished by Supplier and corresponding date by which each is to be completed; (ii) the Fees to be paid by JCI; (iii) the applicable acceptance criteria (if any); (iv) the name of the Project Manager for each Party; and, (v) such additional requirements as may be mutually agreed upon by the Parties thereto. Each SOW will be governed by the terms of this Agreement and will be binding upon the Parties and will be deemed to constitute a part of this Agreement as if fully set forth herein and all rights and obligations of the Parties will be deemed to apply to such SOW as if fully set forth therein.

3.4 Project Managers. In each SOW Supplier and JCI shall each designate a Project Manager who shall be the principal point of contact for all matters under the particular SOW. The Project Managers shall have the authority to represent each of their respective Parties and make any changes to an SOW pursuant to the procedures set forth herein. Supplier and JCI may each replace its Project Manager with a new Project Manager by providing written notice to the other Party in accordance with the notice provision contained herein.

3.5 Equipment Maintenance. Unless otherwise agreed to by the Parties in an SOW, Supplier will be responsible for obtaining and maintaining all Equipment required for Supplier to perform the Services at its sole cost and expense.

4. DELIVERABLES; OWNERSHIP

4.1 Deliverables. As part of the Services, Supplier shall deliver to JCI the deliverables set forth in an applicable SOW, as well as all reports, information, materials, and other work product that Supplier, its agents, employees, and/or subcontractors may develop that arise out of performance of the Services (collectively, the "Deliverables"). Except for previously developed ideas, concepts, know-how, knowledge, techniques, approaches, and methodologies proprietary to Supplier (or which Supplier licenses from third-parties), which do not encompass any Confidential Information or property information belonging to JCI (the "Supplier Methodologies"), JCI shall have title to, ownership of, and all proprietary rights in Supplier's work product related to the Services and the Deliverables, including all works-in-progress, all of which shall be considered "work made for hire," as defined by the copyright laws of the United States. Supplier agrees to assign and herewith assigns to JCI any and all work products and works-in-progress related to the Services and the Deliverables. At JCI's request, Supplier shall execute all documents as may be necessary to assign such rights to JCI, and to protect JCI's rights in the Services and Deliverables, and all works-in-progress. If any Deliverable which constitutes copyrightable subject matter is not deemed to be a "work made for hire", then the Supplier shall, and hereby does, grant to JCI an exclusive perpetual, irrevocable, royalty free, transferable, world-wide license to use such

Deliverable in any manner and in every medium, whether now known or hereafter devised, for any purpose and to create derivative works thereof.

4.2 Moral Rights Waiver. Supplier hereby waives, and shall procure the waiver of each of its employees and agents of, any and all of moral rights arising under any federal or state law of the United States or any law of any other country, region or subdivision thereof in and to the Deliverables related to the Services, and any contribution thereto, and hereby agrees that JCI shall have all rights flowing from this waiver including, without limitation, the right to modify the Deliverables for any and all past, present or future uses now known or hereinafter discovered and Supplier agrees to execute all further documentation, if any, necessary to implement or reflect this waiver.

4.3 Supplier Methodologies License. In the event any Supplier Methodologies are incorporated into or are used in connection with the Deliverables, then Supplier hereby grants to JCI a worldwide, non-exclusive, royalty-free, perpetual, irrevocable right to access, use and reproduce any such Supplier Methodologies in connection with the Deliverables and such product.

5. REPORTS; CHANGES; ACCEPTANCE

5.1 Reports. Pursuant to each SOW, Supplier shall provide the JCI's Affiliate that issued the SOW with a report of Supplier's progress under such SOW no less often than once per week. In addition, Supplier acknowledges that JCI uses a standard form to measure and to track savings with its Suppliers, attached hereto as Schedule D. Accordingly, Supplier agrees that it shall complete the contents of such form no later than ten (10) business days of each calendar month during the Initial or any Renewal Term of this Agreement.

5.2 Changes. JCI may, upon reasonable notice to Supplier in writing, request changes to the Services provided pursuant to a particular SOW by notifying Supplier of the requested change, including such details as will allow Supplier to evaluate it. If JCI requests a change to the Services, Supplier shall promptly notify JCI, in writing, if Supplier believes that an adjustment in the Fees to be paid to Supplier with respect to the applicable SOW or an adjustment to the applicable project schedule is required in order to accommodate such change. If Supplier believes that a change in applicable Fees or project schedule is required, Supplier shall submit to JCI a reasonably detailed proposal, including but not limited to, an itemized budget reflecting all Fees and expenses for the requested change. If the Parties agree on such change and any resulting changes to the Fees to be paid to Supplier or the applicable project schedule, the Parties shall amend the SOW to reflect such change or otherwise document in writing Supplier's agreement to make such change.

5.3 Acceptance Evaluation. INTENTIONALLY DELETED

5.4 Third Party Intellectual Property. If Supplier intends to develop a Deliverable in a manner that requires JCI to use any software or other intellectual property of a third party ("Third Party Materials") in order to use such Deliverable, then Supplier will: (i) provide JCI with prior written notice, specifying in reasonable detail the nature of the Deliverable's dependency on the Third Party Materials, and (ii) arrange for JCI to obtain (for no additional cost or on such terms as may be acceptable to JCI) a perpetual, irrevocable, fully paid up, royalty-free, non-exclusive right and license to use the Third Party Materials in connection with JCI's use of the Deliverable.

5.5 Training. If a Deliverable requires JCI's personnel to be trained in order to properly use the Deliverable, Supplier will provide on-site training in the use of such Deliverable for all users designated by JCI, at a time or times reasonably agreeable to both Parties. All initial training by Supplier in the proper use of a Deliverable shall be at no additional charge, unless a fee for such training is specified in a SOW.

6. SUPPLIER STAFF.

6.1 Supplier Employees. Supplier shall at all times remain the employer of all of its employees (and remain liable for its Personnel) performing the Services, and Supplier shall perform all of the responsibilities of an employer under applicable federal, state, and local laws and regulations. Supplier shall be responsible for: (a) selecting and hiring its employees legally, including compliance with all applicable laws in connection therewith; (b) assuming full responsibility for the actions of its Personnel while performing Services; (c) the supervision, direction and control of its Personnel performing Services; (d) paying its employees' wages and other benefits that Supplier offers to such employees in accordance with applicable laws; (e) paying or withholding all required payroll taxes and mandated insurance premiums; (f) providing worker's compensation coverage for employees as required by law; (g) fulfilling the employer's obligations with respect to unemployment compensation; and (h) compliance with any and all applicable laws and regulations regarding health, safety and environmental matters. Supplier shall cause each of its Personnel performing services for JCI hereunder to sign the Acknowledgement Form shown in Schedule C, which shall be kept on file for each of Supplier's Personnel. Supplier shall indemnify JCI from a claim made by any Supplier employee against JCI alleging rights or benefits as a JCI employee.

6.2 Conduct of Supplier Personnel. Whenever present at JCI premises, Supplier shall comply and shall cause its Personnel to comply with any and all applicable health, safety and environmental laws and regulations and JCI on-site policies and procedures and all reasonable instructions or directions issued by JCI, and otherwise conduct themselves in a businesslike manner. If JCI

shall request Supplier to remove any of its Personnel for any reason from the work hereunder (including, without limitation, lack of competence or conduct that interferes with JCI's operations), Supplier shall promptly cause such individual to be removed and replaced at no cost to JCI; provided, however, except as otherwise provided herein, Supplier retains the sole right to hire and fire its Personnel, and shall be solely responsible for oversight of its Personnel and any decision to fire its Personnel.

6.3 Subcontractors. Prior to subcontracting any of the Services, supplier shall notify JCI of the proposed subcontract and shall obtain JCI's written approval of such subcontract. In no event shall any subcontract release Supplier from its responsibility for its obligations under this Agreement and Supplier shall indemnify JCI to the extent provided for hereunder. Supplier shall be responsible for the work and activities of its employees, agents and subcontractors, including compliance with the terms of this Agreement. Supplier shall be responsible for all payment to its employees, agents and subcontractors. Supplier shall promptly pay for all services, material, equipment and labor used by Supplier in providing the Services and Supplier shall keep JCI's premises, and any deliverables from Supplier to JCI, free of all liens.

7. SECURITY REQUIREMENTS.

7.1 Supplier shall comply with the security requirements set forth in Schedule E.

8. PAYMENTS AND INVOICING.

8.1 Designated Fees. Supplier agrees to provide JCI with the pricing and discounts for applicable Fees in accordance with the Pricing Schedule. Subject to the terms and conditions herein and applicable law, all costs and expenses relating to the Services are included in the Fees and additional fees shall not be charged to or reimbursed by JCI. Unless different payment terms are stated in the Order, the applicable Country Supplement, or required by law, payment on undisputed invoices will be processed 120 days from the invoice posting date on the next scheduled payment run. Payment runs occur twice a month, around the 5th and 22nd of each month. Payment shall be in US dollars unless otherwise stated in a SOW. The making of any payment or payments by JCI, or on the behalf of any JCI Affiliate, as the case may be, shall not imply JCI's acceptance of such Services or the waiver of any warranties or requirements of, or rights to make any claims under, this Agreement. Supplier shall bring any claim for Supplier's improper invoicing of JCI within twelve (12) months of the date Supplier has furnished Services that are the subject of the invoice, otherwise, the Supplier will have been deemed to have waived any and all rights that it has to such claims. JCI may withhold payment pending receipt of evidence, in the form and detail requested by JCI, of the absence of any liens, encumbrances, or claims on Deliverables provided under the Order. Payment will be made in the currency expressly stated in the Order; if no such currency is noted, payment will be made in U.S. Dollars.

8.2 Additional Expenses. If and to the extent expressly agreed to by the Parties in an SOW, JCI shall reimburse Supplier for reasonable and documented travel-related expenses actually incurred and required by the performance of Services consistent with JCI's **TRAVEL REIMBURSEMENT GUIDELINES FOR JOHNSON CONTROLS SUPPLIERS** incorporated by this reference and available for download here: **JCI Travel Guidelines**. Travel time shall not be considered as time spent providing Services hereunder and is therefore not billable hereunder. Except as expressly provided in an SOW, JCI will not be responsible for any fees or costs of ordinary commuting, premium or first-class travel, cancellations, commitment or signing fees, overhead or other administrative charges.

8.3 Set-Off; Credits. With respect to any amount that (a) should be reimbursed to JCI or (b) is otherwise payable to JCI pursuant to this Agreement, JCI may deduct the entire amount owed to it against the Fees or against the expenses owed by JCI to Supplier under this Agreement. Any unused credits against future payments owed to JCI shall be paid to JCI within thirty (30) days after the termination or expiration of this Agreement.

8.4 Taxes. JCI will be responsible for applicable sales, use, excise and similar taxes imposed on JCI's consumption of the Services. Any taxes for which JCI is responsible must be listed as separate line items on Supplier's invoice. Once such taxes have been paid by JCI, no additional tax assessments, applicable penalties, interest or late charges billed to Supplier will be paid for any such too low invoiced taxes. In addition, if Supplier fails to provide JCI with timely notice of any tax audit that could result in an increase in the amount of sales or use taxes assessed hereunder, then JCI shall not be required to pay any additional taxes assessed as a result of such audit. Supplier shall be solely responsible and liable for the payment of any and all taxes imposed on its provision of the Services, all taxes relating to Supplier's Personnel, and all taxes based on the net income or gross revenues of Supplier.

8.5 Audit Rights. Supplier shall, at its sole cost and expense, maintain complete and accurate books and records, specifically including, without limitation, the originals or copies of documents supporting entries in Supplier's books of account, such as time and payroll registers and related third party invoices, covering all activities and transactions arising out of or relating to this Agreement. During any Initial or Renewal Term of this Agreement, and for a period of three (3) years following the termination hereof for any reason, JCI, its duly authorized representatives, and any regulatory entity having jurisdiction over JCI, shall have the right upon forty-eight (48) hours prior notice and during normal business hours to examine and copy (at no cost to JCI) such books and records, and all other documents and materials in the possession of or under the control of Supplier, with respect to the subject matter and terms of this Agreement that, in JCI's reasonable judgment, have a bearing on or pertain to matters, rights,

duties, or obligations covered by this Agreement, including without limitation the right to verify Supplier's overhead costs and rates. In addition, JCI, its authorized representatives and any regulatory entity having jurisdiction over JCI shall: (a) have access to Supplier facilities; (b) be permitted to interview current or former employees of Supplier with respect to matters pertinent to Supplier's performance of this Agreement; (c) have access to all necessary records; and (d) be furnished, without charge, adequate and appropriate workspace to perform the examinations provided for in this Section. Any other cost associated with an on-site audit shall be borne by JCI. If the results of an audit reveal that the Supplier has overcharged JCI, whether intentionally or inadvertently, then JCI shall be entitled to a refund in the amount of the overcharge, plus ten percent (10%) of the overcharge. Supplier shall reimburse JCI for the reasonable costs of the audit in the event of any overcharge that is found that exceeds ten percent (10%) of the actual amounts that JCI owes Supplier. JCI's exercise of any right to audit at any time(s) or its acceptance of any statement or the payment thereof by JCI shall be without prejudice to any of JCI's right or remedies that it might have at law or in equity and shall not bar JCI from thereafter disputing the accuracy of any payment or statement. Supplier shall remain fully liable for any amounts found to be due under this Agreement without consideration of any payments made under this Section.

8.6 Benchmarking. After the first anniversary of the Effective Date, JCI shall have the right but not the obligation, at its own cost and expense, and no more frequently than once during any twelve (12) month period, to obtain the services of an independent third party reasonably acceptable to Supplier and subject to confidentiality obligations no less restrictive than those found in this Agreement, to benchmark the services (including performance, service levels, and charges) against other Suppliers performing similar services under similar terms and conditions to ensure that JCI is obtaining competitive pricing and levels of service. Should such benchmarking result in an indication that JCI is paying more than market competitive pricing and/or receiving less than competitive service levels, Supplier has 30 days to provide alternate benchmarking that substantiates Supplier's competitive pricing and levels of service or to adjust pricing and levels of service to JCI's benchmark. If after such 30-day period Supplier has neither provided such alternative benchmarking nor adjusted pricing and/or levels of service in accordance with the benchmark, JCI may either terminate the agreement with Supplier or continue to require Supplier to perform under the existing Agreement. Should JCI terminate this agreement under this provision, the termination will be handled as a termination for cause under this Agreement.

9. SUPPLIER'S REPRESENTATIONS AND WARRANTIES

9.1 Supplier represents and warrants that:

(a) Supplier shall perform the Services hereunder in a professional and efficient manner, using due care, skill, diligence and at a level equivalent to industry best standards and practices;

(b) Supplier is not a party to any agreement that would prohibit Supplier from entering into this Agreement or fully performing the Services hereunder;

(c) Supplier has full right, title and authority to perform the Services and provide JCI the rights to the Deliverables granted hereunder, and that the Deliverables are free of liens, encumbrances, claims or security interests of any kind;

(d) there is no outstanding, or threatened, litigation, arbitrated matter or other dispute, including strikes and lockouts, to which Supplier is a party that would reasonably be expected to have a material adverse effect Supplier's ability to fulfill its obligations under this Agreement;

(e) the Services performed will be fit for the business purposes of JCI as described in this Agreement or an applicable SOW;

(f) the Services and/or Deliverables shall not impair or violate any copyright, trademark, patent, trade secret or the intellectual property or other rights of any third-party;

(g) JCI shall have no obligation to pay any third party any fees, royalties or other payments for JCI's use of any third party materials imbedded within the Deliverables;

(h) Supplier shall perform the Services hereunder in compliance with all applicable federal, state, county, and municipal statutes, laws, regulations, codes, ordinances and orders ("Laws"), and specifically, those Laws related to the protection of the Personal Information of JCI's customers and employees, including but not limited to, protected health information, Personally Identifiable Information ("Personally Identifiable Information" is any information which can be used to identify, contact, or locate a single person), consumer report information, and any processed data incorporating such information (collectively, "Personal Information"), and Supplier shall obtain all applicable permits and licenses required in connection with its obligations under this Agreement;

(i) the Deliverables will be free of any and all (i)"time bombs," time-out or deactivation functions or other means designed to terminate the operation of the Supplier (other than at the direction of the user); (ii)"back doors" or other means whereby Supplier or any other party may remotely access and/or control JCI's Networks without JCI's express authorization; (iii) any functions whereby the Deliverable transmits data to any destination not specified by JCI; (iv) copy prevention mechanisms; (v) functions or routines that will surreptitiously delete or corrupt data in such a manner as to interfere with the normal operation of the Deliverables; or (vi) computer viruses; and

(j) except as set forth on Schedule F, the Deliverables: (i) do not contain any software, program, module, code, library, database, driver or similar component (or portion thereof) that is royalty free, proprietary software, the use of which requires any contractual obligations by the use such as, without limitation, that software that is subject to, distributed, transmitted, licensed or otherwise made available under any of the following licenses: GNU General Public License, GNU Library or "Lesser" Public License, Berkeley Software Design (BSD) license (including Free BSD and BSD-style licenses), MIT license, Mozilla Public Licenses, IBM Public License, Apache Software License, Artistic License (e.g., PERL), Sun Industry Standards Source License, Sun Community Source License (SCSL), Intel Open Source License, Apple Public Source License, or any substantially similar license, or any license that has been approved by the Open Source Initiative, Free Software Foundation or similar group (collectively, "Open Source Software"), and (ii) do not require the use of any Open Source Software in order to function in its intended fashion.

EXCEPT FOR THE WARRANTIES GIVEN BY SUPPLIER IN THIS AGREEMENT, SUPPLIER MAKES NO OTHER WARRANTIES, EXPRESS OR IMPLIED.

10. **CONFIDENTIALITY**

10.1 Confidential Information.

(a) The Recipient shall use the Confidential Information only for the purpose of meeting its obligations or exercising its rights under this Agreement, and shall not, without limitation, use the Confidential Information to: (i) compete directly or indirectly with the Discloser; or (ii) interfere with any actual or proposed business of the Discloser.

(b) The Recipient shall not disclose or otherwise make available any of the Confidential Information to anyone, including employees, contractors and representatives, except those employees, contractors and representatives of the Recipient and entities controlled by, controlling or under common control with the Recipient who (1) need to know the Confidential Information for the purpose of meeting Recipient's obligations or exercising its rights under this Agreement, and (2) are bound by obligations of non-use and non-disclosure substantially similar to those set forth herein. The Recipient shall be responsible for any use or disclosure of the Confidential Information by such employees, contractors, representatives or commonly controlled entities.

(c) The Recipient shall use its best efforts (but in any event not less than those employed for safeguarding its own proprietary information) to keep the Confidential Information and/or any knowledge which may be imparted through examination thereof or working therewith confidential.

10.2 Compelled Disclosure. The Recipient may disclose the Confidential Information to the extent that such disclosure is required by law or court order, provided that the Recipient shall promptly provide to the Discloser written notice prior to such disclosure and shall provide reasonable assistance in obtaining an order or other remedy protecting the Confidential Information from public disclosure at the Disclosing Party's sole cost and expense.

10.3 Return of Confidential Information. Each Party shall, upon termination or expiration of this Agreement or applicable SOW, or at any time upon demand by the other Party, promptly return to the other Party any and all Confidential Information together with any copies or reproductions thereof and destroy all related data in its computer and other electronic files. Upon the return, or destruction, of Confidential Information the Recipient will erase all copies of the Discloser's Confidential Information from all forms of magnetic and electronic media using a method that ensures that it cannot be recovered; provided, however, that each Party may keep one (1) copy of the Confidential Information with its legal counsel for archive purposes.

10.4 Injunctive Relief. Each Party acknowledges that disclosure of the other Party's Confidential Information by it or breach of the provisions contained herein may give rise to irreparable injury to the other Party and such breach or disclosure may be inadequately compensable in money damages. Accordingly, each Party may seek injunctive relief against the breach or threatened breach of the foregoing undertakings. Such remedy will not be deemed to be the exclusive remedy for any such breach but will be in addition to all other remedies available at law or in equity.

10.5 Insider Trading. JCI's Confidential Information may constitute material inside information under the securities laws of the United States, and use of this information to trade in the securities of JCI's parent Johnson Controls International plc or sharing the information with others who trade in the securities of JCI's parent is a violation of this Agreement and may be a violation of law.

11. **INDEMNIFICATION**

11.1 Indemnity. Supplier shall defend, indemnify and hold harmless JCI, its parents, Affiliates, , and each of their respective directors, officers, employees, and shareholders (the "JCI Indemnified Parties"), from and against any and all suits, claims, actions, liabilities, losses, damages, costs and expenses (including, but not limited to, interest, penalties, reasonable attorneys' fees and other expenses of litigation) and causes of action of whatsoever kind (collectively referred to as "Claims") which may be incurred by, asserted against, or recoverable from any JCI Indemnified Party arising out of or relating to any of the following:

(a) damage to, destruction of, or loss of property (including a JCI Network as defined in Schedule E) or the injury to or death of any person arising out of or in connection with Supplier's or its Personnel's performance of its obligations hereunder;

(b) the negligent or wrongful acts or omissions of Supplier or its Personnel;

(c) any claim made by a third party based upon infringement or misappropriation of any intellectual property right, other proprietary right or contractual right in connection with the Deliverables, Services, or any other resources or items provided by Supplier under this Agreement (the "Supplier Provided Resources"), or

(d) any defect of imperfection in design, material, or workmanship of any Supplier Provided Resources provided to JCI hereunder.

11.2 Infringement Remedy.

(a) If, as a result of any such claim, Supplier is enjoined from providing the Supplier Provided Resources to JCI, or JCI is enjoined from using the Supplier Provided Resources, or in Supplier's opinion either of the foregoing is likely to occur, Supplier, at its sole cost and expense, shall promptly take one or more of the following actions:

(i) modify the Supplier Provided Resources, as the case may be, so that it is no longer infringing (provided its functionality is not impaired);

(ii) replace the Supplier Provided Resources with functionally equivalent applications or services; or

(iii) obtain the right for Supplier to continue providing the Supplier Provided Resources to JCI, or the right for JCI to continue using the Supplier Provided Resources.

(b) If Supplier, using its best efforts, cannot remedy the situation within a reasonable period of time (such time not to exceed under any circumstance 20 (twenty) days), then at JCI's election and request, Supplier shall promptly reimburse JCI for all Fees paid pursuant to the SOW pertaining to such infringing Deliverables or Services. Notwithstanding any such reimbursement, replacement or modification, Supplier's obligations to defend and indemnify JCI shall not be diminished or eliminated.

11.3 Indemnification Procedure. The JCI Indemnified Parties shall have the right at their discretion and sole cost to be represented by their own counsel and to participate in the defense of any action in which a JCI Indemnified Party is named as a party defendant, and the JCI Indemnified Parties' prior written approval will be required for any settlement that reasonably can be expected to require a material affirmative obligation of or result in any ongoing material liability to a JCI Indemnified Party. In addition, in the event a Claim involves software, including but not limited to software containing Open Source Software, Supplier shall provide JCI with all necessary assistance in addressing such Claim, including but not limited to promptly providing JCI (or a JCI designee) with access to the source code for such software and/or related information for the purpose of assessing and remediating such Claim.

12. INSURANCE

12.1 Required Insurance. Prior to commencement of this Agreement, Supplier shall procure, and for the Term of this Agreement shall maintain in full force and effect during the Term, at its sole cost and expense, insurance in accordance with the terms and conditions in Schedule H, attached hereto and incorporated by reference, and will otherwise fully comply with such terms and conditions.

12.2 Excess Liability. The insurance coverage's and limits specified herein shall not be construed in any way as limits of liability or as constituting acceptance by JCI of responsibility for losses in excess of insurance coverages or limits. No acceptance and/or approval of any insurance by JCI shall be construed as relieving or excusing the Supplier from any liability or obligation imposed by the provisions of the Agreement.

13. LIMITATION OF LIABILITY

(a) NEITHER SUPPLIER NOR ANY JCI COMPANY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING IN CONNECTION WITH THIS AGREEMENT, WHETHER IN AN ACTION IN CONTRACT, TORT, STRICT LIABILITY OR NEGLIGENCE, OR OTHER ACTIONS, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, EXCEPT SUCH LIMITATION SHALL NOT APPLY TO ANY CLAIMS ARISING FROM SUPPLIER'S VIOLATION OF LAW, BREACH OF ITS CONFIDENTIALITY OBLIGATIONS OR DATA SECURITY REQUIREMENTS, DEFENSE AND INDEMNITY OBLIGATIONS, WILLFUL MISCONDUCT OR NEGLIGENCE.

(b) NEITHER SUPPLIER'S NOR JCI'S TOTAL LIABILITY TO THE OTHER PARTY FOR DIRECT DAMAGES SHALL EXCEED THE TOTAL AMOUNT PAID OR PAYABLE BY JCI (IN THE AGGREGATE) FOR THE PERFORMANCE OF THE SERVICES UNDER THE SOW GIVING RISE TO THE DAMAGES. THIS DIRECT DAMAGES LIMITATION ON LIABILITY SHALL NOT APPLY TO (A) AMOUNTS PAYABLE IN RESPECT OF INDEMNIFICATION CLAIMS, (B) DAMAGES ARISING FROM OR RELATING TO (I) BREACHES OF THE CONFIDENTIALITY SECTIONS OF THIS AGREEMENT; (II) A PARTY'S

WILLFUL MISCONDUCT, NEGLIGENCE OR VIOLATION OF LAW; OR (III) SUPPLIER'S FAILURE TO COMPLY WITH JCI'S SECURITY REQUIREMENTS AS SET FORTH IN THIS AGREEMENT.

14. TERM & TERMINATION

14.1 Term; Renewal. This Agreement will become effective on the Effective Date and will continue in full force and effect for the longer of (a) twelve months; or (b) the expiration or termination of all SOWs issued hereunder (the "Initial Term") unless earlier terminated in accordance with this Agreement. Upon expiration of the Initial Term, this Agreement will automatically renew on the same terms for successive one (1) year periods (each a "Renewal Term" together with the Initial Term, the "Term") unless and until: (a) this Agreement is terminated in accordance with its terms; or (b) JCI gives Supplier notice of its intention not to renew this Agreement prior to any anniversary date of this Agreement or pursuant to a SOW; provided, however, that this Agreement and all SOWs hereunder shall terminate five (5) years from the Effective Date of this Agreement unless the Parties mutually agree to extend the Agreement and/or any applicable SOWs in writing.

14.2 Termination for Convenience. Notwithstanding anything to the contrary in this Agreement or any SOW, JCI may terminate this Agreement, or any applicable SOW, in whole or in part for convenience and without cause and without further liability or penalty at any time by providing written notice to Supplier.

14.3 Termination for Cause. If either Party defaults in the performance of, or fails to perform, any of its material obligations under this Agreement, including any or all SOWs, and such default is not remedied within thirty (30) days of the receipt of written notice from the non-defaulting Party, then the non-defaulting Party shall have the right to terminate this Agreement, either in whole or in part, by providing written notice of such termination to the other Party and may avail itself of any and all rights and remedies to which it may be entitled at law, in equity or under this Agreement.

14.4 Termination for Insolvency. Either Party may terminate this Agreement, including all SOWs, if any one of the following events occurs: (a) the other files a voluntary petition in bankruptcy or an involuntary petition is filed against it; (b) the other is adjudged bankrupt; (c) a court assumes jurisdiction of the assets of the other under a federal reorganization act, or other statute; (d) a trustee or receiver is appointed by a court for all or a substantial portion of the assets of the other; (e) the other becomes insolvent, suspends business or ceases to conduct its business in the ordinary course; or (f) the other makes an assignment of its assets for the benefit of its creditors. Each Party will give prompt written notice of any such event relating to it.

14.5 Framework Agreement. The Parties acknowledge that this Agreement is a global framework agreement pursuant to which a number of SOWs may be issued. Accordingly, for the avoidance of doubt and except as otherwise provided for hereunder, termination of the Agreement shall not automatically result in the termination of any SOW, each SOW being terminable in accordance with its own provisions; provided, however, that the terms and conditions of this Agreement shall continue to govern any remaining SOW until the work under that SOW has been either been completed or the SOW is otherwise terminated in accordance with its terms, if applicable. If the SOW is silent in regard to termination, then either Party may avail itself of the termination rights under this Agreement for that particular SOW.

14.6 Effect of Termination. After receipt of a notice of termination, and except as directed by JCI, Supplier shall immediately: (i) stop work as directed in the notice; (ii) place no further subcontracts or orders for materials, services, or facilities, except as necessary to complete the continued portion of the Agreement or SOW, if any; (iii) terminate all subcontracts to the extent they relate to Services terminated; and (iv) deliver to JCI all works and Deliverables completed through the termination date, as well as all works-in-progress. After termination, Supplier shall submit a final termination settlement to JCI for all work performed up to termination of this Agreement. Following such termination JCI shall have no further liability to Supplier, other than for valid charges incurred for conforming Services provided through the effective date of termination. If JCI's notice of termination specifies that such termination will be effective on a date subsequent to the date of such termination notice, Supplier shall continue to perform the Services during said notice period if requested by JCI.

15. DISPUTE RESOLUTION

15.1 Dispute Discussion. In the event of a dispute between the Parties arising out of this Agreement, and as a condition precedent to any right of action, representatives of each Party shall meet (either in person or by telephone), within ten (10) days after receipt of a notice from either Party specifying the nature of the dispute, to review a Party's claims for the basis of such dispute and attempt to resolve in good faith all such claims. Thereafter, if the Parties are unable to resolve the dispute within such time period, the matter shall be escalated to a Vice President (or a more senior officer) of each Party, who will meet, either in person or by telephone, within fifteen (15) days of such escalation. If the dispute remains unresolved after such escalation, then the Parties may proceed with all remedies available at law or in equity. Notwithstanding the foregoing, in the event of a threatened, actual or claimed breach of the Confidential Information or intellectual property provisions hereunder, either Party may by-pass the provisions of this dispute discussion provision and immediately seek relief in a court of competent jurisdiction to stay any threatened or continued breach of the foregoing.

15.2 Continuity of Services. Supplier acknowledges that the timely and complete performance of its obligations pursuant to this Agreement is critical to the business and operations of JCI. Accordingly, in the event of a dispute between JCI and Supplier, Supplier shall not interrupt the performance of its obligations under this Agreement, disable any equipment used in providing the Services, or perform any action that prevents, slows down, or reduces in any way the performance of the Services or JCI's ability to conduct its business during the resolution of such dispute unless and until this Agreement expires or is terminated in accordance with the provisions hereof.

16. M&A ACTIVITY

16.1 Divestiture. Should JCI, from time to time, sell, transfer or otherwise divest (whether by way of spin-offs, restructurings, reorganizations or otherwise) itself of the equity ownership, or substantially or a majority of all of its assets, or any division, or business unit (all jointly hereafter referred to as "Divested Unit"), and as part of such transfer JCI agrees to provide transitional services to the Divested Unit following the divestiture of the Divested Unit, including the continued receipt of the Services by such Divested Unit, then JCI shall have the right to do so for the remainder of the Term of this Agreement after the completion of any such transfer with no additional payment to Supplier, except for those Fees set forth in this Agreement or an applicable SOW. Additionally, if a Divested Unit is a party to a previously issued SOW, then Supplier agrees to continue to allow the Divested Unit to continue to obtain Services pursuant to the terms of the SOW for the remainder of its term, provided that such Divested Unit continues to pay any applicable Fees due for such Services.

16.2 Acquisitions. In the event that JCI acquires a business entity ("Acquired Business") that receives services from Supplier pursuant to an existing agreement, then at JCI's option, the Acquired Business's agreement with Supplier may be cancelled (without penalty) and any further services performed for the Acquired Business shall be performed in accordance with this Agreement.

17. COMPLIANCE PROVISIONS

17.1 The Parties to the Agreement agree to comply with all the provisions contained in the COMPLIANCE CLAUSES FOR SUPPLIERS incorporated by this reference and available for download here Compliance Clauses for Suppliers ("Compliance Provisions"). .:The Compliance Provisions shall apply to the Agreement and any Schedule, Exhibit or SOW.

17.2 Data Protection. Supplier represents and warrants that its processing, storage, and transmission of Personal Data complies with all applicable privacy and data protection laws, all other applicable regulations and directives, and the terms of this Agreement. Supplier agrees that it will not sell Personal Information; retain, disclose, or use Personal Information for any purpose other than providing the Services and any Deliverables under an SOW to JCI; or retain or use Personal Data outside of its direct business relationship with JCI. Upon expiration or termination of this Agreement, Supplier will delete from its records any Personal Data in its possession and shall comply with the requirements for protecting Personal Data set forth in Schedule G.

18. GENERAL PROVISIONS

18.1 Notices. All notices required or permitted under this Agreement will be in writing and will be deemed received when (a) delivered personally; (b) three days after having been sent by registered or certified mail; or (c) one day after deposit with a recognized commercial express courier specifying next day delivery. All communications will be sent to the persons and addresses identified below or to such other address as may be designated in a SOW or by a Party by giving written notice to the other Party pursuant to this paragraph.

If to JCI:

Johnson Controls, Inc.
5757 North Green Bay Avenue
Milwaukee, Wisconsin 53209

Attn: _____

With a copy that shall not constitute notice to:
Johnson Controls, Inc.
507 E. Michigan Street
Milwaukee, WI 53202

Attn: Procurement Counsel

If to Supplier:

_____
_____
_____
Attn: _____

With a copy that shall not constitute notice to:

_____
_____
_____
Attn: _____

18.2 Rights in Bankruptcy. All rights and licenses granted under or pursuant to this Agreement by Supplier to JCI are, and will otherwise be deemed to be, for purposes of Section 365(n) of the United States Bankruptcy Code, or replacement provision therefore (the "Code"), licenses to rights to "intellectual property" as defined in the Code. The Parties agree that JCI, as licensee

of such rights under this Agreement, will retain and may fully exercise all of its rights and elections under the Code. The Parties further agree that, in the event of the commencement of bankruptcy proceedings by or against Supplier under the Code, JCI will be entitled to retain all of its rights under this Agreement.

18.3 Intentionally Left Blank.

18.4 Amendment; Waiver. This Agreement may be amended, and the observance of any term may be waived, only with the written consent of both Parties. Any waiver by either Party hereto of any provision of this Agreement will not be construed as a waiver of any other provision of this Agreement, nor will such waiver be construed as a waiver of such provision with respect to any other event or circumstance, whether past, present or future.

18.5 No Publicity. Supplier shall not, without the prior written consent of JCI, in any manner disclose, advertise or publish the fact that Supplier has furnished or contracted to furnish to JCI the Services described in this Agreement or any SOW, and Supplier shall not use the name, trade name or trademarks of JCI in any manner in any of its advertising or marketing literature, customer lists, web sites, press releases or any other document or communication (in electronic or paper form).

18.6 Assignment. Supplier acknowledges that JCI may assign this Agreement to any Affiliate, without the consent of Supplier. Supplier hereby acknowledges that the Services to be provided to JCI hereunder are unique and personal. Accordingly, Supplier shall not assign this Agreement in whole or in part, or any rights hereunder without the prior written consent of JCI, which consent may be withheld for any reason at JCI's sole discretion. Any attempted assignment without such written consent shall be null and void. The provisions of this Agreement shall be binding upon and inure to the benefit of the respective successors and permitted assigns of each Party.

18.7 Relationship of Parties. This Agreement shall not be construed as creating any agency, partnership, joint venture, or other similar legal relationship between the Parties; nor will either Party hold itself out as an agent, partner, or joint venture party of the other Party. Both Parties shall be, and shall act as, independent contractors. Neither Party shall have authority to create any obligation for the other Party, except to the extent stated herein.

18.8 Section Headings. The headings of the sections, paragraphs, and appendices herein are for the Parties' convenient reference only and will not define or limit any of the terms or provisions hereof.

18.9 Counterparts and Electronic Signatures. This Agreement may be executed in multiple counterparts each of which shall be deemed an original but all of which together shall constitute one and the same Agreement. The counterparts of this Agreement and all other documents executed in connection herewith may be executed and delivered by facsimile or other electronic signature method or process, including but not limited to Docusign, by any of the parties to any other party and the receiving party may rely on the receipt of such document so executed and delivered by facsimile or other electronic means as if the original had been received.

18.10 Severability. If any provision or provisions of this Agreement will, for any reason, be deemed unenforceable or in violation of law, such unenforceability or violation will not affect the remaining provisions of this Agreement, which will continue in full force and effect and be binding upon the parties hereto.

18.11 Governing Law and Jurisdiction. Supplier agrees that any and all disputes, claims or litigation arising from or related in any way to this Agreement shall be resolved exclusively by the courts in the State of Wisconsin. Supplier waives any objections against and agrees to submit to the personal jurisdiction of the state and federal courts in Milwaukee County, Wisconsin. Supplier waives any objections or defenses it may have based upon an inconvenient forum. This Agreement will be governed by and construed in accordance with the laws of the State of Wisconsin, without regard to its conflict of law provisions.

18.12 Time is of the Essence. TIME IS OF THE ESSENCE IN SUPPLIER'S PERFORMANCE OF ITS OBLIGATIONS HEREUNDER. Supplier shall promptly notify JCI in the event Supplier, for any reason, anticipates difficulty in complying with the required schedule or in meeting any of JCI's requirements.

18.13 Mutual Negotiation. The Parties agree that the terms and conditions of this Agreement are the result of negotiations between the Parties and that this Agreement will not be construed in favor of or against any Party by reason of the extent to which any Party or its professional advisors participated in the preparation of this Agreement.

18.14 Cumulative Rights & Remedies. Any enumeration of a Party's rights and remedies set forth in this Agreement is not intended to be exhaustive. A Party's exercise of any right or remedy under this Agreement does not preclude the exercise of any other right or remedy. All of a Party's rights and remedies are cumulative and are in addition to any other right or remedy set forth in this Agreement, any other agreement between the parties, or which may now or subsequently exist at law or in equity, by statute or otherwise.

18.15 No Exclusivity. The Parties agree that this Agreement is not exclusive and that JCI has the right at its discretion at any time to engage other parties to perform services of a similar nature as the Services performed by Supplier.

18.16 Force Majeure. Neither Party shall be held responsible for delay nor default cause by fire, riot, act of nature, terrorist acts or other of political sabotage, or war where such cause was beyond, respectively, that Party's reasonable control. Such Party shall, however, make all reasonable efforts to remove or eliminate such as cause for delay or default and shall, upon cessation of the cause, diligently pursue performance of its obligations under the Agreement or an applicable SOW. If any Force Majeure event exceeds a thirty (30) day period, both Parties may terminate the Agreement or an applicable SOW with notice to the other.

18.17 Minority & Women-owned Business Enterprises (US Only). Supplier acknowledges that diversity among the suppliers from whom JCI purchases goods and services is important to JCI. As such, Supplier will make good faith efforts to purchase seven percent (7%) of purchased goods and services provided under this Agreement or in regard to any purchases that Supplier makes as part of its overall business from Minority-owned Business Enterprises ("MBE") and three percent (3%) from Woman-owned Business Enterprises ("WBE"). For the purposes of this provision, an MBE is a business that is owned and controlled by racial and/or ethnic minorities including but not limited to: African Americans; Hispanic Americans; Native Americans; Asian Pacific Americans; Asian Indian Americans. A WBE is a business that is owned and controlled by a woman or women. Supplier has agreed to make good faith efforts to use such MBE's and WBE's in connection with this Agreement. Supplier agrees to provide diversity spend performance to JCI on a quarterly basis. Supplier may be asked to participate in outreach efforts such as conferences and trade shows.

18.18 Survivability. Each term and provision of this Agreement that would by its very nature or terms survive any termination or expiration of this Agreement shall survive any termination or expiration of this Agreement, regardless of the cause thereof.

18.19 Entire Agreement. This Agreement, together with all of its Schedules and SOWs constitutes the entire agreement between Supplier and JCI relating to the subject matter hereof and supersedes all other such prior or contemporaneous oral and written agreements and understandings. Notwithstanding the foregoing, neither JCI nor Supplier shall be relieved of any of its respective obligations with respect to any information subject to the terms of any confidentiality agreement entered into by JCI and Supplier prior to the Effective Date. No shrink-wrap, click-wrap, browse-wrap or other terms and conditions or agreements ("Additional Terms") provided with any products or software hereunder will be binding on JCI, even if use of such products or software requires an affirmative "acceptance" of those Additional Terms before access is permitted. All such Additional Terms will be of no force or effect and will be deemed rejected by JCI in their entirety. Either party may scan, fax, email, image, or otherwise convert this Agreement into an electronic format of any type or form, now known or developed in the future. Any unaltered or unadulterated copy of this Agreement produced from such an electronic format will be legally binding upon the parties and equivalent to the original for all purposes, including litigation.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement as of the Effective Date first above written.

JOHNSON CONTROLS, INC.	**SUPPLIER**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

SCHEDULES

Schedule A – Pricing Schedule
Schedule B - Form of Statement of Work
Schedule C – Contractor Acknowledgment Form
Schedule D – Supplier Reporting Template
Schedule E - Security Requirements
Schedule F – Open Source Software
Schedule G – Personal Data Processing Terms
Schedule H – Insurance

SCHEDULE A

PRICING SCHEDULE

SCHEDULE B

FORM OF STATEMENT OF WORK

THIS SOW is entered as of _____, by and between Supplier and the JCI entity designated below. The Parties hereto acknowledge that they are entering into this SOW pursuant to the provisions of the Global Services Agreement dated as of _____, between Supplier and JCI _____. The Parties further acknowledge and agree that the provisions of the Global Services Agreement shall apply to this SOW as though such provisions were set forth herein in their entirety.

Party:	SUPPLIER	JCI ENTITY
Name:		
Address:		
State of Incorporation:		

Project Name:

Commencement Date: **Completion Date:**

Project Managers: **For Supplier** **For JCI**

Address:

Phone:

e-mail:

Description of Services To Be Performed (Add attachment if needed.):

Description of Deliverables (Add attachment if needed.):

Deliverable Milestones (Add attachment if needed.):

_____ DATE: _____

_____ DATE: _____

_____ DATE: _____

ARE PAYMENTS TIED TO MILESTONES IN LIEU OF TIME OR SOME OTHER METHOD OF PAYMENT? IF "YES", EXPLAIN IN THE BOX BELOW.

Acceptance Criteria (Attach Specifications and other criteria if applicable.)

If Acceptance Criteria are not specified, the Services or Deliverables shall not be deemed to have been accepted until JCI has notified Supplier that the Services or Deliverables are satisfactory to JCI in all respects.

Basis for Determining Fee

Firm Fixed Rate:

Time and Material Rates:

Estimated Total Expenses

Estimated Total Cost

The total cost shown above may not be exceeded without the prior written approval of JCI. Unless the fee basis is a firm fixed price, JCI is under no obligation to spend any minimum amount.

Billing Address:

Key Supplier Personnel:

Name or Role	Skill Level	Service Locations

IN WITNESS WHEREOF, the Parties hereto, through their duly authorized officers, have executed this SOW to the Global Services Agreement as of the date first above written.

Supplier:		**JCI:**	
By:		By:	
Name:		Name:	
Title:		Title:	
Date:		Date:	

SCHEDULE C

ACKNOWLEDGMENT FORM FOR SUPPLIERS/INDEPENDENT CONTRACTORS

PLEASE READ THIS ACKNOWLEDGMENT FORM CAREFULLY BEFORE SIGNING BELOW.

I acknowledge that I am not an employee of Johnson Controls or any of its Affiliates (individually and collectively, the "Company") but have the following status (please check appropriate box):

_____ I am an Employee of

_____
(Please print name of Supplier with whom employed/engaged).

_____ I am a Supplier/Independent Contractor to

_____
(Please print name of Supplier with whom employed/engaged).

_____ I am a self-employed Supplier/Independent Contractor.

I understand that because I am not an employee of Company, Company is not responsible for paying my salary and withholding appropriate taxes, paying social security, workers' compensation, state disability, and unemployment or for providing any benefits on my behalf or on behalf of my spouse or dependents, including those that may be legally required. Such obligations are the responsibility of the agency/consulting firm by which I am employed. If I am self-employed, I understand that these are my own obligations.

I also expressly acknowledge and agree that because I am not an employee of the Company, I am not entitled or eligible to participate in any of the Company's employee benefits programs (nor are my spouse or any dependents), and I hereby waive all rights to such benefits, including any right to file a claim for any employee benefits under the Employee Retirement Income Security Act, applicable state or local law, or under any Company policy, practice, procedure, or program.

I hereby consent to (a) Supplier's disclosure of my personal information to Company, and (b) Company's receipt and use of such personal information as necessary in support of the terms conditions and obligations of the Agreement between Company and Supplier. I acknowledge and agree that Company may share all such information with its parents, subsidiaries, affiliates and its/their successor corporations or any subcontractor or assignee, within and outside the country in which I reside and am located and thereby subject such information to the laws of such countries.

I further acknowledge receipt of Johnson Controls Acceptable Use Policy available for download at: **Link to Acceptable Use Policy** and agree to comply with its terms.

I agree to comply with all applicable Company policies, procedures, rules, and regulations.

_____ _____
(Please Print Name) Date

_____
Signature

_____ _____
Witness: Date

SCHEDULE D

SUPPLIER REPORTING TEMPLATE

SCHEDULE E

SECURITY REQUIREMENTS

1. Protection of Company Data & Personal Information

1.1 "Company Data" means all Confidential Information whether entered in a Statement of Work, project specifications, documentation, software or equipment by or on behalf of Company, its Affiliates, Company and/or its customers and information derived from such information, including as stored in or processed through diagnostic tools, hardware, firmware or software.

1.2 "Personal Information" means any personally identifiable information included in any Confidential Information that may be used to directly or indirectly identify or contact any person, including without limitation, any Company employees, customers or prospective customers and their personnel. Personal Information includes the sub-category "Personal Sensitive Information" ("PSI"). PSI is the following information that requires additional control and protection: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, credit cards, debit cards, bank account numbers, social security numbers, social insurance numbers, passwords, security challenge information, driver's license numbers, unique biometric data and Personal Identification Codes ("PIC"). PSI also includes Personal Health Information ("PHI") and Non-Public Personal Information ("NPPI") and similarly restricted information, as such terms are defined under any applicable privacy law of the United States, any other country or any political subdivision thereof, if applicable, including by not limited to the Health Information Portability and Privacy Act, if applicable (collectively, the "Privacy Laws") and any other information that Company may identify in writing as PSI.

1.3 Ownership and Treatment of Company Data.

1.3.1 Access to any Company Data or any Company Networks (as hereinafter defined) shall be (a) subject to compliance with all applicable Company policies and procedures, (b) limited solely to such Company Data as is required to accomplish the Purpose, and (c) access may be restricted or revoked by Company in its sole discretion at any time without notice. Supplier will not grant access to Company Networks to any third party or use any third party computer systems to access Company Networks or Company Data without first obtaining Company's written consent.

1.3.2 Company Data will be and remain, as between the parties, the property of Company. Supplier will not modify, reformat, reorganize or delete Company Data in any manner without the express written consent of Company and only in the manner permitted in writing by Company. Supplier will not possess or assert any lien or other right against or to Company Data. No Company Data, or any part thereof, will be commercially exploited by or on behalf of Supplier. Company shall own and retain all right, title and interest, including all intellectual property rights, in and to all Company Data and any information submitted to the applications by its users that is not otherwise Supplier's confidential information. Supplier acknowledges and agrees that notwithstanding any reformatting, modification, reorganization or adaptation of the Company Data (in whole or in part) during its incorporation, storage or processing, or the creation of derivative works from the Company Data, the Company Data will remain as such and will be subject to the terms and conditions of this Agreement. This Agreement does not grant to Supplier any license or other rights, express or implied, in the Company Data, except as expressly set forth in this Agreement..

1.3.3 Supplier will notify Company within twenty-four hours of any unauthorized modifications, deletions, reorganizations, reformatting or losses of data and use its best efforts, as directed by Company, to correct any errors occurring in any Company Data and restore any such modifications, deletions, reorganizations, reformats or losses of any Company Data to the extent that such errors or losses are caused by Supplier.

1.3.4 Protection of Company Data & Personal Information. Supplier shall manage Company Data and Personal Information in its control subject to the requirements of Schedule 1 below, Supplier Information Security Requirements, as amended by Company upon written notice to Supplier from time to time.

1.3.5 Supplier and its Personnel will not attempt to access, or allow access to, any Company Data or Personal Information which they are not permitted to access under this Agreement or the Service Agreement. If such access is attained, Supplier will follow the reporting process described in this Agreement.

1.3.6 Unless Company's Vice President, CIO, or their delegate of authority approves in writing, in no event will Supplier store any Company Data on any server or other equipment located outside of the United States or Canada or allow access to any to Company Data from outside of the United States or Canada.

1.3.7 Supplier is expressly prohibited from using any Personal Information obtained under this Agreement or the Service Agreement, to contact or market to any person, including any employees, customers or prospects of Company through any means and/or for any other purpose. Supplier agrees that such Personal Information will not be given to any third party for any use whatsoever.

1.4 Additional Data Privacy for PSI. Without limiting any prohibitions regarding the treatment of Personal Information, at all times during and after the Term of this Agreement, Supplier shall use, handle, collect, maintain, and safeguard all PSI in accordance with a Privacy Policy reasonably acceptable to Company and consistent with the requirements articulated in this Agreement and with all applicable Canadian and United States federal, provincial, and state consumer privacy laws, regulations and rules

(collectively, "Privacy Rules") which may be in effect during the Term of this Agreement as it concerns the subject matter of this Agreement. Supplier further acknowledges that it alone is responsible for understanding and complying with its obligations under the Privacy Rules. If the PSI includes any credit card information Supplier shall be responsible for complying with all applicable information security practices promulgated by the applicable federal, provincial, state, and municipal laws, regulations, and statutes pertaining to the acquisition, handling, and disposition of all such credit card information, and also by industry associations, including, but not limited to, the applicable standards of the Payment Card Industry ("PCI") Data Security Standard.

1.5 NOT USED.

1.6 Security Requirements.

1.6.1 Supplier shall not use its own computer systems to store Confidential Information or access Company Networks without prior written consent from Company. If Company grants permission for Supplier to use its own computer systems to store Confidential Information or access Company Networks or Confidential Information, such use and storage shall be subject to such conditions as required by Company. Without limiting the generality of the foregoing, if Supplier uses its own computer systems to store Confidential Information or access Company Networks, Supplier shall implement minimum security measures as specified herein, and specifically as set forth in Schedule 1, The Supplier Information Security Requirements, to protect Supplier's computer systems, networks and databases, and the data processed, transmitted or stored thereon (including, without limitation, Company Data and Personal Information) against the risk of penetration by, or exposure to, a third party via any system or feature utilized by Supplier in storing or accessing Company Data. Unless otherwise specified in the security requirements set forth herein, such protections will include, but not be limited to: (a) protecting against intrusions, including but not limited to intrusions of operating systems or software, (b) encrypting Confidential Information, and (c) securing the computer systems and network devices.

1.6.2 Supplier shall employ the highest industry standard of encryption mechanisms as is customary in the industry to protect Confidential Information which is transmitted over any wireless connection or across any untrusted connection (including, but not limited to, the public Internet). Without limiting the generality of the foregoing, Supplier shall ensure that (a) all transmissions of Company Data and Personal Information between the applications and an authorized user are transmitted using HTTPS and 128-bit or higher Secure Sockets Layer encryption, (b) all Personal Sensitive Information, including back-up copies thereof, stored by Supplier at Supplier's data center are encrypted using 128-bit or higher encryption, and (c) any Company Data and Personal Information, including backup copies thereof, that are removed from Supplier's facility or stored off-site are encrypted using 128-bit or higher encryption. In addition, Supplier must process and store Personal Sensitive Information on equipment dedicated solely to processing Personal Sensitive Information and must keep Personal Sensitive Information physically separate from other customers' information.

1.6.3 Supplier shall notify Company, through Company's designated contact and any other designated security escalation channel within twenty-four hours, if Supplier knows of, or has reasonable belief of, a breach of security of a Supplier system or database that contains Personal Information or any other Confidential Information, or the knowledge or reasonable belief of actual loss or theft of any such data, or access by any unauthorized party to such data, and will cooperate, work with Company and provide necessary information concerning such breach sufficient for Company to evaluate the likely consequences and any legal or regulatory requirements arising out of the event unless the sharing of such data is prohibited by law. Supplier shall use its best efforts to immediately terminate any security breaches or suspicious activity. Supplier shall not allow any security breach or suspicious activity to persist for any amount of time or for any reason except as required by law, or as deemed reasonably necessary by Supplier to determine the identity of the perpetrator and to stop such breach or suspicious activity. If any breach of the security, confidentiality, or privacy of the Company Data or Personal Information requires notification by Company to any party under any of the Privacy Laws, Company shall have sole control over the timing, content, and method of such notification and Supplier shall reimburse Company for its out-of-pocket costs in providing the notification.

1.7 Occurrence Reports. Within twenty-four (24) hours following Supplier's discovery of the occurrence of a security breach or suspicious activity, Supplier shall provide Company with written documentation of the cause, remedial steps and future plans to prevent a recurrence of the same or similar breach or suspicious activity. If such remedial plan is acceptable to Company, Supplier shall immediately implement the proposed remedial plan or in a mutually agreed upon timeframe. If such remedial plan is unacceptable, based on Company's reasonable judgment, Supplier shall promptly but in any event no later than five (5) days enter into good faith negotiations to address the proposed remedial plan. Supplier shall reasonably cooperate with Company security investigation activities and with the preparation and transmittal of any notice or any action, which Company in its sole discretion may deem appropriate or required by law, to be sent or done for customers or other affected third parties regarding any known or suspected security breach.

1.8 NOT USED.

1.9 Company Networks.

1.9.1 "Company Network" means any computers, computer systems and networks of Company and Company customers. If access to Company Networks is required by Supplier, then Company shall determine the nature and extent of such access. If remote access to Company's Networks is given to Supplier, then any and all information relating to such remote access shall be considered Company's Confidential Information. In addition, any and all access to Company Networks shall be subject to the following:

(a) Company's Networks will be used by Supplier solely for the Purpose;

(b) Access to Company Networks will be restricted to Supplier's Personnel who need access in order for Supplier to fulfill its obligations under this Agreement and the Service Agreement; and no access rights will be transferred to any other individuals without the prior written consent of Company; and

(c) Supplier shall use commercially reasonable efforts to ensure that its Personnel do not attempt to break any security systems related to the Company Networks, or attempt to obtain access to any programs or data beyond the scope of the access granted, in writing, by Company.

1.9.2 Without limiting any of its other rights, Company shall have the right to restrict and monitor the use of the Company Network, and to access, seize, copy and disclose any information, data or files developed, processed, transmitted, displayed, reproduced or otherwise accessed on Company Networks. Company may exercise its rights reserved hereunder: (a) to ensure compliance by Supplier's Personnel with Company's policies and procedures while on Company Networks; (b) to work with Supplier to investigate conduct that may be illegal or may adversely affect Company; and (c) to prevent inappropriate or excessive personal use of Company Networks. Supplier will advise its Personnel concerning the rights stated hereunder

2. Company Security Requirements. Supplier shall adhere to the Security Requirements described in Schedule 1 hereto.

3. Required Background Checks. Following is a list of specific background checks that must be performed and documented prior to permitting Supplier Personnel to have access to Confidential Information. Supplier is responsible for obtaining and maintaining documentation substantiating that all items listed have been performed. Audits may be performed by Company upon reasonable notice to Supplier and during normal business hours.

TYPE OF CHECK
Social Security Number Verification (Includes Trace)
Criminal Search - Minimum 7 years (County Criminal; residence, school, & employment) – all counties provided or developed
US Department of Treasury's Office of Foreign Assets Control (OFAC) Specially Designated National or a Blocked Persons
Employment Verification - last 3 employers or past 7 years whichever comes first
Education Verification (highest level obtained post high school)
Professional License or Certificate Verification (if appropriate)

COMPANY DATA ACCESS AGREEMENT
Schedule E - 1
INFORMATION SECURITY REQUIREMENTS

The following items are considered Company's minimum security requirements. This Schedule E-1 is not meant to be a comprehensive list of security requirements. Supplier. These requirements apply to Supplier operations as well as any third-party that may provide services on behalf of Supplier.

1.0 Definitions.
1.1 "Company Production Data" means Confidential Information that resides in a production environment. Data that is masked and in Development and/or Test environments is not included.
1.2 "Data Masking" means the process of modifying records to conceal Company Production Data, especially when such records are copied from a Company production environment.
1.3 "Information Processing System(s)" means the individual and collective electronic, mechanical, or software components of Supplier operations that store and/or process Confidential Information.
1.4 "Information Security Event" is defined as any situation where it is suspected or confirmed that Confidential Information is lost; is subject to unauthorized or inappropriate access, use, or misuse; the security, confidentiality, or integrity of the information is compromised; or the availability of Supplier Information Processing Systems is compromised by external attack.
1.5 "Provider" means any third party with access to Confidential Information by, through or under Supplier including sub-contractors of whatever tier.

1.6 "Security Breach" is defined as an unauthorized access to Supplier's facilities or Information Processing Systems or networks used to service, store, or access Confidential Information.
2.0 Security and Confidentiality. Before receiving, or continuing to receive, Company Data or Confidential Information, Supplier will and will require any of its Providers with access to Confidential Information, Company Networks, or Company Data to implement and maintain an information security program that ensures that: (a) Confidential Information and Supplier's Information Processing Systems are protected from internal and external security threats; and (b) Confidential Information is protected from unauthorized access and disclosure. Supplier will request consent from Company prior to processing and/or storing Company Production Data, or refreshing such data, in a development or test environment.
3.0 Security Policy.
3.1 Formal Security Policy. Consistent with the requirement of this Schedule E-1, Supplier will create and provide to Company an information security policy that is approved by Supplier's management, published and communicated to all Supplier Personnel and relevant Providers.
3.2 Security Policy Review. Supplier will review the information security policy at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
4.0 Organizational Security.
4.1 Provider Access. Prior to allowing Providers to access Confidential Information, Supplier will require Providers to agree in writing to terms substantially similar to the confidentiality provisions of this Agreement to maintain the confidentiality of Confidential Information
4.1.2 In addition, prior to allowing Providers to access Company Data, including Supplier Information Processing Systems or media containing Company Data, Supplier will:
(a) Submit a written request for the access to Company and receive consent for the access; and
(b) Identify and mitigate risks to Company Data from this access.
4.1 Subsequent Party Access.
4.1.1 Supplier will include as part of its contracts with Providers having access to Confidential Information provisions requiring such Providers to meet or exceed the confidentiality obligations of this Agreement.
4.1.2 In addition, Supplier will include as part of their contracts with Providers having access to Company Data substantially similar security requirements as contained in this document and make this a requirement for all subsequent parties receiving Company Confidential Information.
5 Asset Management.
5.1 Asset Inventory. Supplier will maintain an inventory of all Supplier Information Processing Systems and media containing Confidential Information.
5.2 Acceptable Use. Supplier will implement rules for the acceptable use of information and assets which is no less restrictive than industry best practice and consistent with the requirements of this exhibit.
5.3 Equipment Use While on Company Premises. While on Company's premises, Supplier will not connect hardware (physically or via a wireless connection) to Company Networks unless necessary for Supplier to perform services under this Agreement or the Service Agreement. Company has the right to inspect or scan such hardware before or during use.

5.4 Portable Devices. The following restrictions apply to storing Confidential Information on portable devices:

(a) Company Data may not be stored on any portable device, including but not limited to, laptops, Personal Digital Assistants, mobile devices, MP3 devices, and USB devices, except as authorized by Company;

(b) Company Data containing any Personal Information or any information concerning any third party may not be stored on portable devices including, but not limited to, laptops, Personal Digital Assistants, mobile devices, MP3 devices, and USB devices unless approved by Company and the Company Data on the devices is encrypted and secured from unauthorized access; and

(c) All other Confidential Information may not be stored on portable devices including, but not limited to, laptops, Personal Digital Assistants, and MP3 devices unless the devices are password protected to secure them from unauthorized access.

5.5 Personally-owned Equipment. Confidential Information may not be stored on personally owned equipment not controlled by Supplier.

5.6 Protection of Data at Rest. Supplier shall use and employ a high standard of data protection mechanisms as is customary in the industry to protect Company Data as defined in this Agreement.

5.6.1 All Company Personal Sensitive Information at rest, including back-up copies thereof, stored by Supplier at Supplier's data center are encrypted using 256-bit AES encryption, or encryption mechanisms providing equal or higher protection than 256-bit AES.

5.6.2 Any Company Data, including backup copies thereof, which are removed from Supplier's facility or stored off-site, are encrypted using 256-bit AES or encryption mechanisms providing equal or higher protection than 256-bit AES.

Supplier must process and store Company Data on computer server hardware dedicated solely to processing Company Data and must keep Company's Data on physically separate computer server hardware from non-Company information.

5.6.3 Any Confidential Information may not be stored within a file or database in the Demilitarized Zone ("DMZ").

5.6.4 All keys used for encryption must be handled in accordance with documented key management processes and procedures.

6 Human Resources Security.

6.1 Security Awareness Training. Prior to Supplier employees and Providers receiving access to Confidential Information, they will receive security awareness training appropriate to their job function. Supplier will also ensure that recurring security awareness training is performed.

6.2 Removal of Access Rights. The access rights of all Supplier Personnel and Provider users to Supplier Information Processing Systems or media containing Confidential Information will be removed rapidly, and always within twenty-four hours of termination of their employment, contract or agreement, or adjusted upon change.

6.3 Screening. Ensure that criminal background checks are conducted on all Supplier and Supplier Provider's Personnel prior to permitting access to Confidential Information or Company Networks in accordance with this Agreement, relevant laws, and regulations.

7 Physical and Environmental Security.

7.1 Secure Areas. Supplier will secure all areas, including loading docks, holding areas, telecommunications areas, cabling areas and off-site areas that contain Information Processing Systems or media containing Confidential Information by the use of appropriate security controls in order to ensure that only authorized personnel are allowed access and to prevent damage and interference. The following controls will be implemented:

(a) Access will be controlled and restricted by use of a defined security perimeter, appropriate security barriers, entry controls and authentication controls. A record of all accesses will be securely maintained;

(b) All personnel will be required to wear some form of visible identification to identify them as employees, Suppliers, visitors, et cetera;

(c) Visitors to secure areas will be supervised, or cleared for non-escorted accessed via an appropriate background check. Their date and time of entry and departure will be recorded; and

(d) Physically secure and maintain control over all paper and electronic media (e.g., computers, electronic media, paper receipts, paper reports, and faxes) that contain Company Data.

8 Communications and Operations Management.

8.1 Protections Against Malicious Code. Supplier will and will require its Providers to:

(a) Implement detection, prevention, and recovery controls to protect against malicious software (malware), which is no less than current industry best practice and train its Personnel on the prevention and detection of malicious software;

(b) Ensure anti-malware mechanisms are deployed on all systems commonly affected by malware (e.g. PC's and servers) and are capable of detecting, removing, and protecting against other forms of malicious software, including spyware and adware; and

(c) Ensure anti-malware mechanisms are current, actively running, and capable of generating audit logs.

8.2 Media Handling. Supplier will and will require its Providers to protect against unauthorized access or misuse of Confidential Information contained on media by use of a media control management program and provide a copy of the program to Company.

8.3 Media and Information Disposal. Supplier will and will require its Providers to securely and safely dispose of media

(including but not limited to hard copies, disks, CDs, DVDs, optical disks, USB devices, hard drives) containing Confidential Information when no longer required by the establishment of procedures, but in no event any longer than to include, but not be limited to:

(a) Disposing of media containing Confidential Information so that it is rendered unreadable or undecipherable, such as by burning, shredding, pulverizing or using techniques in compliance with DoD Standard 5220.22-M;

(b) Maintaining a secured disposal log that provides an audit trail of Confidential Information media disposal activities; and

(c) Providing proof to Company certifying that all Confidential Information was purged. The proof will be provided to Company within thirty (30) business days after the information was purged.

8.4 Exchange of Information. To protect confidentiality and integrity of Confidential Information and Company Data in transit, Supplier will and will require its Providers to:

(a) Perform an inventory, analysis and risk assessment of all data exchange channels (including but not limited to HTTP, HTTPS, SMTP, modem, and fax) to identify and mitigate risks to Confidential Information and Company Data from these channels;

(b) Monitor and inspect all data exchange channels to detect unauthorized information releases;

(c) Ensure that appropriate security controls using approved data exchange channels are employed when exchanging Confidential Information and Company Data;

(d) Employ industry standard enhanced security measures (at a minimum 128-bit AES encryption) to encrypt Confidential Information and Company Data transmitted via the Internet;

(e) Ensure Company PSI is not sent via e-mail; and

(f) Ensure that Confidential Information (including persistent cookies) or information about Company customers or employees is not harvested by Supplier and Provider web pages.

8.5 Monitoring. To protect against unauthorized access or misuse of Confidential Information residing on Supplier Information Processing Systems, Supplier will:

(a) Employ current industry best practice security controls and tools to monitor Information Processing Systems and log user activities, exceptions, unauthorized information processing activities, suspicious activities and information security events. Logging facilities and log information will be protected against tampering and unauthorized access. Logs will be kept for at least 90 days online.

(b) Perform frequent reviews of logs and take necessary actions to protect against unauthorized access or misuse of Confidential Information.

(c) At Company's request, make logs available to Company to assist in investigations to the extent that such log disclosures do not place the data or systems of other Supplier customers at risk or expose other Supplier customer confidential information.

(d) Comply with all relevant legal requirements applicable to monitoring and logging activities.

(e) Ensure that the clocks of all relevant information processing systems are synchronized using an authoritative national or international time source.

(f) Employ, monitor and keep up to date data loss prevention technology, network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises and losses.

8.6 Access Control.

8.6.1 User Access Management. To protect against unauthorized access or misuse of Confidential Information residing on Supplier Information Processing Systems, Supplier will:

(a) Employ a formal user registration and de-registration procedure for granting and revoking access and access rights to all Supplier Information Processing Systems;

(b) Employ a formal password management process; and

(c) Perform recurring reviews of users' access and access rights to ensure that they are appropriate for the users' role.

8.6.2 User Responsibilities. To protect against unauthorized access or misuse of Confidential Information residing on Supplier Information Processing Systems, Supplier will:

(a) Ensure access to systems and applications storing or transmitting Company Data or Confidential Information is limited to only those individuals whose job requires such access based on a need-to-know;

(b) Ensure that Supplier Information Processing Systems users follow industry standard security practices and in the selection and use of strong passwords;

(c) Ensure that unattended equipment has appropriate protection to prohibit access and use by unauthorized individuals;

(d) Ensure that Confidential Information contained at workstations, including but not limited to paper and on display screens is protected from unauthorized access.

8.7 Network Access Control. Access to internal, external, Provider and public network services that allow access to Supplier Information Processing Systems shall be controlled. Supplier will:

(a) Ensure that current industry best practice standard authentication mechanisms for network users and equipment are in place and updated as necessary;

(b) Ensure electronic perimeter controls are in place to protect Supplier Information Processing Systems from unauthorized access;

(c) Ensure a stateful firewall is in place for each Internet connection and between any DMZ and the Intranet. Firewalls shall be configured to deny all traffic except the traffic that is required for business reasons.

(d) Ensure authentication methods are used to control access by remote users;

(e) Ensure physical and logical access to diagnostic and configuration ports is controlled; and

(f) Ensure wireless implementations are only used if required for business reasons, put into practice WPA, WPA2, 802.11i or a superseding standard and must not use WEP.

8.8 Operating System Access Control. To protect against unauthorized access or misuse of Company Data or Confidential Information residing on Supplier Information Processing Systems, Supplier will:

(a) Ensure that access to operating systems is controlled by a secure log-on procedure;

(b) Ensure that Supplier Information Processing System users have a unique identifier (user ID);

(c) Ensure that the use of utility programs that are capable of overriding system and application controls are highly restricted and tightly controlled. Ensure that inactive sessions are shut down after a defined period of inactivity; and

(d) Employ restrictions on connection times to provide additional security for high risk applications.

8.9 Mobile Computing and Remote Working. To protect Confidential Information residing on Supplier Information Processing Systems from the risks inherent in mobile computing and remote working, Supplier will:

(a) Identify and mitigate risks to Confidential Information from mobile computing and remote working; and

(b) Develop policy and procedures for managing mobile computing and remote working.

9 Information Systems Acquisition, Development and Maintenance.

9.1 Security of System Files. To protect Supplier Information Processing Systems and system files containing Confidential Information, Supplier will ensure that access to source code is restricted to authorized users who have a direct need to know. Supplier will:

(a) Ensure that the integrity of files in the operating environment are maintained and monitored for approved change;

(b) Ensure that all systems and software have the latest vendor-supplied security patches;

(c) Establish a process to identify newly discovered security vulnerabilities and update system and application standards to address new vulnerability issues; and

(d) Ensure internal and external network vulnerability scans are conducted at least quarterly and network and application layer penetration testing at least once a year.

9.2 Security in Development and Support Processes. To protect Supplier Information Processing Systems and system files containing Confidential Information, Supplier will:

(a) Ensure that the implementation of changes is controlled by the use of formal change control procedures;

(b) Employ appropriate industry best practice security controls to minimize information leakage;

(c) Employ oversight quality controls and security management of software development; and

(d) Employ system, application and source code scanning and analysis tools and a framework for remediation of findings.

9.4.1 Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted system hardening standards as defined, for example, by SysAdmin Audit Network Security Institute (SANS), National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).

10 Information Security Incident Management.

10.1 Reporting Information Security Events and Weaknesses. To protect Supplier Information Processing Systems and system files containing Company Confidential Information, Supplier will:

(a) Implement a process to ensure that Information Security Events and Security Breaches are reported through appropriate management channels as soon as possible but in any event no later than eight hours after the occurrence of the event;

(b) Train all Personnel and require all Provider users of information systems and services how to report any observed or suspected Information Security Events and Security Breaches; and

(c) Notify / email Company at CO-NA-GIS-IncidentResponse-DG@JCI.com within twenty-four hours of all Information Security Breaches or suspected breaches. Following any such event or breach, Supplier will notify Company whether or not Confidential Information was compromised or released to unauthorized parties, the Confidential Information affected and the details of the event or breach.

11 Data Masking.

11.1 Applicability. This section details the technology security requirements for masking personally identifiable Company customer and employee data ("Company Production Data"). Data masking procedures employed by Supplier must meet or exceed the requirements established herein and apply them to:

(a) All activities performed within a Supplier's environment that uses Company Production Data; and

(b) Supplier Personnel, external business alliances or anyone using Company Production Data.

11.1.1 The requirement to mask Company Production Data applies to all Information Processing Systems outside of Company's Production Environments, including those of Supplier's Providers.

11.1.2 At Company's request, and in a format acceptable to Company, Supplier will provide information affirming that its data masking efforts meet the requirements of this Agreement.

11.2 When to Mask Company Data. Supplier will mask Company Production Data if the data is moved outside of Company's production environment (such as quality control, test and development environments). If a business need exists to use Company Production Data for non-production activities the Supplier will obtain written permission from Company. Masking may be accomplished as follows:

11.2.1 Supplier may develop its own tools to mask Company Production Data as long as the masking meets or exceeds the specifications contained herein.

NOTE – BECAUSE MASKED DATA RECORDS MAY STILL CONTAIN INFORMATION THAT IS CLASSIFIED AS CONFIDENTIAL INFORMATION OR PII (E.G. NAMES, CREDIT CARD NUMBERS, BANK ACCOUNT INFORMATION, SOCIAL SECURITY NUMBERS, PASSWORDS, BIRTH DATES, ETC.) THE MASKED DATA FILE MUST BE HANDLED AND PROTECTED ACCORDING TO THIS AGREEMENT AND APPLICABLE LAW.

11.3 Masking Requirements. The following fields require special handling including but not limited to masking.

(a) Names (includes any name field and UserID or account name);

(b) Addresses (includes any address field, property location, garage location, et cetera);

(c) Email Address (includes any Email address field);

(d) Phone Number (includes any Phone Number Field including Home Phone, Personal Phone, Business Phone, et cetera);

(e) Date of Birth;

(f) Driver's License Number;

(g) Social Security or Social insurance Number;

(h) Financial information (includes, Credit Card, Bank Account, FICO or Beacon score, or other sensitive financial information); and

(i) Passwords or security codes (e.g., application passwords, PIC, etc.)

11.4 Disposal of Masked Data. Supplier will remove masked records and excluded production data from non-production environments as soon as the non-production activities are complete. Company considers non-production activities to be complete when the production data is no longer required to re-accomplish the activity or produce documentation.

COMPANY DATA ACCESS AGREEMENT
Schedule E-2

GOVERNMENT SECURITY REQUIREMENTS

1. Supplier's Use of U.S. Resources

1.1 Use Permitted. Individuals performing services (physical or logical) or having unescorted access within the Company Space (defined below), will meet the following individual eligibility requirements for access to U.S. Government Controlled Unclassified Information or Technology[1], and Non-Controlled Unclassified Government Contract-related Information (collectively, "Sensitive Government Data"):

(a) Supplier will only use individuals who are resident citizens of the United States, and have an active U.S. Government Public Trust background investigation of NAC-I, which has been adjudicated and approved through the respective U.S. Government Central Adjudication Facility ("CAF") Authority (collectively, "U.S. Resources").

(b) Individuals, who do not meet the definition of a U.S. Resource, may have limited access to the Company Space provided that those individuals are escorted and under constant supervision by a U.S. Resource, and are effectively precluded from access to Sensitive Government Data. This requirement does not apply to Medical, Police, Fire or other emergency responders', when responding in an official capacity within the Company Space. When requested, these officials will be afforded access to all areas of the Company Space through key or access control. Company will be notified immediately, when these situations occur. Notwithstanding the foregoing, Supplier Personnel who are not U.S. Resources may access the Company Space via the Company-provided fail-over switch in any event in which life, health or safety is threatened as determined by Supplier in its reasonable discretion (an "Emergency Event"); provided that Supplier will notify Company promptly of any Emergency Event and following any Emergency Event, Supplier will make available to Company at the Service Location the Supplier Personnel who accessed the Company Space and will cause such Supplier Personnel to execute any non-disclosure agreement, in form and substance satisfactory to Supplier in its reasonable discretion, as may be required by Company. Unless otherwise agreed to in writing by Company, Supplier agrees to allow only those personnel who are eligible to work in the United States to have access to Company Space. All Supplier Personnel performing Services that requires access to Company Space will be fully qualified to perform the tasks assigned them. Supplier will provide Company with such information regarding proposed Supplier Personnel to be assigned to perform Services as Company may reasonably request, provided that Supplier shall not be required to provide any such information in violation of applicable Law. Company will have the right, in its reasonable discretion, to reject the assignment of any such Supplier Personnel, and upon such rejection Supplier will propose alternate personnel.

1.2 Company Space. Company Space means the Company worksite and the physical space where Company Networks and Company Data reside. For example, if backup data sits in a locked file cabinet, if a server resides in a closet, if a device resides in a server rack, if an application resides on a system; each of these are examples of "Company Space".

2. SUPPLIER'S USE OF CLEARED RESOURCES

2.1 Use Permitted. Individuals performing services (physical or logical) or having unescorted access within the Company Space, will meet the following individual eligibility requirements for access to U.S. Government Classified Information or Technology[2]: Supplier will only use individuals who are resident citizens of the United States, and have an active U.S. Government security clearance investigation of NACLC/SECRET, which can be verified through the Joint Personnel Adjudication System (collectively, "Cleared Resource"). Individuals who do not meet the definition of a Cleared Resource, and who are resident citizens of the United States, may have limited access to the Company Space provided that those individuals are escorted and under constant supervision by a Cleared Resource, and are effectively precluded from access to Classified Information or Technology. Resident Aliens ("Permanent Resident") and Non-Resident Aliens ("Visa Holder" or "Work Authorizations") will not perform services (whether physical or logical) and will not have access (whether escorted or unescorted), except as expressly agreed in writing in advance by Company and approved by the Company Corporate Facility Security Officer. This requirement does not apply to Medical, Police, Fire or other emergency responders', when responding in an official capacity within the Company Space. When requested, these officials will be afforded access to all areas of the Company Space through key or access control. Company will be notified immediately, when these situations occur. Notwithstanding the foregoing, Supplier Personnel who are not Cleared Resources may access the Company Space via the Company-provided fail over switch in any Emergency Event; provided that Supplier will notify Company within twenty-four hours of any Emergency Event and following any Emergency Event, Supplier will

[1] Controlled Unclassified Information or Technology, the export of which is controlled by the International Traffic in Arms Regulations ("ITAR") or the Export Administrative Regulations ("EAR"). The export of technical data, which is inherently military in nature, is controlled by the ITAR. The export of technical data, which has both military and commercial uses, is controlled by the EAR. Controlled Unclassified Information includes other forms information or technology that is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

[2] Any information or technology that has been determined pursuant to Executive Order 13526 (or any predecessor or successor thereof) to require protection against unauthorized disclosure and is so designated. The classifications TOP SECRET, SECRET, and CONFIDENTIAL are used to designate such information.

make available to Company at the Service Location the Supplier Personnel who accessed the Company Space and will cause such Supplier Personnel to execute any non-disclosure agreement, in form and substance satisfactory to Supplier in its reasonable discretion, as may be required by Company. Supplier agrees to use only those personnel who are eligible to work in the United States to have access to Company Space. All Supplier Personnel performing Services that requires access to Company Space will be fully qualified to perform the tasks assigned them. Supplier will provide Company with such information regarding proposed Supplier Personnel to be assigned to perform Services as Company may reasonably request, provided that Supplier shall not be required to provide any such information in violation of applicable Law. Company will have the right, in its reasonable discretion, to reject the assignment of any such Supplier Personnel, and upon such rejection Supplier will propose alternate personnel.

3. FEDERAL INFORMATION SECURITY MANAGEMENT ACT.

(a) Sensitive Government Data. If Supplier may have access to Sensitive Government Data, Company will provide in connection therewith any specific remote hands instructions, construction, maintenance, and administrative requirements necessary for the Company Space to be constructed and maintained, and remote hands tasks to be performed, in compliance with the Federal Information Security Management Act ("FISMA") with a SC Sensitive Government Data type = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, NOT APPLICABLE)}. Supplier will construct and maintain the Company Space in accordance with such construction and maintenance requirements.

(b) Classified Information or Technology. If Supplier may have access to Classified Information or Technology, Company will provide in connection therewith any specific remote hand instructions, construction, maintenance and administrative requirements necessary for the Company Space to be constructed and maintained, and remote hands tasks to be performed, in compliance with the National Industry Security Program Operating Manual (DoD 5220.22-M) and FISMA, with a SC Classified Information type = {(confidentiality, HIGH), (integrity, HIGH), (availability, MODERATE)}. Supplier will construct and maintain the Company Space in accordance with such construction and maintenance requirements.

(c) FISMA Certification and Accreditation. If specifically requested by Company, Supplier will complete and submit to Company an annual statement regarding Supplier's compliance with the FISMA Certification and Accreditation process, or provide written documentation demonstrating Supplier's FISMA Program is under the cognizant authority of FedRAMP.

4. EXPORT COMPLIANCE AND SECURITY CLASSIFICATIONS.

Supplier understands that certain Company Data may be subject to: (i) U.S. and other export control laws and regulations; or (ii) U.S. Defense Department ("DoD") procedures such as those governing release of "Controlled" or "Uncontrolled Technical Data", "Sensitive" but unclassified data, or U.S. Government classified data (as defined in any applicable regulation) to certain foreign nationals. The Parties agree not to transfer or otherwise export or re-export (and to cooperate to prevent such transfers of) any such Company Data except in compliance with applicable Laws. For Company Data, regulated transfers may include those made to foreign nationals in the United States or another country. The Parties will work together as needed to create policies and procedures, regarding the access to and transfer of such materials. Supplier agrees not to allow any access to any such identified Company Data by any personnel that Supplier employs who are on the U.S. Treasury Department's list of Specially Designated Nationals, on the U.S. Commerce Department's Denied Persons List, Entity List or Unverified List, or who are nationals of Cuba, Iran, Sudan, or Syria, or any other countries that may be added to the list of U.S. embargoed countries from time to time. Supplier agrees not to allow access by any personnel that Supplier employs that are not U.S. Resources to Company Data identified in advance by Company as subject to DoD restrictions, ITAR (Title 22 of the U.S. Code of Federal Regulations, Parts 120– 130, as amended), and the EAR (Title 15 of the U.S. Code of Federal Regulations, Subtitle B, Parts 730–774, as amended), or similar restrictions. The Parties acknowledge that Supplier is not registered as an Arms Manufacturer with the Directorate of Defense Trade Controls. Supplier and Company will cooperate to restrict access to any other Company Data to such U.S. Resources and personnel as may lawfully receive it without an export license unless and until any and all required licenses are obtained. Supplier agrees to abide by all applicable Laws in the performance of the Services, including those related to exports as defined in both the ITAR and EAR.

Company represents that software provided by Company and used as part of the Services contains no encryption or, to the extent that it contains encryption, the software is approved for export without a license. Supplier's acceptance of any order for Services for such software is contingent upon the issuance of any applicable export license required by the United States Government. Supplier is not liable for delays or failure to deliver a Service resulting from Company's failure to obtain such license. Company will be liable for any breaches of this paragraph by Company.

5. GOVERNMENT CLAUSES. AS SET FORTH BELOW, THIS AGREEMENT INCORPORATES CERTAIN U.S. FEDERAL GOVERNMENT PROVISIONS BY REFERENCE WITH THE SAME FORCE AND EFFECT AS IF THEY WERE GIVEN IN FULL TEXT. THE FAR, DFAR, AND DEAR MAY BE OBTAINED AT THE FOLLOWING GOVERNMENT WEB SITES: HTTP://WWW.ARNET.GOV/FAR/ FOR FAR; HTTP://WWW.ACQ.OSD.MIL/DPAP/DARS/INDEX.HTML FOR DFAR; AND HTTP://WWW.PR.DOE.GOV/DEAR.HTML FOR DEAR. WHENEVER NECESSARY TO MAKE THE CONTEXT OF THE U.S. FEDERAL GOVERNMENT CLAUSES SET FORTH BELOW APPLICABLE TO THE AGREEMENT, THE TERM "SUPPLIER" WILL MEAN SUPPLIER, THE TERM "CONTRACTING OFFICER" OR "COGNIZANT SECURITY OFFICE" WILL MEAN

COMPANY, THE TERM "CONTRACT" WILL MEAN THE AGREEMENT, AND THE TERM "SUBCONTRACT" WILL MEAN ANY LOWER-TIERED SUBCONTRACT ISSUED BY SUPPLIER. SUPPLIER WILL COMPLY WITH THE NATIONAL INDUSTRY SECURITY PROGRAM OPERATING MANUAL (DOD 5220.22-M) AND ANY REVISIONS TO THAT MANUAL. TO THE EXTENT THAT A SOW INDICATES THAT A CLAUSE SET FORTH BELOW IS TO BE INCORPORATED BY REFERENCE INTO THE AGREEMENT, SUCH CLAUSE IS HEREBY INCORPORATED BY REFERENCE INTO THE AGREEMENT:

- FAR 52-204-2 Security Requirements
- DFAR 252.204-7000 Disclosure of Information
- DFAR 252.223-7007 Safeguarding Sensitive Conventional Arms, Ammunition and Explosives
- DEAR 952-204-2 Security Requirements
- DEAR 952-204-75 Public Affairs
- E.O. 13556 Controlled Unclassified Information
- E.O. 13526 Classified National Security Information

SCHEDULE F

OPEN SOURCE SOFTWARE

[SUPPLIER TO PROVIDE LIST OF OPEN SOURCE SOFTWARE, IF LEFT BLANK, SUPPLIER REPRESENTS THAT ITS SOFTWARE DOES NOT CONTAIN ANY OPEN SOURCE CODE.]

SCHEDULE G

Personal Data Processing Terms (Rev.10-13-2021)

These Personal Data Processing Terms ("Terms") are entered in between on behalf of itself and its Affiliates ("JCI") and [INSERT NAME OF PROCESSOR] ("Processor"), together ("Parties").

Preamble.
These Terms set forth confidentiality, security, and privacy requirements with respect to Personal Data Processed by Processor as part of the provision by Processor of the Services described in the Global Services Agreement ("GSA"). In the event of any conflict between the provisions of these Terms, its Schedules, and the provisions set forth in the GSA, the provisions that are more protective of Personal Data shall prevail.

1. **Definitions.** For the purposes of these Terms:

"Affiliates" means all affiliated entities, including any parent, sister, daughter or subsidiary companies, of JCI or Processor. Any reference to Affiliates in these Terms shall also be deemed to include all Personnel of such Affiliates.

"Controller" means a natural or legal person that determines the purposes and means of Processing of Personal Data.

"Data Protection Rules" means the relevant national, federal, state and local laws and regulations that apply to the Processing of Personal Data, including but not limited to any applicable privacy and information security laws and regulations.

"Data Subject" means an identified or identifiable natural person who can be identified directly or indirectly, including by reference to an identification number or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity. A legal person may qualify as Data Subject under the Data Protection Rules of specific jurisdictions, in which case such legal person shall also be considered a Data Subject for the purposes of these Terms.

"Personal Data" means any information relating to a Data Subject.

"Process", "Processing" or "Processed" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Processor" means a natural or legal person that processes Personal Data on behalf of a controller.

"Personnel" means any employee, contractor, or agent.

"Schedule 1" and "Schedule 2" mean the Schedules to these Terms attached hereto and forming an integral part of these Terms.

"Security Incident" means any: (i) transfer or disclosure to or access by third parties or Processing in breach of these Terms or the Data Protection Rules; (ii) loss of, or unauthorized access to or disclosure of, Personal Data resulting from breach of the safeguards described at Section 6 of these Terms or from a failure to establish such safeguards; (iii) or any event directly or indirectly affecting the confidentiality, integrity, or authenticity of Personal Data that is or was Processed by Processor on behalf of JCI or in connection with the Services.

"Services" means the Services provided by Processor to JCI under the MSA.

"Sub-Processor" means any data processor engaged by Processor or by any other Sub-Processor that Processes Personal Data on behalf of JCI. Any reference to a Sub-Processor in these Terms shall also be deemed to include all Personnel of the Sub-Processor.

"Supervisory Authority" means a data protection authority or similar regulator as defined under Data Protection Rules.

2. **JCI's Authority.**
Processor shall only Process Personal Data for the business purpose of providing the Services and all such Processing shall be strictly in compliance with the requirements set out in these Terms and in compliance with JCI's instructions as issued from time to time.

3. **Processor Obligations**.
Processor shall, and Processor shall ensure that its Personnel, Affiliates and Sub-Processors shall, Process all Personal Data fairly and lawfully, respect the privacy of Data Subjects and comply with all Data Protection Rules. Processor shall also ensure that its Personnel, Affiliates and Sub-Processors shall have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Processor shall not (i) obtain any rights to any Personal Data by virtue of providing the Services, (ii) transfer or disclose any Personal Data (in part or in whole) to any third party, except as stipulated in these Terms, or (iii) Process or use any Personal Data for its own purposes or benefit. Processor shall notify JCI of any change in operations or legislation which is likely to have an adverse effect on its ability to comply with these Terms.

4. **International Transfers.**
4.1. General. All transfers of Personal Data shall be in compliance with the Data Protection Rules applying to JCI, or the JCI Affiliate which exports the Personal Data. Onward transfers of Personal Data by Processor shall be made in strict compliance with such Data Protection Rules. Processor shall provide to JCI at least ninety (90) days of advance written notice prior to transferring Personal Data outside the country where the relevant Data Subjects reside.
4.2. Transfers from EEA Countries and the UK. All transfers of Personal Data from: i) the European Economic Area or Switzerland, hereinafter referred to collectively as the "EEA"; or ii) from the United Kingdom ("UK"), to countries outside the EEA or UK must be in strict compliance with the Data Protection Rules applying to the JCI Affiliate located in the EEA or UK which exports the Personal Data. For this purpose, Processor and/or its Affiliates shall enter into the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 ("Model Contract") with JCI as needed to satisfy cross-border transfer obligations under applicable Data Protection Rules. In circumstances where the JCI affiliate is a controller and Processor is a processor with respect to Personal Data, Module Two of the Model Contract (for controller to processor transfers) shall apply, the terms of which are hereby incorporated by reference and subject to the terms of Schedule 1. In circumstances where the JCI affiliate has entered into a contract with a JCI customer and is processing Personal Data as a processor on behalf of said customer, Module Three of the Model Contract (for processor to processor transfers) shall apply to any transfers of Personal Data between the JCI affiliate and Processor, the terms of which are hereby incorporated by reference and subject to the terms of Schedule 1. The Annexes to the Model Contract shall be annexed to these Terms as Schedule 1. Where Personal Data is subject to the Data Protection Rules of the UK, Processor and/or its affiliates shall, in addition to the Model Contract, enter into the 'UK Addendum to the EU Commission Standard Contractual Clauses' ("UK Addendum"). The UK Addendum shall be annexed to these Terms as Schedule 2. A Model Contract may not be necessary in case the Personal Data is transferred to a country that has been identified by the European Commission or the UK Government as providing adequate protection to Personal Data or to a Processor and/or its Affiliates offering protection to Personal Data under applicable Binding Corporate Rules.
4.3. Onward Transfers. Onwards transfers of Personal Data by Processor shall be made in strict compliance with Data Protection Rules and – if applicable - the annexed Model Contract at Schedule 1 . Where onwards transfers are subject to the Model Contract incorporated by reference in accordance with Section 4.2 of these Terms, the Processor shall ensure that the Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 (Module Three for processor to processor transfers) are incorporated into the contract with the Sub-Processor before the onwards transfer takes place.

5. Third Parties and Sub-Processors.
Processor may subcontract work that relates to Personal Data under these Terms only in accordance with JCI's instructions. Processor represents that it shall provide a list of all relevant Sub-Processors (i) prior to starting Processing, (ii) at a later date when Processor uses a new Sub-Processor, and (iii) at any time upon JCI's request. This list should also include all geographic locations where Processing may take place. JCI may object to the use of a new Sub-Processor in writing if the new Sub-Processor represents an unacceptable risk to the protection of the Personal Data as determined by JCI. All Sub-Processors must comply with applicable Data Protection Rules and must be bound by an agreement that is substantially similar to these Terms, including but not limited to substantially the same provisions on international transfers, confidentiality and information security, cooperation and enquiries, Security Incidents and breach notification, and inspection and audit rights. JCI shall be granted the same rights granted in these Terms vis-à-vis the Sub-Processor. The Sub-Processing agreement shall be provided to JCI promptly upon request. Processor shall remain liable for all acts or omissions of Sub-Processors with respect to the Personal Data.

6. **Confidentiality and Information Security**.
Processor shall keep Personal Data strictly confidential and represents that it has implemented adequate physical, technical and organizational measures, which are reasonable based upon the sensitivity of the Personal Data and/or necessary to secure the

Personal Data and to prevent unauthorized access, disclosure, alteration or loss of the same in light of the relevant risks presented by the Processing. In particular, such measures shall include, but shall not be limited to:

- Preventing access by unauthorized persons to Processing facilities and systems, where Personal Data is Processed or used (physical access control).

- Preventing unauthorized use of Processing systems (admission control).

- Ensuring that those persons authorized to use a Processing system are only able to access Personal Data within the scope of their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization during Processing or use and after recording (virtual access control).

- Ensuring that, during electronic transfer, transportation or when being saved to data carriers, Personal Data cannot be read, copied, modified or deleted without authorization, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged (transmission control).

- Ensuring that it is possible to check and ascertain whether and by whom Personal Data has been accessed, modified or deleted from Processing systems (input control), and ensuring that such access, modification and deletion of Personal Data is, in fact, monitored for any unusual or suspicious activities.

- Ensuring that Personal Data Processed under these Terms can only be Processed in accordance with the instructions issued by JCI (assignment control).

- Ensuring that Personal Data is protected against accidental malfunctions or loss (availability control).

- Ensuring that Personal Data collected for different purposes can be Processed separately (separation control).

- Maintaining a process for regularly testing, assessing and evaluating the effectiveness of physical, technical and organizational measures to ensure the security of the Processing.

- Ensuring that Processor has developed and implemented appropriate privacy and data protection policies and procedures, and that all Personnel who are involved in Processing the Personal Data have been appropriately trained to Process the Personal Data in accordance with such policies and procedures as well as in accordance with these Terms and applicable Data Protection Rules.

- Ensuring that disposal of Personal Data is accordance with Section 10 of these Terms is implemented in a secure manner.

At the request of JCI, Processor shall provide the former with a comprehensive and up-to-date confidentiality and information security concept relating to the Processing of Personal Data under these Terms. In the event that JCI requires Processor to amend any confidentiality and information security measures, Processor shall cooperate with JCI to implement such measures as soon as practicable.

- Processor shall ensure that its Personnel, Affiliates' Personnel and Sub-Processors' Personnel are subject to legally binding confidentiality and information security obligations that meet or exceed the requirements set forth in these Terms and that survive the termination of their employment.

7. **Cooperation and Enquiries**.

The Parties shall co-operate with each other to promptly and effectively handle enquiries, complaints, audits or claims from any court, governmental official, Supervisory Authority, third parties or individuals (including but not limited to the Data Subjects). Processor shall inform JCI of any such enquiry, complaint or claim within 24 hours of Processor's receipt of such enquiry, complaint or claim, unless prohibited under national law. Processor shall – specifically in such cases – provide all information that is necessary for JCI to fulfill its obligations under the applicable Data Protection Rules and these Terms, including the completion of privacy impact assessments and including making available all information necessary to demonstrate compliance by Processor with its obligations under these Terms. The Parties shall cooperate to respond appropriately to the exercise of any rights of any Data Subjects, in a timely manner, including with respect to objection to Processing, access, rectification, erasure, restriction, blocking, withdrawing consent, automated decision-making, profiling and portability of Personal Data. If a Data Subject seeks to object to the Processing of, or seeks to access, rectify, erase, restrict or block Personal Data pertaining to him or her, or exercise any rights regarding automated decision-making, withdrawal of consent, profiling or portability, Processor shall co-operate with JCI to take the actions required under the Data Protection Rules in accordance with JCI's instructions.

8. **Security Incidents and Breach Notification**

Processor shall inform JCI as soon as possible and in any event within 24 hours of discovering a Security Incident or a potential Security Incident, including a Security Incident concerning business contact information. The information should provide the details of the Security Incident, including (i) information on the Data Subjects affected, including categories and numbers of Data Subjects affected, and jurisdiction(s) where Data Subjects are located; (ii) a description of the nature of Security Incident, including the day on which or time period during which the Security Incident occurred and the cause of the Security Incident if known; (iii) a description of the Personal Data that was compromised or potentially compromised; (iv) the identity and contact details of a contact person who can answer questions on behalf of the Processor; (v) the likely consequences of the Security Incident, including an assessment of the risk of harm to Data Subjects; and (vi) a description of the steps taken to reduce the risk of harm to the Data Subjects, as well as the steps intended to be taken and/or recommended by the Processor to minimize possible harm. Processor shall provide all additional information reasonably requested or required by JCI in connection with the Security Incident. Processor shall fully cooperate with JCI in connection with the investigation, containment and remediation of the Security Incident.

In addition, Processor will inform JCI within 24 hours if (i) Processor or its Personnel, Affiliates or Sub-Processors infringe Data Protection Rules or obligations under these Terms, (ii) significant failures occur during the Processing, or (iii) there is reasonable suspicion of the occurrence of an event as defined under (i) and (ii) of this paragraph. In consultation with JCI, Processor must take appropriate measures to secure Personal Data and limit any possible detrimental effect on Data Subjects.

The Parties are aware that Data Protection Rules may impose a duty to inform the Supervisory Authority or affected Data Subjects in the event of a Security Incident. Processor shall assist JCI in providing notice to the Supervisory Authority and affected Data Subjects and meeting any other requirements that may apply to JCI or any of its Affiliates pursuant to applicable Data Protection Rules. Processor shall notify JCI of any Security Incident prior to notifying any Supervisory Authority or Data Subject of the Security Incident, and the form and content of such notification(s) shall be subject to JCI's approval (subject to any mandatory form or content requirements under applicable Data Protection Rules), unless Processor cannot provide such advance notification to JCI and also comply with its legal obligations under applicable Data Protection Rules.

9. **Inspection & Audit Rights**.

Upon prior written notice, JCI may inspect Processor's operating facilities or conduct an audit to ascertain compliance with these Terms. This right includes, but is not limited to, the verification of whether Processor has implemented appropriate physical, technical and organizational controls and procedures to protect the confidentiality, integrity and security of the Personal Data. The inspection may be carried out by JCI, or an independent third party, or by means of a self-assessment process approved by JCI. Processor shall fully cooperate with any such audit and investigation procedures initiated by JCI.

10. **Retention, Return and Deletion of Personal Data**:

These Terms shall remain in force until the latest of: (i) the date the Services provided under the MSA are completed, (ii) all Personal Data has been returned to JCI and/or irrevocably deleted/destroyed, (iii) the expiration or termination of the MSA, or (iv) the expiration of any confidentiality obligations.

The Processor shall not retain Personal Data (or any documents or records containing Personal Data, electronic or otherwise) for any period of time longer than is necessary to serve the purposes of the MSA.

Upon expiration of the purposes for Processing the Personal Data, termination of these Terms, or at any time at the request of JCI, Processor, at the discretion of JCI, shall return to JCI or irrevocably destroy and delete all Personal Data and other materials containing Personal Data, including existing copies of the Personal Data, subject to Processing, unless otherwise required by applicable law. Additionally, all Personal Data should be irretrievably expunged from any computer, server, media or storage device, word processor or similar device in which it was stored or Processed by Processor or by its Sub-Processors. Processor shall certify that this has been done upon JCI's request. Processor shall warrant that it, its Personnel, Affiliates and any Sub-Processors shall continue to be bound by their obligations of confidentiality after termination of the MSA or these Terms.

11. **Indemnity**.

In the event of non-compliance with any of the provisions of these Terms on the part of Processor or its Personnel, Affiliates or Sub-Processors, Processor shall defend, indemnify, and hold harmless JCI, its Affiliates and its directors, officers and Personnel from and against any third-party claims, actions, applications, demands, complaints, damages, or liabilities (including reasonable legal fees and disbursements) arising from such non-compliance.

12. **Governing Law.**
These Terms are governed by the law of the country that governs the GSA and the Parties submit to the jurisdiction of the courts referred to in the GSA without regard to provisions related to conflicts of law.

13. **Variation of the Terms.**
These Terms may only be modified by a written amendment signed by each of the Parties.

14. **Invalidity and Severability.**
If any provision of these Terms is found by any court of administration body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect the other provisions of these Terms. Where permitted by applicable law, the Parties agree that in the place of the invalid provision, a legally binding provision shall apply which comes closest to what the Parties would have agreed if they had taken the partial invalidity into consideration.

IN WITNESS WHEREOF, the Parties have executed these Terms as of the last dated signature below.

Executed by:	Executed by:
Johnson Controls, Inc.	**[INSERT NAME OF PROCESSOR]**
By:_____ (Authorized Signature)	By:_____ (Authorized Signature)
Name:_____	Name:_____
Date:_____	Date:_____

SCHEDULE 1 – Model Contract for Transfers from EEA Countries

Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 (Module Two for controller to processor transfers)

In relation to Personal Data transferred subject to Module Two of the Model Contract in accordance with Section 4.2 of these Terms:

a. for clause 9(a), option 2 (general written authorisation) is selected and the specified time period is thirty (30) days;
b. the optional language at clause 11(a) (redress) is used**;**
c. for clause 17, the second option (governing law of the EU Member State in which the data exporter is established) is used; and
d. for clause 18(b), the selected forum shall be the courts of the EU Member State in which the data exporter is established.

Standard Contractual Clauses annexed to Commission Implementing Decision (EU) 2021/914 (Module Three for processor to processor transfers)

In relation to Personal Data transferred subject to Module Three of the Model Contract in accordance with Section 4.2 of these Terms:

a. for clause 9(a), option 2 (general written authorisation) is selected and the specified time period is thirty (30) days;
b. the optional language at clause 11(a) (redress) is used;
c. for clause 17, the second option (governing law of the EU Member State in which the data exporter is established) is used; and
d. for clause 18(b), the selected forum shall be the courts of the EU Member State in which the data exporter is established.

ANNEXES TO THE MODEL CONTRACT

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name: _____[The **Johnson Controls affiliates** established in the European Economic Area ("EEA") as referenced in Appendix A attached hereto and legally represented by Power of Attorney set forth in the Intra-Group Agreement dated 1st July 2017, by Johnson Controls Inc. with Address: 5757 North Green Bay Avenue, Milwaukee, Wisconsin 53209, USA]

_____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

___ The EEA-based affiliates of Johnson Controls., a global diversified company in the fire & security, building and technology industries.

_____

Signature and date: _____

Role (controller/processor):

2. …

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: _____

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

_____

_____

Signature and date: _____

Role (controller/processor): 2. …

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

…

Categories of personal data transferred

…

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

…

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

…

Nature of the processing

…

Purpose(s) of the data transfer and further processing

…

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

…

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

…

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

…

APPENDIX A – DATA EXPORTER ENTITIES

The Johnson Controls affiliates referenced in this Appendix A are party to the Model Contract as data exporter. This Appendix A reflects the EEA based Johnson Controls affiliates that are party to the Intra-Group Agreement dated 1st July 2017 and which are referenced in Schedule 1 to that agreement and which is available at www.johnsoncontrols.com/IGA. Processor understands that additional Johnson Controls affiliates (not identified at the time of the execution of the Model Contract) may from time to time become party to the aforementioned Intra-Group Agreement. Parties agree that such additional Johnson Controls affiliates will, through their accession to the aforementioned Intra-Group Agreement become party to the Model Contract for the transfer of personal data to Processor and Processor agrees to process and protect personal data it imports from such data exporters under the Model Contract.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

Measures for ensuring physical security of locations at which personal data are processed

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

…

SCHEDULE 2 – UK Addendum to the Model Contract

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

UK Addendum to the EU Commission Standard Contractual Clauses

DATE OF THIS ADDENDUM:

1. The EU Commission Standard Contractual Clauses, incorporated by reference to these Terms in accordance with Section 4.2 and Schedule 1 to these Terms (the "Clauses") are dated [INSERT DATE.] This Addendum is effective from: Choose one option and delete the other:
The same date as the Clauses.

BACKGROUND:

2. The Information Commissioner considers this Addendum provides appropriate safeguards for the purposes of transfers of personal data to a third country or an international organisation in reliance on Articles 46 of the UK GDPR and, with respect to data transfers from controllers to processors and/or processors to processors.

INTERPRETATION OF THIS ADDENDUM

3. Where this Addendum uses terms that are defined in the Clauses those terms shall have the same meaning as in the Clauses. In addition, the following terms have the following meanings:

This Addendum	This Addendum to the Clauses
The Clauses	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021 incorporated by reference in accordance with Section 4.2 and Schedule 1 to these Terms.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.

SCHEDULE H

INSURANCE

Supplier warrants that it will continuously maintain in force insurance with the following requirements during the term of this Agreement and any JCI purchase order or SOW issued in connection with this Agreement, including any extensions, and until Supplier completes work to the satisfaction of JCI. Supplier shall not commence any work of any kind under this Agreement until it complies with all of these insurance requirements, and until it files evidence of such compliance satisfactory to JCI as to form and content. Neither approval of the insurance by JCI nor procurement or maintenance of insurance by Supplier shall relieve or decrease the liability of the Supplier hereunder. Failure to maintain insurance shall constitute a material breach of this Agreement.

1.1 Definitions

(a) Professional Liability Insurance; Errors & Omissions Liability Insurance. Such insurance will include coverage for any and all errors, omissions or negligent acts in the delivery of Products, Services and Licensed Programs contemplated under this Agreement, including but not limited to, contingent bodily injury and property damage liability, non-owned intangible property of others (such as the data that could be damaged, lost, stolen or inappropriately disclosed by Supplier), degradation, nonperformance and infringement of any proprietary right of any third party, including copyright, trade secret, and trademark infringement as related to Supplier's performance under this Agreement and defense costs. The policy shall cover the liability of JCI by reason of any actual or alleged error, omission, negligent act or wrongful act of Supplier committed in rendering or failing to render any Products, Services and Licensed Programs in accordance with this Agreement. The Professional Liability and Errors & Omissions Liability Insurance retroactive coverage date will be no later than the Effective date of this Agreement.

(b) Network Liability Insurance which shall (a) cover, without limitation, the liability of Supplier associated with: unauthorized use, access, or disclosure of confidential or private information, transmission of a computer virus or denial of service that results from a failure of security; content, including copyright and trademark infringement and invasion of privacy arising out of material displayed in the course of business; identity theft; cyber extortion; cyber terrorism, all as related to Supplier's/Subcontractor's performance under this Agreement. JCI, its officers, agents and employees shall be included as additional insured.

1.2 Standard Conditions. All insurance policies must be written by companies with a current AM Best rating or equivalent of A-V or better. JCI shall, without exception, be given not less than thirty (30) days' notice prior to cancellation for other than non-payment of premium of any insurance required by this contract. Non-payment of premium shall require ten (10) days' notice of cancellation. JCI and any other entities as may be reasonably requested shall be named as additional insureds under the Commercial General Liability and Automobile Liability policies with respect to work performed under this contract including without limitation, with respect to third party claims or actions brought directly against Supplier or JCI and Supplier as co-defendants and arising out of this agreement. It should contain a provision that JCI although named as additional insured, will nonetheless be entitled to recovery for any loss suffered by JCI as a result of Supplier's negligence. It is expressly agreed and understood by and between Supplier and JCI that the insurance afforded the additional insureds shall be the Primary insurance and that any other insurance carried by JCI shall be excess of all other insurance carried by Supplier and shall not contribute with the Supplier's insurance. Supplier waive their rights of recovery and will cause their insurers to waive their rights of subrogation under all liability coverage's required including their respective agents and employees. Supplier hereby releases JCI, including their respective affiliates, directors and employees, for losses or claims for bodily injury, property damage or other insured claims arising out of performance under this contract. Supplier agrees to comply with all insurance laws, regulations and statues in the jurisdiction in which the agreement applies. Supplier is solely responsible for any deductibles and/or self-insured retentions on their insurance policies. Supplier will provide evidence of insurance upon request and annually as long as insurance is required to be in force. Evidence of insurance must include complete copies of any required endorsements.

1.3 Coverage Limits.

The following minimum insurance coverage and limits are required. The procurement and maintenance of the below insurance coverage shall not limit or affect any liability which Supplier may have by virtue of this contract. All insurance policies related to the minimum coverage and limits should be issued on an occurrence form with the exception of Professional Liability/Errors & Omissions insurance. A claims made or project based policy to meet Professional Liability/Errors & Omissions insurance is acceptable as long as the retroactive date precedes the date of this contract and as long as upon expiration or termination of this agreement, Supplier will maintain an active policy, or purchase an extended reporting period providing for claims first made and reported to the insurance company within three (3) years after final payment under this Agreement. All limits are stated in U.S. Dollars.

Type of Insurance	**Minimum Limits**
Commercial General Liability*, including premises, operations, independent contractors, products-completed operations, personal and advertising injury, and liability assumed under an insured contract **	$5,000,000 per occurrence, general aggregate; Commercial General Liability limits may be met with a combination of General Liability and Umbrella/ Excess Liability policy limits
Automobile Liability covering all autos used in connection with the work performed, including owned, non-owned and hired autos	$5,000,000 combined single limit covering property damage and bodily injury
Workers' Compensation prescribed by applicable local law	The greater of $1,000,000 per occurrence or the amounts proscribed by law.
Employer's Liability	$1,000,000 each accident, each employee, each disease – policy limit or as required by local law
Professional Liability/Errors & Omissions each occurrence, including /Network and Privacy Liability	$10,000,000 each occurrence
Blanket Fidelity Bond/Crime Insurance	$5,000,000 each claim
Employee dishonesty and computer fraud	$10,000,000 each claim
Electronic data processing all risk property insurance on equipment, data, media, valuable papers, including extra expense coverage, with a minimum limit adequate to cover such risks on a replacement cost basis	

** If Commercial General Liability (CGL) does not automatically cover Supplier's contractual liability under this agreement, Supplier shall obtain a specific endorsement adding such coverage. If said CGL policy is written on a "claims made" basis instead of a: per occurrence" basis, Supplier shall arrange for adequate time for reporting losses. Failure to provide contractual liability endorsement coverage or adequate reporting time shall be at Supplier's sole risk.

Delivery of Certificates of Insurance. Certificates evidencing such insurance shall be furnished to JCI prior to commencement of work and are to provide a thirty (30) day notice of material change or cancellation. Certificates will state that all coverage's carried by Bidder are primary with respect to any coverage carried by JCI.