Data Access Agreement

This **Data Access Agreement** ("Agreement"), made as of February 28, 2020 ("Effective Date") by and between **JOHNSON CONTROLS, INC.**on behalf of itself and its Affiliates (collectively, "Company" or "JCI") **and INSERT SUPPLIER FULL NAME** ("Supplier"). Company and Supplier may each be referred to herein individually as a "party" or collectively as the "parties."

WHEREAS, Supplier, in the performance of its services (the "Purpose") pursuant to an agreement between Supplier and Company, dated [INSERT DATE OF UNDERLYING/EXISTING AGREEMENT BETWEEN COMPANY AND SUPPLIER, IF ANY – IF NO EXISTING AGREEMENT, DISCUSS WITH LAW DEPARTMENT] (the "Service Agreement") may require access to Confidential Information (as hereinafter defined);

WHEREAS, the parties recognize the sensitive, proprietary and confidential nature of Confidential Information and desire to maintain the confidentiality, privacy and security of the Confidential Information in compliance with the provisions of this Agreement.

NOW THEREFORE, in consideration of the mutual covenants contained in this Agreement the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. Confidential Information.

1.1 Defined. "Confidential Information" means any information disclosed or made available by or on behalf of Company, Company's Company customer, or a Company Affiliate (defined below) to Supplier during the term of this Agreement, whether directly, through access to computer systems, networks, work-site, or indirectly through any other third party, other than information that:

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

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

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

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

2. Maintenance of Confidentiality.

2.1 Use. Supplier shall use the Confidential Information only for the purpose of performing Supplier's obligations under the Agreement for the benefit of JCI (the" Purpose"), and shall comply with the security requirements set forth in the **SECURITY ADDENDUM** attached hereto as Exhibit A, including Schedule 1 and Schedule 2, all of which are incorporated herein by reference. Supplier shall not use the Confidential Information to: (i) compete directly or indirectly with Company; or (ii) interfere with any actual and/or proposed business of Company.

2.2 Nondisclosure. Supplier shall not disclose or otherwise make available any of the Confidential Information to anyone, including employees, consultants, agents, directors, officers, shareholders and representatives (individually and collectively, "Personnel"), except to the extent that such persons (a) need to know the Confidential Information for the Purpose; and (b) who are bound by obligations of non-use and non-disclosure substantially similar to those set forth herein. Supplier shall be responsible for its Personnel's use or disclosure of the Confidential Information.

2.3 Care. Supplier 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.

2.4 Compelled Disclosure. Supplier may disclose the Confidential Information to the extent that such disclosure is required by law or court order, provided that Supplier shall promptly provide Company 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.

3. Term and Continuing Obligations.

3.1 Term. This Agreement will commence as of the Effective Date and the exchange of information hereunder will terminate immediately upon Company's notice thereof.

3.2 Survival. Supplier's duty to protect the Confidential Information will survive termination of this Agreement (subject to the exceptions set forth in Section 2.1(a) to (d)) or such shorter period as required by applicable law.

3.3 Return of Confidential Information. At the written request of Company, Supplier shall promptly return the Confidential Information, including, without limitation, summaries, extracts, and any copies thereof.

4. No Grant of License or Warranty. Company's disclosure of Confidential Information hereunder will neither constitute nor be construed as a grant of any license or other property right in any portion of such Confidential Information. **THE CONFIDENTIAL INFORMATION IS PROVIDED AS IS, EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR ANY OTHER WARRANTY, WHETHER EXPRESSED OR IMPLIED.**

5. **Miscellaneous**.

5.1 On June 30, 2012, ADT Security Services, Inc. ("ADT") changed its name to Tyco Integrated Security LLC. On

September 2, 2016 Johnson Controls, Inc. merged with Tyco International plc. Therefore, any occurrences of the terms "ADT" or "Tyco" or "Johnson Controls" or "JCI" in the Service Agreement for purposes of this Data Access Agreement shall be replaced with the term "Company".

5.2 Affiliate. The term "Affiliate" means any company or entity that has Johnson Controls International plc ("JCI PLC") as its ultimate parent company, as well as any entity or joint venture in which JCI PLC or a JCI PLC Affiliate has any ownership, or any third party with whom JCI PLC or its Affiliate has a contractual relationship to resell such party's products and/or services.

5.3 Equitable Relief. Supplier hereby acknowledges that disclosure of the Confidential Information by it or breach of the provisions contained in this Agreement will give rise to irreparable injury to Company, its Affiliates, and/or its customers and such breach or disclosure is inadequately compensable in money damages. Accordingly, Company, its Affiliates, and/or its customers may seek and obtain 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 equity. Supplier hereby further acknowledges and agrees that the covenants contained herein are necessary for the protection of Company's, its Affiliates' and Company's legitimate business interests and are reasonable in scope and content.

5.4 Insider Trading. 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 Company or its customers or sharing the information with others who trade in the securities of Company or its customers is a violation of this Agreement and may be a violation of law.

5.5 Choice of Law. This Agreement will be governed by and construed in accordance with the laws of the State of Florida without regard to the conflicts of laws rules thereof. The parties irrevocably submit to the jurisdiction of the state and federal courts of the State of Florida located in Palm Beach County to resolve any disputes arising under or related to this Agreement.

5.6 Waiver. Except as otherwise specifically provided for hereunder, Company shall not be deemed to have waived any of its rights hereunder or under any other agreement with respect to the subject matter hereof unless such waiver is in writing and signed by Company waiving said right. Except as otherwise specifically provided for hereunder, no delay or omission by Company in exercising any right with respect to the subject matter hereof will operate as a waiver of such right or any such other right. A waiver on any one occasion with respect to the subject matter hereof will not be construed as a waiver of any right or remedy on any future occasion.

5.7 Severability. All of the provisions of this Agreement will be considered as separate terms and conditions and in the event any provision will be held void, voidable, or legally invalid or otherwise unenforceable by any court of competent jurisdiction of law or in equity, all the other terms, conditions, and provisions contained herein will remain in full force and effect.

5.8 Notices. All notices given pursuant to this Agreement will be in writing and will be deemed to have been given when delivered by hand, or mailed by registered or certified mail, return receipt requested, postage prepaid to the above stated address of the party and, if address to Company to the attention of its Law Department, or any other address that a party may designate in accordance with the provisions of this paragraph, provided that notice of change of address will be deemed given only when received.

5.9 Assignment. Supplier acknowledges that Company may assign this Agreement to any Affiliate, without the consent of Supplier. Supplier hereby acknowledges that the services to be provided by Supplier are unique and personal. Accordingly, Supplier shall not assign this Agreement in whole or in part without the prior written consent of Company, which may be withheld for any reason at Company's sole discretion. The provisions of this Agreement shall be binding upon and inure to the benefit of the respective successors and permitted assigns of each party.

5.10 Entire Agreement. This Agreement constitutes the entire agreement between the parties hereto with respect to the subject matter hereof and may not be released, discharged, amended or modified except by an instrument in writing executed in the same manner as this Agreement by duly authorized representatives of each of the parties hereto. This Agreement imposes no obligation on either party to purchase, sell, license, transfer, or otherwise dispose of any technology, services or products and does not create any agency or partnership relationship.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the Effective Date shown above.

JOHNSON CONTROLS, INC.	**INSERT SUPPLIER FULL NAME**
By: _____	By: _____
Signature of Authorized Representative	Signature of Authorized Representative
Name Printed: _____	Name Printed: _____
Its: _____	Its: _____
Title	Title

Data Access Agreement
Exhibit A

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)

Data Access Agreement

Exhibit A - Schedule 1

INFORMATION SECURITY REQUIREMENTS

The following items are considered Company's minimum security requirements. This Schedule 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 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.

Data Access Agreement

Exhibit A - Schedule 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

[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.

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 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