CYBERSECURITY AND PRIVACY AGREEMENT

MPW Industrial Services Group, Inc. ("MPW") provides the following Cybersecurity and Privacy Agreement ("Agreement"), which apply to suppliers providing goods or services to MPW. In addition to any additional agreed upon terms and conditions, all goods or services provided by vendor, any subsidiary or affiliate, or their agents (all referred to as "Vendor") are expressly limited and conditioned upon acceptance of the following Agreement, and no provision, printed or otherwise, contained in any order, acceptance, confirmation, or acknowledgement which is inconsistent with this Agreement is accepted by MPW unless specifically agreed to in writing by MPW.

1. **Relationship to Other Agreements.** This MPW Cybersecurity and Privacy Agreement ("Cybersecurity Agreement") is intended to be additive or cumulative to any other agreement, exhibits, or attachments (the "Purchasing Agreement") thereto. In the event of any inconsistency between the terms of this Cybersecurity Agreement and the Purchasing Agreement, the terms of this Cybersecurity Agreement shall control and take precedence. A related term in the Purchasing Agreement thereto is inconsistent only if it cannot be performed because it conflicts with a term or condition in this Cybersecurity Agreement.

2. **Definitions.** Solely for purposes of this Cybersecurity Agreement, the following terms shall have the following meanings:
   a. Applicable Laws. Any and all acts, codes, statutes, laws, treaties, ordinances, judgments, decrees, injunctions, writs, orders, rules, regulations, directives, permits, guidelines, policies and interpretations (to the extent mandatory), as any of them may be amended from time to time, of any government authority, or any department or agency of any government authority, to the extent having jurisdiction over MPW (and its affiliates), Vendor, the performance of the Services, the Deliverables, the Purchasing Agreement, or in connection with testing, commissioning, demonstration, operation, acceptance or maintenance of the Services or Deliverables.
   b. Confidential Information. All written or oral information, data, analyses, documents, and materials furnished or made available by the disclosing party to the receiving party in connection with the Purchasing Agreement, and any and all analyses, compilations, studies, documents, or other material prepared by the receiving party to the extent containing or based upon disclosing party's Confidential Information. All MPW data is Confidential Information, regardless of whether it is marked as "confidential" or "proprietary." Confidential Information does not include information, data, analyses, documents, or materials that: (1) are, when furnished, or thereafter become available to the public other than as a result of a disclosure by the receiving party, (2) are already in the possession of or become available to the receiving party on a non-confidential basis from a third party who had a lawful right to disclose this information without any obligation to restrict its further use or disclosure, or (3) the receiving party can demonstrate that this information has been independently developed without a violation of the Purchasing Agreement.
   c. Cyber Incident. A Cyber Incident is (a) any unauthorized access to, use of, or other breach in the security of Vendor's computing systems that contain MPW Data, or any other accidental or unauthorized access to, interception of, acquisition, disclosure, use, modification, loss, damage, or destruction of MPW Data; or (b) if caused by the action or inaction of Vendor, any unauthorized access to, use of, or other breach in the security of MPW's Computing Systems, or any unauthorized

access to, interception of, disclosure or acquisition of MPW Data caused by the action or inaction of Vendor, Vendor's affiliates or Subcontractors.

d. Cyber System Information. Information about the Cyber System that could be used to gain unauthorized access or pose a security threat to the Cyber System. Examples of Cyber System Information may include, but are not limited to, security procedures or security information about Cyber Systems, physical access control systems, and electronic access control or monitoring systems that are not publicly available and could be used to allow unauthorized access or unauthorized distribution; collections of network addresses; and network topology of the Cyber System.
e. Deliverables. The materials, software, documentation, and any other works delivered by Vendor to MPW under the Purchasing Agreement.
f. MPW's Computing Systems. MPW's and its affiliates; respective electronic computing and information systems, computers, servers, applications, files, electronic mail, electronic equipment, wireless devices, databases, data storage, and other data resources, and MPW-sponsored connections to the internet communications network.
g. MPW Data. Any non-public information whether or not designated by MPW or its representatives as Confidential Information at the time it is provided or made available to Vendor, and all information Vendor derives from such information, including any deliverables created by Vendor for MPW.
h. MPW Personal Information. Any information in the possession or under the control of MPW or any of its affiliates, or that is furnished or made available by MPW or any of its affiliates to Vendor, that identifies an individual, or that relates to, describes, or is capable of being associated with, an identifiable individual (whether a current or former MPW employee, customer, or otherwise), including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, government issued identification number, insurance policy number, medical information or health insurance information, education, employment, employment history, bank account number, credit card number, debit card number, any other financial information, combination of online account user name/ID and password and/or security question together with the answer, or information regarding the individual's electric energy usage or electric service, including, without limitation, service account number, electricity demand (in kilowatts), monthly billed revenue, credit history, rate schedule(s), meter data, or number or type of meters at a premise. MPW Personal Information includes "personal information" as defined in The California Consumer Privacy Act, California Civil Code Section 1798.100 – 1798.199.
i. Purchasing Agreement. The applicable contract/agreement, exhibit, or attachment correlating to the Cybersecurity Agreement that will be signed between Vendor and MPW.
j. Services. The services to be performed by Vendor, or which Vendor causes a Subcontractor to perform, the creation, provision, or furnishing of Deliverables, and all other obligations of Vendor as required by the Purchasing Agreement.
k. Subcontractor. A third party to whom Vendor delegates a portion of its performance obligations under the Purchasing Agreement.
l. Vendor. Any entity or person that provides products or services to MPW or its affiliates. Vendor includes, but is not limited to, Contractor, Consultant, and Licensor, as those terms may be used in the Purchasing Agreement.

3. **Additional Warranties and Representations.** In addition to any other representations and warranties contained in the Purchasing Agreement, and notwithstanding any statement in the Purchasing Agreement limiting the applicable warranties, Vendor hereby represents and warrants that it has read and understood this Cybersecurity Agreement and that Vendor is fully compliant with them. Vendor further warrants that, throughout the term of the Purchasing Agreement and as long as Vendor continues

to have access to, is in possession of, or acquires MPW Data or has access to MPW's Computing Systems, Vendor will continue to comply fully with this Cybersecurity Agreement. Vendor shall immediately notify MPW if it knows or reasonably believes that it is not compliant with any of the requirements of this Cybersecurity Agreement. Vendor further represents and warrants that it is not and has not been a party to any current, pending, threatened or resolved enforcement action of any government agency, or any consent decree or settlement with any governmental agency or private person or entity regarding any failure in Vendor's data security safeguards, or otherwise regarding information privacy or security.

4. **Additional Indemnification Obligations.** Vendor shall, and Vendor shall cause its Subcontractors to, indemnify, defend and hold harmless MPW and its affiliates, officers, directors, employees, agents, representatives, successors, and assigns from and against any and all losses, liabilities, damages and claims, and all related costs and expenses (including any costs or expenses related to increased regulatory or administrative oversight), fines, penalties, or interest, including reasonable legal fees and costs, arising out of, in connection with, resulting from or relating to any claim relating to Vendor or its Subcontractor's breach of any of Vendor's material obligations under this Cybersecurity Agreement.

5. **Limitation of Liability Exception.** Any limitations of liability set forth in the Purchasing Agreement, including but not limited to limitations of liability with respect to consequential damages or total aggregate damages, shall not apply to damages arising out of, in connection with, resulting from or relating to Vendor or its Subcontractor's breach of any of Vendor's material obligations under this Cybersecurity Agreement.

6. **Confidentiality and Non-Disclosure Obligations.** This Section 6 shall apply notwithstanding any provision to the contrary in the Purchasing Agreement. Vendor shall hold MPW Data in strict confidence, and Vendor may distribute or disclose such information only as specifically provided in a purchase order or statement of work, or as otherwise expressly authorized in writing by MPW. Vendor's obligations under this Section 6 shall apply regardless of whether such information falls within the definition of Confidential Information under the Purchasing Agreement and shall continue until such time as MPW provides notice that such information may be distributed or disclosed without restriction. This Section 6 shall survive the termination or expiration of the Purchasing Agreement.

7. **Additional Insurance.** Vendor shall have cyber liability insurance covering (a) liability arising from theft, dissemination and/or use of Confidential Information stored or transmitted in electronic form and (b) liability arising from the introduction of a computer virus into, or otherwise causing damage to, a customer's or third person's computer, computer system, network or similar computer related property and the data, software and programs stored thereon. Such insurance will be maintained with limits of no less than $5,000,000 per claim and in the annual aggregate, and may be maintained on a stand-alone basis, or as part of any errors and omissions coverage required in the Purchasing Agreement. This insurance shall have a retroactive date that equals or precedes the effective date of the Purchase Agreement. Vendor shall maintain such coverage until the later of: (1) a minimum period of three years following termination or completion of the applicable Purchase Agreement, or (2) until Vendor has returned or destroyed all MPW Data in its possession, custody or control, including any copies maintained for archival or record-keeping processes. All such insurance policies shall be written by reputable, financially sound insurance companies reasonably acceptable to MPW and shall include provisions for thirty (30) days' prior written notice to MPW of cancellation, material change or non-renewal. Any such cancellation, material change or non-renewal shall not affect Vendor's obligation to maintain the insurance coverages set forth above. All liability insurance policies required above shall be written on an "occurrence" policy form. Vendor shall not commence performance of the Services

until a certificate of insurance evidencing such insurance has been delivered to and approved by MPW. Vendor shall be responsible for payment of all deductibles on claims under Vendor's insurance policies. All such policies of Vendor shall be primary coverage regardless of whether or not MPW has similar coverage. MPW shall be named as an Additional Insured on all such policies of insurance. Vendor shall not self-insure without prior written approval of MPW. The required limits of liability may be satisfied by a combination of primary and excess insurance policies.

8. **Additional Audit Rights.** MPW has the right to conduct an audit of Vendor for adherence to the terms of this Cybersecurity Agreement not more than once per year; or more often upon notification or reasonable belief by MPW of any Cyber Incident as described in this Cybersecurity Agreement, or as required to comply with regulatory requirements. MPW also has the right to audit any Subcontractor or Vendor service provider upon notification of any Cyber Incident involving the Subcontractor or Vendor service provider. Vendor will cooperate with any audit and require the cooperation of any Subcontractor or Vendor service provider. MPW may require Vendor to participate in annual security risk assessments of any security systems or environments which store, manage, process, or access MPW Confidential Information.

9. **Termination for Breach.** If Vendor breaches any of the terms and conditions of this Cybersecurity Agreement, then MPW may in its discretion immediately terminate the Purchasing Agreement for cause without giving Vendor an opportunity to cure. In such case, MPW shall not be responsible for any termination liability.

10. **Rights in the Event of Breach.** MPW shall have the right to bring immediate suit in a court of competent jurisdiction against Vendor for a breach of this Cybersecurity Agreement by Vendor or any of its Subcontractors, employees, agents, or representatives to whom this Cybersecurity Agreement applies.

11. **Vendor Obligations.**
    a. It is Vendor's obligation to (i) implement and maintain appropriate measures to protect its electronic network and systems from Cyber Incidents that could make MPW's Computing Systems vulnerable to unauthorized access or use and to protect MPW Data in its possession, custody, or control from accidental or unauthorized access, acquisition, disclosure, use, modification, loss, damage, or destruction; (ii) regularly review and revise those measures to address new or ongoing risks and to implement industry best practices and legal requirements regarding cybersecurity and privacy; and (iii) to cooperate with MPW in its efforts to minimize risks to MPW's Computing Systems and MPW Data and reduce the impact of any unauthorized access to the MPW's Computing Systems, or disclosure or unauthorized use of MPW Data.
    b. Vendor's security measures to protect its electronic network and systems from Cyber Incidents that could make MPW's Computing Systems vulnerable to unauthorized access or use to protect MPW Data in its possession, custody, or control shall be no less rigorous than industry cybersecurity and privacy best practices.
    c. In accordance with industry best practices and applicable laws, Vendor shall conduct a background investigation for every employee receiving access to MPW's Computing Systems or MPW Data. For new hires and current employees who do not yet have access to MPW's Computing Systems or MPW Data, the background check shall occur before the employee receives such access. For existing employees who already have access to MPW's Computing Systems or MPW Data, the background check should be conducted promptly. Background checks must include the following:

i. Background verification including whether the prospective employee has been convicted of a felony, property crime or fraud in any state where the individual has resided, studied, or worked during the past seven years; and
ii. Check of United States' Specially Designated Nationals List and the Denied Persons List.

12. **Cybersecurity and Privacy Requirements.** The following provides the cybersecurity and privacy requirements Vendor must maintain as long as Vendor has access to MPW's Computing Systems or access to, possession, custody, or control of MPW Data.
    a. Management of Information Security. Vendor shall maintain, update as necessary, and adhere to a comprehensive written information security program (the "Information Security Program") that: (i) contains appropriate administrative, technical, and physical safeguards to protect its electronic network and systems from Cyber Incidents that could make MPW's Computing Systems vulnerable to unauthorized access or use and to protect MPW Data in its possession, custody, or control; (ii) complies with applicable laws and regulations and conforms to industry best practices; (iii) is reviewed and revised for adequacy and effectiveness at regular intervals (at least annually and whenever there is a change in Vendor's practices that may affect the security of MPW Data or MPW's Computing Systems). While providing the Services, Vendor shall not alter or modify its Information Security Program in such a way that it will weaken or compromise the confidentiality, availability, or integrity of MPW Data or MPW's Computing Systems.
    b. Employee Policies. Vendor shall provide its personnel with privacy and information security training before providing such personnel access to MPW's Computing Systems or MPW Data and at least annually thereafter. Vendor shall maintain employee completion reports and make such completion reports available to MPW upon MPW's written request. Vendor shall review the contents of its security and privacy awareness and training program at least annually to ensure it is updated and reflects current, relevant security information. Depending upon the nature of the engagement MPW may specify in the purchase order, work order, or statement of work that Vendor shall supplement its information security training program with training or materials that MPW provides. Upon request, Vendor shall certify compliance with these training requirements.
    c. Vendor Management. Vendor shall assess and track cybersecurity and privacy risk associated with Subcontractors or its service providers with access to MPW's Computing Systems or MPW Data and shall take all commercially reasonable actions to promptly remediate these risks. Vendor shall contractually obligate Subcontractors or its service providers to (1) use industry best practices to protect their electronic network and systems from Cyber Incidents that could make MPW's Computing Systems vulnerable to unauthorized access or use and to protect MPW Data when accessed, processed, or stored by a Subcontractor or service provider and (2) immediately report to Vendor any reasonably suspected or confirmed Cyber Incident that could impact MPW's Computing Systems or MPW Data.
    d. Off-Shoring. Vendor shall not permit access to MPW's Computing Systems or transmit, access, use, or store MPW Data outside the United States without MPW's prior written permission. Vendor is responsible for understanding and complying with the applicable cybersecurity and privacy laws and regulations of the foreign jurisdictions from which MPW agrees that MPW's Computing Systems or MPW Data may be accessed, used, or stored. As part of any offshoring request, Vendor shall inform MPW of any applicable foreign laws or regulations that may reduce the confidentiality, availability, or integrity of MPW's Computing Systems or of MPW Data or impose additional burdens on MPW.
    e. Asset Management. All of Vendor's or its Subcontractor's devices, including cell phones or other portable storage devices, used to store MPW Data shall be equipped with industry standard security and encryption features, which shall include at a minimum remote wipe and remote shutdown capabilities. Vendor's and Subcontractors' personnel may not access or store MPW Data on any

personal or third-party devices, including mobile devices, tablets or personally owned laptops, unless such devices have been configured with industry standard security and encryption features, which shall include at a minimum remote wipe and remote shutdown capabilities.

f. Physical and Environmental Security. Vendor shall take appropriate steps to prevent unauthorized physical access, as well as accidental and intentional damage, to Vendor's physical premises and electronic systems that access, use, store or otherwise process MPW's Data. Vendor shall also protect against environmental risks (e.g. earthquakes, tornados, power failures) including by appropriate redundancies and backups) and systems malfunctions or failures.

g. Communications and Operations Management. Vendor shall maintain written procedures and technological controls for the following areas.
   i. **Malware Protection.** Vendor shall use anti-malware software on networks, servers, workstations, and portable devices that may be used to access MPW's Computing Systems, or to access, use, or store, MPW Data; the malware signatures shall be regularly updated in a timely manner.
   ii. **Patches and Updates.** Vendor shall follow industry best practices for patching and updating software and firmware on networks, servers, workstations, and portable devices that may be used to access MPW's Computing Systems, or to transmit, access, use, or store, MPW Data.
   iii. **Administrative Activity.** Vendor shall minimize administrative privileges and allow personnel to only use administrative accounts when required.
   iv. **Email Relaying.** Vendor shall secure access and prevent misuse of its own email resources.
   v. **Physical Media Tracking.** Vendor shall establish effective processes and procedures for handling, storing, and transporting media to protect MPW Data from unauthorized access and/or disclosure.
   vi. **Unapproved Wireless Networks.** Vendor shall have all network connections and devices adequately tracked, managed, authorized, and controlled to protect against threats and to maintain security for the systems and applications using the network.
   vii. **Wireless Network Encryption.** Vendor shall implement processes and tools to control the use of wireless local area networks, access points, and wireless systems, including industry best practice encryption for authorized wireless access points.
   viii. **System and Data Recovery.** Vendor shall regularly back-up MPW Data and systems that access, store, or use MPW Data. Backups of these systems and data shall be available, including the event of a disaster and the ability to restore from such backups shall be tested periodically.
   ix. **Change Control.** Changes affecting MPW's Computing Systems or MPW Data must be made with a formal change control program.
   x. **Data Encryption.** MPW Data, including any backups, must always be secured through industry best practice whole disk or media encryption and file or database encryption (if applicable) and strong access controls; and transmission of MPW Data must always be encrypted (using industry best practices).

h. Access Control. Vendor shall control access to its technology assets and MPW Data, including implementation of the following requirements:
   i. **Password Controls.** Password controls must meet industry best practices.
   ii. **Logical and Physical Access Authorizations and Suspensions.** Vendor shall limit access to MPW's Computing Systems and MPW Data only to active users who require access to perform the Services. Vendor shall immediately notify MPW management to promptly revoke or disable user access rights to MPW's Computing Systems and to MPW Data of any employee who is terminated, resigns, or retires, or who is reassigned from work requiring access to MPW's Computing Systems or to MPW Data. Vendor also shall immediately revoke the employee's or former employee's access to MPW Data in Vendor's possession, custody, or control.

iii. **Multifactor Authentication for Remote Access.** Vendor shall use two-factor authentication for remote access to systems that access or store MPW Data.

iv. **Return or Destruction of MPW Data.** As between MPW and Vendor, all MPW Data shall be and remain the property of MPW. Unless different requirements regarding the retention and destruction of MPW Data are included in the "Confidentiality" or "Non-Disclosure" section of the Purchasing Agreement, the following requirements shall apply to all MPW Data: At the end of each engagement, Vendor may keep one copy of the MPW Data solely for back-up storage purposes. The destruction of all MPW Data shall require use of industry best practices for rendering information irretrievable

i. Security Incident and Communications Management.

i. Vendor shall implement a formalized information security incident management program (the "Security Incident Management Program"). The program shall describe how the organization will report incidents internally and to affected external parties. It shall also identify Vendor's incident response team (the "Vendor Incident Response Team") and define their roles and responsibilities.

ii. Vendor shall regularly scan systems for vulnerabilities. Vendor shall rank all vulnerabilities and promptly remediate detected vulnerabilities ranked as critical, high, or moderate. Vendor will use commercially reasonable efforts to identify and notify MPW in writing within one business day of identification of any critical, high, or moderate vulnerabilities, risks or threats that could potentially impact MPW Data and that Vendor cannot remediate within 30 days.

13. **Changes in Law.** If either Vendor or MPW becomes aware of any changes to the law related to the subject matter of this Cyber Agreement , then that Party shall notify the other Party of the change, and the Parties shall meet in good faith as soon as practicable to discuss achieving compliance with the changed legal requirements.

14. **Audit.** During the term of this Agreement and thereafter, for as long as Vendor retains access to MPW Computing Systems, MPW Data, or MPW Personal Information, MPW representatives and agents will be entitled to conduct audits of Vendor's relevant operations, facilities, systems, etc. to confirm that Vendor has complied with the requirements laid out in this Agreement (the "Security Audits"). Any Security Audit shall be scheduled and conducted during normal business hours and shall not unreasonably interfere with Vendor's business activities. In the event that any Security Audit results in the discovery of material security risks to MPW Computing Systems, MPW Data, MPW Personal Information, or violations of applicable federal and state consumer privacy laws, rules, and regulations, Vendor shall (i) respond to MPW in writing with Vendor's plan to promptly take reasonable measures and corrective actions necessary to effectively eliminate the risk or cure the violation, at no cost to MPW, and (ii) allow MPW and the MPW's customers to review any system and transaction logs related thereto which pertain to MPW Data, MPW Personal Information or data potentially compromised. Vendor shall have five (5) business days to cure such security risk or violation, unless the parties mutually agree in writing to a longer period of time for such cure. MPW's right, and the right of the MPW's customers, Vendor representatives and agents, to conduct a Security Audit, and any exercise of such right, shall not in any way diminish or affect Vendor's duties and liabilities under this Agreement.

15. **Governing Law.** This Cybersecurity Agreement shall be governed by, and construed in accordance with, the laws of the State of Ohio, unless the Purchasing Agreement specifies another state's law, in which case that state's law shall apply to this Cybersecurity Agreement.