APPDENDIX S

Cyber Security Requirements

1. DEFINITIONS

The following terms have the meanings set forth below when used in this Exhibit. Terms used in this Exhibit with initial-capitalized letters but not defined herein have the meanings set forth in the Contract, or, if the Contract does not include any such meaning, the meaning given to such term in common technical usage.

"**Contract**" means that certain Power Purchase Agreement, dated as of _____, 20___, between Seller and PacifiCorp.

"**Confidential Business Information**" has the meaning as defined in the Contract and in addition includes, for the sake of this Exhibit, any information that can be used to identify or distinguish the identity of an individual, employee, or customer of PacifiCorp, including but not limited to name, social security number, date and place of birth, customer account number, customer address, customer energy usage information, credit or bank account number, passport or driver's license numbers, or any information that is linked or linkable to an individual, employee, or customer that is not otherwise classified as public information by PacifiCorp, including but not limited to; medical, financial, and employment information.

"**Data**" means any information, formulae, algorithms, or other content that PacifiCorp or PacifiCorp's employees, agents and end users upload, create or modify in connection with the performance of PacifiCorp's obligations under the Contract. Data also includes user identification information and metadata which may contain Data or from which PacifiCorp's Data may be ascertainable.

"**DMARC**" means Domain-based Message Authentication, Reporting and Conformance.

"**Help Desk**" means both the telephone number 515-281-2967 and the e-mail address GlobalSecurityOperations@brkenergy.com.

"**Prohibited Vendors**" has the meaning ascribed thereto in Section 7 of this Exhibit.

"**Security Incident**" means any circumstance when (i) PacifiCorp knows or reasonably believes that the confidentiality, integrity, or availability of any Confidential Business Information has been adversely impacted, including but not limited to, incidents where Confidential Business Information has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, or obtained by any unauthorized person, by any person in an unauthorized manner, or for an unauthorized purpose; (ii) Seller knows or reasonably believes that an act or omission has adversely impacted the cybersecurity of the products or services provided to PacifiCorp by Seller or the physical, technical, administrative, or organizational safeguards protecting Seller's systems or PacifiCorp's systems holding Confidential Business Information; or (iii) Seller receives any

complaint, notice, or communication which relates directly or indirectly to (A) Seller's handling of Confidential Business Information or Seller's compliance with the Data safeguards in the Contract (including this Exhibit) or applicable law in connection with Confidential Business Information or (B) the cybersecurity of the products or services provided to PacifiCorp by Seller.

"**Sensitive Personnel**" means all personnel with authorized unescorted physical access or authorized cyber access to PacifiCorp's covered units.

2. SCOPE OF THIS EXHIBIT

a. This Article applies to Seller and its personnel and subcontractors that provide hardware, software, or services to PacifiCorp that may impact the confidentiality, integrity, or availability of PacifiCorp's networks, systems, software, Data, or Confidential Business Information for the term of the Contract.

b. With respect to cybersecurity matters, this Exhibit will take precedence over any other Exhibits which contain cybersecurity provisions to the extent of any conflict between such Exhibits.

3. CYBER SECURITY CONTROLS

a. Without limiting Seller's obligations elsewhere in this Exhibit or the Contract, Seller must implement baseline security safeguards and controls to protect PacifiCorp's networks, systems, software, Confidential Business Information, and Data that are no less rigorous than accepted industry practices, specifically those set forth in the latest published version of the National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF)..

b. Seller agrees to notify PacifiCorp of Seller-deemed applicable security vulnerabilities in hardware, software, and services provided under the Contract in a timely manner.

c. Seller warrants that Seller installed hardware, software, and patches installed by Seller under the Contract will not contain malicious code. Seller agrees to provide a method to verify the integrity and authenticity of all software and patches provided by Seller.

d. Seller must follow all applicable PacifiCorp requirements for all remote access to PacifiCorp's System. Seller's personnel will only have gated interactive remote access to PacifiCorp's networks, PacifiCorp's System, and PacifiCorp's applications, through a PacifiCorp firewall and/or secure network connection and such access must be performed on a secure connection, which PacifiCorp will provide and maintain. Upon either (i) personnel termination actions or (ii) changes in the status of Sensitive Personnel which removes their need for remote access, Seller must report such termination or change in status to PacifiCorp's Help Desk. In the case of Sensitive Personnel and/or involuntary termination, notification must be immediate. In all other cases, notification must be within one (1) business day.

e. Seller must ensure that email from Seller and any services provided under the Contract:

1. Originate from a domain or domains with a published DMARC policy of “reject” and with a published Sender Policy Framework policy consisting of valid senders and a “fail” directive (-all). If the optional DMARC “pct” directive is used, "pct” must be set to “100”;

2. Passes a DMARC authentication check;

3. Utilizes a DomainKeys Identified Mail (DKIM) 2048 bit key; and

4. Supports Transport Layer Security (TLS).

f. Seller must encrypt and sign file transfers to or from PacifiCorp via Gnu Privacy Guard (GPG), Pretty Good Privacy (PGP), or another mutually agreeable payload encryption solution. Encryption must utilize National Institute and Technologies-approved algorithms, key lengths and cryptoperiods, with a two (2) year key lifetime or other mutually agreeable payload encryption solution.

g. Seller must utilize physical or virtual token-based multi-factor authentication compliant with National Institute of Standards and Technologies Authentication Assurance Level Two (2) or higher for remote access into Seller networks and external access to Seller email. Authenticators classified as Restricted by National Institute of Standards and Technologies guidance, such as short message service text messages or email, are prohibited.

h. If Seller requires receipt and retention of PacifiCorp Data during the term of the Contract and in accordance with the scope of the Contract, Seller must follow all applicable PacifiCorp requirements for storage, transfer, disposition and access of PacifiCorp Data as set forth in the Contract, including but not limited to:

i. Seller requests for PacifiCorp Data must be limited solely to the extent necessary to perform the services under the scope of the Contract and must be subject to PacifiCorp approval of transfer and storage implementations.

ii. Seller must permanently delete PacifiCorp Data in temporary transfer locations as soon as Seller moves such data to a storage location.

iii. Seller must restrict access to PacifiCorp Data to only necessary Seller personnel and in accordance with the scope of the Contract.

iv. Seller must delete or return PacifiCorp Data to PacifiCorp within the Contract term when retention of PacifiCorp Data is no longer necessary to fulfill Contract obligations.

i. If Seller's scope under the Contract includes an application programming interface, Seller must provide to PacifiCorp a specification for its interface aligned to the latest version available from the OpenAPI Initiative or mutually-agreed equivalent.

4. OVERSIGHT OF COMPLIANCE

a. If the Contract includes hosted or cloud services, Seller must provide annually to PacifiCorp a Statement on Standards for Attestation Engagements (SSAE) Service Organization Control (SOC) 2 Type II audit covering the scope of the Contract and pertaining directly to Seller.

b. If the Contract does not include hosted or cloud services, Seller must provide for one of the following:

1. Annually provide to PacifiCorp a copy of ISO 27001 certification covering the scope of the Contract and pertaining directly to Seller; or

2. Annually provide to PacifiCorp a copy of a third-party audit covering the security controls relevant to hardware, software, or services provided under the Contract and pertaining directly to Seller, including audit results and Seller's plan to correct any negative findings; or

3. Allow PacifiCorp to conduct an assessment, audit, examination, or review of Seller's security controls to confirm Seller's adherence to the terms of this Exhibit, as well as any applicable laws, regulations, and industry standards, not more than once per year or upon notification of any Security Incident or complaint regarding Seller's privacy and security practices. PacifiCorp may elect to obtain the services of a mutually agreeable third party to conduct this assessment, audit, examination, or review on behalf of PacifiCorp. PacifiCorp will give Seller no less than thirty (30) days' notice of its intent to conduct such assessment, audit, examination, or review. As part of this assessment, audit, examination, or review, PacifiCorp may review all controls in Seller's physical and/or technical environment in relation to all Confidential Business Information being handled and/or hardware, software, or services being provided pursuant to the Contract. Seller must fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, application software, and systems relevant to the provision of hardware, software, or services under the Contract.

5. SECURITY INCIDENT PROCEDURES; EQUITABLE RELIEF

a. In the event of a Security Incident, the Seller must:

1. notify PacifiCorp of the Security Incident as soon as practicable by telephone, but no later than forty-eight (48) hours after becoming aware of it and in writing within five (5) business days to the Help Desk; and

2. provide PacifiCorp with support through the below contact to assist with Security Incident management, response, and recovery associated with the Security Incident.

b. Immediately following notification of a Security Incident, the Parties will coordinate with each other to investigate such Security Incident and agree to coordinate with the handling of the matter, including: (i) assisting with an investigation and (ii) making available all relevant records and other materials required to comply with applicable law, regulation, industry standards, or otherwise reasonably required by PacifiCorp.

c. The Seller must use commercially reasonable efforts to assist PacifiCorp with the remedy of any Security Incident and help prevent any further or recurrent Security Incident in accordance with applicable privacy laws, regulations, and standards. The Seller must reimburse PacifiCorp for actual reasonable costs incurred in responding to, and mitigating damages caused by, any Security Incident, including all costs of notice and/or remediation pursuant to this Section 5, and to the extent that (i) they are caused by such Seller's negligence, or that of its officers, employees, agents, or subcontractors or (ii) Seller is liable for such failure under applicable law.

d. The Seller must provide all necessary information and assistance to PacifiCorp in any litigation or other formal action deemed commercially reasonable by PacifiCorp to protect its rights relating to the use, disclosure, protection, and maintenance of its Confidential Business Information and Data.

e. Seller acknowledges that any breach of the obligations set forth in this Section 5 may cause PacifiCorp substantial irreparable harm for which monetary damages would not be adequate compensation and agree that, in the event of such a breach or threatened breach, PacifiCorp is entitled to seek equitable relief, including a restraining order, injunctive relief and specific performance. Such remedies will not be deemed to be exclusive but will be in addition to all other available remedies at law or in equity, subject to any other express exclusions or limitations set forth in the Contract.

6. OBLIGATIONS ON TERMINATION AND TERMINATION ASSISTANCE

a. In addition to any other obligations that arise on termination or expiration of the Contract, the Parties agree that, on any expiration or termination of the Contract, upon completion of the delivery of the products and services to be provided under the Contract, or at any time upon PacifiCorp's request, regardless of the circumstance:

1. If Seller has access to PacifiCorp facilities or systems, Seller must immediately surrender to PacifiCorp all access cards, security passes, passwords and other such devices granting access to any PacifiCorp networks or computer systems; and

2. If Seller has PacifiCorp Data, Seller must return any PacifiCorp Data that is in its care, custody or control to PacifiCorp in the format requested by PacifiCorp and Seller must, within fourteen (14) days of receiving PacifiCorp's written confirmation that it can read the Data provided by Seller, (1) permanently delete any copies of the Data in Seller's care, custody or control, and (2) send PacifiCorp written confirmation that such Data has been deleted.

3. If Seller has PacifiCorp hardware or removable media, Seller will return to PacifiCorp all hardware and removable media provided by Seller that contains PacifiCorp Data. PacifiCorp Data in such returned hardware and removable media may not be removed or altered in any way. The hardware must be physically sealed and returned via a bonded courier or as otherwise directed by PacifiCorp. If the hardware or removable media containing PacifiCorp Data is owned by Seller or a third-party, a written statement detailing the destruction method used and the data sets involved, the date of destruction and the person who performed the destruction will be sent to a designated PacifiCorp security representative within fifteen (15) days following expiration of the term of the Contract, or at any time upon PacifiCorp's request. Seller's destruction or erasure of PacifiCorp Data pursuant to this subsection must be in compliance with NIST or ISO Standards.

b. Prior to the expected expiration or termination of the Contract by either Party for any reason, including by means of a default under the Contract, Seller agrees to provide PacifiCorp with the reasonable assistance services requested by PacifiCorp. As may be applicable, these services will include, at a minimum, converting Data, providing parallel services until PacifiCorp has transitioned to a new system, providing on-site technical support, cooperating with PacifiCorp or its designated vendor in developing required interfaces, and such other assistance services as will be necessary or appropriate. The Parties agree that such assistance services may extend beyond the term of the Contract as reasonably required by PacifiCorp.

7. PROHIBITED VENDORS

a. Seller may not use in the provision of the products and services to PacifiCorp under the Contract, whether directly or indirectly using subcontractors, the services, products, component pieces or sub-assemblies of any company identified by the U.S. Government and/or regulatory authorities as a security threat (collectively, the "Prohibited Vendors"), including without limitation the companies identified below and by the U.S. Department of Commerce (which are currently posted on the internet at https://www.bis.doc.gov/index.php/regulations/export-administration-

regulations-ear and as published in 15 CFR, Subchapter C, part 744, Supplement No. 4). Seller is responsible for being familiar with the Prohibited Vendors, including additional Prohibited Vendors that the U.S. Government may identify prior to the later of (i) the date that is sixty (60) days prior to delivery of the applicable item to the site, and (ii) the date such item clears U.S. Customs. If Seller fails to abide by the requirements of this Section, PacifiCorp will provide Seller with notice and an opportunity to cure within thirty (30) days of such notice. Continued failure to abide by this requirement will be considered a material breach of the Contract, entitling Seller to the remedies for material breach as set forth in the Contract.

Prohibited Vendors List

AO Kaspersky Lab

Da Jiang Innovations (DJI)

Dahua Technology Company

Hangzhou Hikvision Digital Technology Company

Huawei Technologies Co. Inc.

Hytera Communications Corporation

ZTE Corporation

Xinjiang Production and Construction Corps

Dago New Energy Corporation

GCL-Poly Energy Holdings Ltd

Xinte Energy Company

East Hope Group

Sieyuan Electric Co., Ltd

Risen Energy America, Inc.

Trina Solar

HT Solar Enerji Anonim Sirketi

Solar City (subsidiary of Tesla)

Xinjiang Uyghur Autonomous Region, China

48th Research Institute of China Electronics Technology Group Corporation (CETC)

Beijing Zhongkexin Electronics Equipment Co., Ltd.

Hunan Red Solar New Energy Science and Technology Co., Ltd.

Hunan Red Solar Photoelectricity Science and Technology Co., Ltd.

All companies listed in the Uyghur Forced Labor Prevention Act Entity List that provide hardware, software or services covered by Section 2(a) of this Exhibit S

b. Seller warrants that Seller will not use in its supply-chain for the provision of the products and services to PacifiCorp contemplated within the Contract, whether directly or indirectly using subcontractors, subsidiaries, parents, or affiliates, any product that was mined, produced or manufactured wholly or in part in the vendor regions identified by the U.S. Government and/or regulatory authorities as a prohibited (collectively, the "Prohibited Vendor Regions"), including without limitation the regions controlled by foreign adversaries identified in 15 CFR 7.4 - Determination of Foreign Adversaries. Seller is responsible for being familiar with the Prohibited Vendor Regions, including additional Prohibited Vendor Regions that the U.S. Government may identify prior to the later of (i) the date that is sixty (60) days prior to delivery of the applicable item to the site, and (ii) the date such item clears U.S. Customs. If Seller fails to abide by the requirements of this Section, PacifiCorp will provide Seller with notice of non-compliance and a 30-day opportunity to cure. Continued failure to abide by this requirement will be considered a material breach of the Contract, entitling Seller to the remedies for material breach as set forth in the Contract. The foregoing provision does not apply to Seller's provision of services that involve transportation and logistics (e.g., motor vehicles, packaging, etc.), office supplies (e.g., furniture, pens, pencils, staples, uniforms, etc.), medical equipment or services (e.g., drugs and pharmaceutical products, personal protective equipment, etc.), or hardware and hand-held tools (e.g., screws, bolts, nails, hammers, screwdrivers, etc.).