APPENDIX S-1

PacifiCorp Cyber Security Requirements

As part of the notice of intent to bid process, PacifiCorp asks all bidders to review Appendix S-1 **PacifiCorp Cyber Security Requirements** and confirm compliance with, or provide a list of exceptions to, the requirements along with bidder's Appendix B-1 **Notice of Intent to Bid** due December 16, 2022.

PacifiCorp Cyber Security Requirements

1. Seller shall maintain security controls to protect the Company's networks, systems, software, Confidential Information, and Data no less rigorous than those set forth in the latest published version of ISO/IEC 27001 – Information Security Management Systems–Requirements and ISO/IEC 27002 – Code of Practice for International Security Management.

2. If providing a web portal or web service, Seller's web services shall use HTTPS/TLS version 1.2 or later for all content.

3. Seller shall encrypt all Company data while at rest as well as when in transit over the network.

4. Seller shall encrypt all Company-related file transfers at rest as well as when in transit over the network.

5. For responses above, Seller shall encrypt using NIST-approved algorithms and key lengths.

6. If Seller product or service allows for PacifiCorp login into Seller's systems, Seller shall support a federated single-sign-on (SSO) authentication for any PacifiCorp accounts, whether via web interface or mobile application. Seller must have the ability to support Azure Active Directory.

7. If Seller product or service allows for PacifiCorp login into systems, and Seller's product or service does not support federated single-sign-on (SSO) authentication, Seller shall support multi-factor authentication compliant with NIST SP 800 63-3 Authentication Assurance Level 2. Seller will provide documentation that supports compliance and describe supported authentication mechanisms.

8. Seller shall ensure that emails sent by the Seller or by any Seller service while under the Agreement to the Company originates from a domain(s) with a published Domain-based Message Authentication, Reporting and Conformance (DMARC) policy of "reject" and with a published Sender Policy Framework (SPF) policy consisting of valid senders and a "fail" directive (-all). If the optional DMARC "pct" directive is used, "pct" must be set to "100";

9. Seller shall ensure that email sent to the Company by Seller or by any Seller service while under the Agreement passes a Domain-based Message Authentication, Reporting and Conformance (DMARC) authentication check;

10. Seller shall ensure that email sent to the Company by Seller or by any Seller service while under the Agreement is signed by a DomainKeys Identified Mail (DKIM) 2048 bit key.

11. Seller shall ensure that email sent to the Company by Seller or by any Seller service while under the Agreement supports Transport Layer Security (TLS).

12. Upon request, Seller shall describe the process to disclose known vulnerabilities to the Company related to products or services provided as they pertain to the proposed service.

13. Upon request, Seller shall describe methods supplied to the Company to verify software integrity and authenticity for any software or patches provided by you as they pertain to the proposed service.

14. Upon request, Seller shall describe process for security event monitoring and notification/alert/response plans, including response to security incidents affecting the Company.

15. Seller shall notify the Company of a Security Incident, no later than 48 hours after discovery, to 515-281-2967 and GlobalSecurityOperations@brkenergy.com .

16. Seller shall coordinate responses to security incidents with the Company that pose a security risk to the Company.

17. Seller acknowledges that rights to any data provided by the Company shall remain exclusive property of the Company.

18. Seller shall not share data with third parties for unrelated commercial purposes, such as advertising or advertising-related purposes.

19. If remote access of any type will be required as part of the service, Seller shall fully describe requirements for remote access to the Company.

20. If remote access of any type will be required as part of the service, Seller shall conform to Company requirements for intermediate host methods for remote access, such as Citrix or Virtual Desktop,

21. If remote access of any type will be required as part of the service, and if a virtual private network is required, Seller shall terminate such remote access in a demilitarized zone network (DMZ). Seller shall not establish virtual private network connectivity to Company corporate networks, which shall be considered a prohibited activity.

22. If remote access of any type will be required as part of the service, Seller shall notify the Company when remote or on-site access is no longer needed by Seller representatives, where applicable.

23. Seller shall disclose facilities necessary to the bid product or service that is located outside the continental United States.

24. Seller shall disclose support staff used during the term of this Agreement located outside the continental United States.

25. Seller shall disclose third parties codependent upon to deliver the Company offering (such as third-party software, implementation, hosting, for example).

26. Seller shall describe methods to securely ship and deliver products to the Company as they pertain to the proposed service.

For Hosted or Cloud Services:

27. If Seller's service is comprised in whole or in part of a cloud-based or hosted services solution, Seller shall undergo, or commit to undergo in a future state, annual Statement on Standards for Attestation Engagements (SSAE) Service Organization Control (SOC) 2 Type 2 audits for the enterprise or covering the applicable scope of services for the term of the Agreement with the Company, as appropriate. Note that a datacenter audit alone will not be sufficient. Seller shall include an audit for datacenter/colocation provider for informational purposes.

28. If Seller's service is comprised in whole or in part of a cloud-based or hosted services solution, Seller's administrative access shall comply with NIST SP 800 63-3 Digital Identity at Authentication Assurance Level 2 or higher, where compromise of one factor does not contribute to compromise of the other factor. Seller shall have the ability to provide compliance documentation and describe supported authentication mechanisms.

PacifiCorp Cyber Security Requirements

Bidder to Check One:

___ Bidder Agrees to PacifiCorp's Cyber Security Requirements

___ Bidder Has Provided a List of Exceptions to PacifiCorp's Cyber Security Requirements

List of Exceptions, if any:

Acknowledged by:

Signature: _____

Bidder Name: _____

Title: _____

Date: _____