Appendix 1
to Professional Services Contract

Special Conditions
Applicable to PacifiCorp
CIPS Covered Assets and Critical Infrastructure Information
NERC CIPS Requirements

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION (NERC)
CRITICAL INFRASTRUCTURE PROTECTION STANDARDS (CIPS)

Capitalized terms used herein shall have the same meaning as set forth in the Contract, unless the context may otherwise require.

Defined Terms:

The terms used in these Special Conditions applicable to PacifiCorp shall have the following meaning:

Company's Criteria shall mean applicable requirements used as the baseline for determining whether an individual is a restricted person, as set forth on Schedule 1, "Background Check Criteria."

Company's Facilities shall mean any facilities owned, operated or otherwise controlled by Company, which require Company authorization to obtain access.

Critical Infrastructure Information shall mean information concerning CIPS Covered Assets that: (i) relates to the production, generation or transmission of energy; (ii) could be useful to a person planning an attack on critical infrastructure; and (iii) provides strategic information beyond the geographic location of the critical asset, and which is identified as Critical infrastructure Information by Company.

Sensitive Personnel shall mean all Personnel with authorized unescorted physical access or authorized cyber access to Company's CIPS Covered Assets.

Unescorted Personnel shall mean all Personnel with authorized unescorted physical access to Company's Facilities.

SECTION 1: ACCESS TO COMPANY'S FACILITIES

1.1 Requirements for Unescorted Personnel and Sensitive Personnel

Company shall specify in the Scope of Work whether or not the Work or Services under this Contract requires: (i) authorized unescorted physical access to Company's Facilities (*i.e.*, use of Unescorted Personnel); or (ii) authorized unescorted physical access or authorized cyber access to Company's CIPS Covered Assets (*i.e.*, use of Sensitive Personnel). For all Personnel who require such access, Consultant shall:

(a) Ensure that Unescorted Personnel and Sensitive Personnel have passed the background checks outlined in subsection 1.3(a) consistent with the Company's Background Check Criteria set forth on Schedule 1 prior to requesting unescorted physical access and/or cyber access to Company's Facilities and/or CIPS Covered Assets, as applicable;

(b) Ensure that Unescorted Personnel and Sensitive Personnel complete Company provided or approved initial CIPS compliance training prior to requesting unescorted physical access and/or cyber access to Company's Facilities and/or CIPS Covered Assets, as applicable;

(c) Ensure that Unescorted Personnel and Sensitive Personnel have passed Consultant's drug and alcohol exam and are in compliance with Consultant's substance abuse/drug and alcohol policy as outlined in Section 2; and

(d) Keep accurate and detailed documentation to confirm completion dates for background checks, all CIPS compliance training (initial and annual training, to the extent applicable), and drug tests, and certify to Company such documentation by completing a Contractor/Vendor Information Form, attached as Schedule 2 hereto, for each Unescorted Personnel or Sensitive Personnel.

Consultant shall not allow any Unescorted Personnel or Sensitive Personnel who have not met the foregoing requirements of this subsection 1.1 to perform Work or Services, unless Consultant has received prior written consent from Company.

1.2 Additional Access Requirements Specific to Sensitive Personnel

In addition to the access requirements outlined in subsection 1.1, with respect to all Sensitive Personnel, Consultant also shall:

(a) Ensure that Sensitive Personnel (and any Personnel with access to Critical Infrastructure Information) are informed of and comply with Company's Critical Infrastructure Information requirements contained in the Contract, including the additional requirements applicable to Critical Infrastructure Information set forth in Section 4 herein, and any confidentiality agreement previously executed by Consultant, if applicable;

(b) In addition to the initial CIPS compliance training requirement outlined in subsection 1.1(b), ensure that Sensitive Personnel complete Company provided or approved CIPS compliance training within Company's prescribed training window, and not less than on an annual basis; and

(c) Immediately report both (i) Sensitive Personnel terminations for cause and (ii) all other Sensitive Personnel terminations or changes in employment status for those who no longer require access, to the Company's Technology Resource Center (TRC). The TRC is available by calling either (503) 813-5555 or (801) 220-5555.

Consultant shall not allow any Sensitive Personnel who have not met the foregoing requirements of this subsection 1.2 to perform Work or Services, unless Consultant has received prior written consent from Company.

1.3 Personnel Screening/Background Check Requirements for Unescorted Personnel and Sensitive Personnel

For all Unescorted Personnel or Sensitive Personnel, the following requirements must be met by Consultant:

(a) Consultant shall conduct, at Consultant's cost and expense, the requisite background checks for the current and past countries of residence of all Unescorted Personnel and Sensitive Personnel consistent with the Company's Background Check Criteria set forth on Schedule 1. All background checks will be conducted in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements or other agreements, if any.

(b) Following the initial background check to obtain authorization for access, the background checks shall be updated no less frequently than every seven (7) years or upon request by Company, and shall, at a minimum, consist of a social security number identity verification and seven (7) year criminal background check, including all convictions for a crime punishable by imprisonment for a term exceeding one (1) year.

(c) Consultant shall ensure that each of the Unescorted Personnel and Sensitive Personnel sign an appropriate authorization form prior to background checks being conducted, acknowledging that the background check is being conducted, and authorizing the information obtained to be provided to Company.

(d) Company has the right to audit Consultant's records supporting each Contractor/Vendor Information Form, attached as Schedule 2, submitted to Company, including background check results, and to verify that the requisite background checks and drug tests were

performed consistent with Company's Background Check Criteria set forth on Schedule 1. Consultant shall provide Company with all requested records supporting Contractor/Vendor Information Forms within a reasonable time after receiving such request, and in the form requested by Company, but not longer than three (3) business days following the date of such request.

(e) For purposes of this Contract, a background check is considered valid pursuant to the Company's Background Check Criteria, set forth on Schedule 1, if it was completed within two (2) years prior to the date on which the Consultant signed a Contractor/Vendor Information Form for each Unescorted Personnel and Sensitive Personnel. Regardless of when performed, all background checks shall be documented pursuant to the requirements set forth in this subsection 1.3.

(f) In the event Company notifies Consultant of the impending expiration of the background check of any Unescorted Personnel or Sensitive Personnel, Consultant shall provide an updated Contractor/Vendor Information Form reflecting a refreshed background check within twenty (20) days of receipt of the notice, in order to avoid revocation of such person's access.

1.4 Consultant Designee

Consultant shall designate one person to be responsible for compliance with the requirements of this Section 1 and all reporting and inquiries (other than Sensitive Personnel terminations or changes in employment status) shall be made via e-mail to CIPS-Contracting@PacifiCorp.com. Sensitive Personnel terminations or changes in employment status should be reported to the TRC pursuant to subsection 1.2(c).

SECTION 3: ADDITIONAL REQUIREMENTS APPLICABLE TO CRITICAL INFRASTRUCTURE INFORMATION

Confidential Information of Company labeled as Critical Infrastructure Information shall be protected consistent with the following requirements: (a) Critical Infrastructure Information shall be protected at all times, either by appropriate storage or having it under the personal observation and control of a person authorized to receive it; (b) each person who works with protected Critical Infrastructure Information is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it; (c) reasonable steps shall be taken to minimize the risks of access to Critical Infrastructure Information by unauthorized personnel (when not in use, Critical Infrastructure Information shall be secured in a secure container, such as a locked desk, file cabinet or facility where security is provided); (d) documents or material containing Critical Infrastructure Information may be reproduced to the minimum extent necessary, consistent with the need to carry out the Work or Services, provided that the reproduced material is marked and protected in the same manner as the original material; (e) material containing Critical Infrastructure Information should be disposed of through secured shredding receptacles or other secured document destruction methods; (f) Critical Infrastructure Information shall be transmitted only by the following means: (i) hand delivery; (ii) United States first class, express, certified or registered mail, bonded courier, or through secure electronic means; (iii) e-mail with encrypted file (such as, WinZip with password) (the password should not be included in e-mail, but should be delivered by phone or in an unrelated e-mail not mentioning the document name; password-protected Microsoft Office documents do not meet the encryption requirements); and (g) documents or material containing Critical Infrastructure Information shall be returned to Company or certified destroyed upon completion of the Work or Services.

Schedule 1

Special Conditions Applicable to PacifiCorp
Background Check Criteria

Company has a policy, "Badge and Access Standards," which outlines Company standards, procedures, compliance policies and workforce responsibilities regarding badges and access to all PacifiCorp controlled areas. Access to Company's Facilities is subject to this policy and requires access to be granted on an as-needed basis after completion of the required background check and training requirements.

In addition, the Company is required to comply with the mandatory Critical Infrastructure Protection Standards (CIPS) issued by the North American Electric Reliability Corporation (NERC) and approved by the Federal Energy Regulatory Commission on January 17, 2008. The CIPS were adopted to ensure that electric utilities, as part of the nation's critical infrastructure, are able to sustain and secure against vulnerabilities that may threaten the electric system and the utilities that operate it. Specifically, Standards CIP-001 through CIP-009 provide a cyber security framework for the identification and protection of assets critical to the reliable operation of the bulk electric system (*i.e.*, CIPS Covered Assets).

In order to ensure compliance with CIPS and the Company's access policy, Company requires that all Personnel who will have authorized unescorted physical access to Company's Facilities (*i.e.*, Unescorted Personnel) and/or authorized unescorted physical access or authorized cyber access to CIPS Covered Assets (including control centers, substations, generation plants, critical cyber assets, etc.) (*i.e.*, Sensitive Personnel) have the appropriate security clearance and security training. A background check of Consultant's Unescorted Personnel or Sensitive Personnel will be considered valid pursuant to these Criteria if it was completed within two (2) years prior to the date the Consultant signed a Contractor/Vendor Information Form for each such person.

Individuals who are considered "restricted persons" may not have unescorted access to Company's Facilities or CIPS Covered Assets. An individual will be considered a "restricted person" if the person meets any of the following criteria:

- Is currently under indictment for a crime punishable by imprisonment for a term exceeding one (1) year;
- Has been convicted (within the past seven (7) years) in any court of a crime punishable by imprisonment for a term exceeding one (1) year;
- Is currently a fugitive from justice; or
- Is an alien illegally or unlawfully in the United States.

If an individual's background check indicates that he/she meets any of the above criteria, the individual will be considered a "restricted person" and unescorted access to Company's Facilities or CIPS Covered Assets will not be authorized.

End of Schedule 1

Schedule 2

Special Conditions Applicable to PacifiCorp

Contractor / Vendor Information Form (CIF)

Contractor / Vendor Information

Company Name: _____
Address: _____
Phone: _____ Fax: _____

Contractor / Vendor Name: _____
(Include middle initial, if applicable: First, Middle, Last)

(1) Successfully Passed Employer's Drug and Alcohol Exam? Yes _____ No __
_____
Date Completed: _____
(Yes – mm/dd/yyyy)

(2) Successfully Passed Employer's Background Check? Yes _____ No___
_____
Date Completed: _____
(Yes – mm/dd/yyyy)

(3) Successfully Completed PacifiCorp's Security trainings? Yes _____ No___
_____
Date Completed: _____
(Yes – mm/dd/yyyy)

I hereby certify that the information provided regarding the Contractor / Vendor is accurate and documentation to support this information will be retained by Contractor / Vendor employer and provided upon Company's request

_____ _____
Manager Signature of Contractor / Vendor Employer *Date*

PacifiCorp Approvals

_____ _____
Signature of PacifiCorp Hiring Manager *Date*

_____
Printed Name of PacifiCorp Hiring Manager

If Contractor / Vendor did not pass the Background Check or Drug and Alcohol Exam, but an exception is requested provide reason for exception:

_____

_____ _____

Accepted by PacifiCorp Chief Compliance Officer *Date*

Contractor / Vendor will not be permitted access to Company controlled areas without the completion of Drug/Alcohol, Background verifications and completion of security training. Send the completed form electronically to Corporate Physical Security at "_Access Administrators" (accessadmins@pacificorp.com) for ID badge issuance. The form may be attached to a request for physical access.

End of Schedule 2