California Independent System Operator Corporation

Protected Data (Market Modeling Data & Intertie Flow Information*)
Non-Disclosure Agreement and Application Access Request Submission Instructions

Eligible entities must enter into the Protected Data Non-Disclosure Agreement (MMD NDA) to gain access to the ISO's market modeling data application, which includes market modeling data and intertie flow information* (see Exhibit B for eligibility requirements). This document contains instructions for: **(1)** entering into a *new* MMD NDA, **(2)** establishing a User Access Administrator (UAA), **(3)** requesting application access, and **(4)** adding/removing users under an *existing* MMD NDA.

*** PLEASE NOTE:** For access to Intertie Flow Information, in addition to the ISO's MMD NDA, eligible entities must be signatories to the Western Interconnection Data Sharing Agreement.

(1) Entering into a new Non-Disclosure Agreement

MMD NDA format and signature:

- The MMD **NDA date space at the top of page 1 must be left blank**. The ISO will fill in the effective date upon ISO execution of the agreement. The full legal name of the entity must be typed or written clearly. Please do not use abbreviations or acronyms.
- Contact information for the Requesting Entity's contact for notices must be typed or written clearly on page 3 of the MMD NDA.
- The MMD NDA must be signed and dated by **an individual who is authorized to enter the entity into an agreement** (generally a Director or above).

Exhibit A:

An Exhibit A must be completed and signed by each individual employee of the Requesting Entity who is seeking access to the application.

- The MMD **NDA date space must be left blank**. The ISO will fill in the effective date of the agreement upon ISO execution.
- The employee's name, employer, contact information, and signature date must be typed or written clearly. Failure to provide all requested information will result in processing delays.

Exhibit B:

An Exhibit B must be completed in its entirety by the Requesting Entity to facilitate the ISO's confirmation of the Requesting Entity's identity and eligibility, and provide a statement of need for the confidential data.

- The MMD **NDA date space must be left blank**. The ISO will fill in the effective date of the agreement upon ISO execution.
- Exhibit B must be signed and dated by an individual who is authorized to enter the entity into an agreement.

Exhibit C:

An Exhibit C must be completed in its entirety by the Requesting Entity **if the entity is a Consulting Entity**.

- The MMD **NDA date space must be left blank**. The ISO will fill in the effective date of the agreement upon ISO execution.
- Consulting Entities are eligible only to the extent that they provide consultancy services to an eligible entity. Exhibit C must disclose the **full name** of each eligible entity to which the Consulting Entity is providing consultancy services. **Each eligible entity must also enter into the MMD NDA**.

- Exhibit C must be signed and dated by an individual who is authorized to enter the entity into an agreement.

WECC Confidentiality Agreement:
If the Requesting Entity does not already have an approved WECC Confidentiality Agreement with WECC, the Requesting Entity must enter into the WECC Confidentiality Agreement. The form is attached to these instructions. Submit the completed form to CAISONDA@caiso.com for submission to WECC.

Please submit all completed and signed forms to:

California ISO, Legal Department
Email: CAISONDA@caiso.com

(2) Establishing a User Access Administrator

The Requesting Entity **must establish a User Access Administrator (UAA)** if the entity does not already have one. **ONLY** the UAA is authorized to submit a request for access on behalf of the entity. To establish a UAA, the Requesting Entity must read the UAA Requirements and complete and submit a UAA establishment form. Upon approval, the Requesting Entity's UAA will receive an email instructing them to register their new certificate, followed by a second email instructing them to download their certificate.

(3) Requesting Application Access

Once the MMD NDA has been approved, a UAA has been established, and the UAA has registered and downloaded their certificate, the UAA must complete and submit a request for access in AIM to either **(1)** market modeling data only, or **(2)** market modeling data and intertie flow information* for individuals who have executed an Exhibit A. Please note that it can take up to 10 business days for access to be provisioned. Additional instructions regarding access requests are located here. The Application Access web page is located here.

(4) Adding/Removing Users under an existing NDA

If a Requesting Entity has already entered into an MMD NDA:

- **To add an employee:** New users must read the existing MMD NDA and execute an Exhibit A. The Exhibit A (first paragraph) must **reference the effective date of the existing MMD NDA**. The UAA must then **(1)** submit the Exhibit A to caisonda@caiso.com for processing and approval; (2) upon approval, log in to the ISO's Access and Identity Management (AIM) application and create a new user, and **(3)** submit a request for access for the new user.
- **To remove an employee:** The UAA must **(1)** notify caisonda@caiso.com of the change; and **(2)** log in to the AIM application, click on the users tab, then click the profile button of the user and in the pop-up window press the revoke button. This will revoke all access the employee has to our systems, including the employee's certificates.

Confidentiality Agreement

Version 2.7

Requests for Non-Public Information should be submitted to and processed by WECC Administrative Services (support@wecc.org).

This WECC Confidentiality Agreement ("Agreement") is entered into by _____ ("Data Recipient") and is effective as of the date agreed to by Data Recipient. Data Recipient agrees to the following terms and conditions pertaining to Non-Public Information.

1. **Non-Public Information**
   a. Non-Public Information shall include any and all information Data Recipient receives from WECC, including, but not limited to, information received through a login to the WECC website, which:
      i. Is designated as "Confidential Information" or "Market Sensitive Information" or is otherwise considered non-public under the WECC Information Sharing Policy;
      ii. Meets the definition of Confidential Information as set forth in Section 1500 of the North American Electric Reliability Corporation Rules of Procedure; or
      iii. Is identified by WECC as non-public or confidential at the time of disclosure.
   b. For the purposes of this Agreement, Non-Public Information shall not include:
      i. Information that is or becomes available in the public domain through no fault or action of Data Recipient;
      ii. Information that was or is acquired by Data Recipient from a source other than WECC in a manner which is not otherwise subject to confidentiality restrictions; or
      iii. Information that was or is independently developed by Data Recipient as demonstrated by Data Recipient's documentation.
2. **Treatment of Non-Public Information**
   a. Data Recipient agrees to keep the Non-Public Information in a secure place in a manner that would prevent any unauthorized access to it and to take all other reasonable precautions to maintain the confidentiality of the Non-Public Information and to prevent unauthorized access to it.
      i. **Artificial Intelligence** – Data Recipient agrees not to use Nonpublic Information in connection with any artificial intelligence (AI) system or tool in such a way that could violate the nondisclosure terms of this Agreement, including, but not limited to, entering Nonpublic Information into any AI systems or tools that could result in the Nonpublic Information becoming available publicly or to third parties.
   b. Data Recipient agrees to not make available, disclose, provide or communicate Non-Public Information to any entity or individual, except:
      i. Employees of Data Recipient who (1) have signed a copy or an acknowledgment of this Agreement or a nondisclosure agreement that covers the Non-Public Information and is at least as restrictive as this Agreement, and (2) need the Non-Public Information for performance of a job function, subject to the limitation on Market Sensitive Information below;

ii. Contractors, consultants, lawyers and other agents, advisors, or representatives ("Representatives") of Data Recipient who (1) have signed a nondisclosure agreement that covers the Non-Public Information and is at least as restrictive as this Agreement, and (2) need the Non-Public Information for the work or representation being performed subject to the limitation on Market Sensitive Information below. In the event Data Recipient shares Non-Public Information with a Representative pursuant to this provision, Data Recipient agrees to be responsible and jointly and severally liable for any breach of confidentiality by that Representative;

iii. As required by FERC orders, rules or regulations, provided that additional data recipients have signed a nondisclosure agreement that covers the Non-Public Information and is at least as restrictive as this Agreement; or

iv. As may be otherwise agreed to by WECC in writing.

3. Market Sensitive Information

a. Data Recipient agrees not to provide or disclose any Market Sensitive Information as identified in the WECC Information Sharing Policy to any person who is (1) a Market Function Employee as defined by the FERC Standards of Conduct, or (2) actively and personally engaged in day-to-day sales of electric power or other electric power marketing functions.

4. Compelled Disclosures

a. Notwithstanding anything to the contrary herein, Data Recipient may disclose Non-Public Information to a governmental authority as required by law, provided that to the extent permitted by law:

i. Data Recipient notifies WECC as soon as reasonably possible of the required disclosure;

ii. Data Recipient does not disclose the Non-Public Information until WECC has had a reasonable opportunity to respond to the required disclosure; and

iii. Data Recipient cooperates with WECC as reasonably requested by WECC to protect WECC's interests in the Non-Public Information.

b. If Data Recipient is an entity subject to state or federal freedom of information laws or an employee of such an entity, Data Recipient represents to WECC that Data Recipient believes the Non-Public Information is eligible for restriction from public disclosure and agrees to:

i. Make all reasonable attempts to restrict the Non-Public Information from public disclosure;

ii. Notify WECC as soon as reasonably possible of any request for the Non-Public Information;

iii. Not disclose the Non-Public Information until WECC has had a reasonable opportunity to respond to the request, except as may otherwise be required by law; and

iv. Cooperate with WECC as reasonably requested by WECC to protect WECC's interests in the Non-Public Information.

5. Disclaimer and Limitations

a. Neither WECC nor any owner or submitter of the Non-Public Information makes any representation or warranty as to the completeness, accuracy, relevance, or usability of the Non-Public Information. All Non-Public Information made available to Data Recipient is made available AS IS AND WITHOUT WARRANTY, EXPRESS OR IMPLIED.

b. There is no obligation on the part of WECC or any owner or submitter of the Non-Public Information to supplement, update, or correct any Non-Public Information, even if the Non-Public Information is supplemented, updated, or corrected for other purposes.

c. Use of the Non-Public Information is at Data Recipient's own risk. Neither WECC nor the owner or submitter of the Non-Public Information shall be liable for any damages arising out of the use of the Non-Public Information.

6. Changes in Employment

a. If at any time during the term of this Agreement Data Recipient or an employee of Data Recipient with access to Non-Public Information ceases to be employed by his or her then current employer, Data Recipient agrees to notify WECC within five (5) business days of the change in employment.

b. If at any time during the term of this Agreement Data Recipient or an employee of Data Recipient has a change in job responsibilities such that Data Recipient or an employee of Data Recipient becomes a Market Function Employee, Data Recipient agrees to ensure that Data Recipient or such an employee of Data Recipient discontinues accessing or using any Market Sensitive Information as identified in the WECC Information Sharing Policy.

7. Term and Termination

a. This Agreement shall continue in effect until terminated. This Agreement may be terminated by WECC or Data Recipient at any time at their sole discretion.

b. Upon any termination of this Agreement, Data Recipient shall return to WECC all Non-Public Information in Data Recipient's possession or destroy all Non-Public Information in Data Recipient's possession and certify to WECC in writing that all Non-Public Information has been returned or destroyed, except as may be stored as a result of automated backup procedures or as may be otherwise required by law, in which case the confidentiality obligations of this Agreement shall survive termination.

8. Procedures for Breach or Loss of Non-Public Information

a. In the event that Data Recipient discloses (without WECC's prior written consent or as otherwise provided herein) or becomes aware that it has experienced a security breach, unauthorized data disclosure, or data loss with respect to any Non-Public Information ("Security Event"), then Data Recipient shall as soon as reasonably possible: (i) use reasonable best efforts to mitigate the Security Event, (ii) notify WECC in writing of (to the extent known): (a) the nature of the Security Event; (b) the Non-Public Information relating to the Security Event; (c) who caused the Security Event and who received access to the Non-Public Information as a result of the Security Event; (d) what Data Recipient has done or will do to mitigate any deleterious effect of the Security Event; and (e) what corrective action Data Recipient has taken or will take to prevent a further Security Event from occurring, and (iii) use reasonable best efforts to assist WECC in making applicable notifications related to the Security Event, including as required by applicable laws and regulations; provided that, the provision and timing of any notifications, if any, including content, will be in the sole discretion of and at the direction of WECC.

9. Miscellaneous Terms

a. This Agreement does not require WECC to disclose any Non-Public Information. Neither this Agreement nor any disclosure of Non-Public Information grant Data Recipient any intellectual

property rights or licenses to such information. Data Recipient agrees to comply with all applicable United States export laws and regulations.

b. This Agreement represents the entire understanding between WECC and Data Recipient related to the Non-Public Information and supersedes all previous communications between WECC and Data Recipient related to this subject. This Agreement can only be modified by written agreement executed by WECC and Data Recipient. Data Recipient may not delegate its duties or obligations under this Agreement without prior written consent from WECC. Any attempt to do so is void.

c. This Agreement shall be for the sole benefit of WECC and any owner or submitter of the Non-Public Information. This Agreement shall be fully enforceable by WECC and any entity whose Non-Public Information is not treated in accordance with this Agreement.

d. Data Recipient agrees that any material breach or attempted or threatened breach of this Agreement could result in irreparable injury to WECC for which damages would be an insufficient remedy. Accordingly, in such instances Data Recipient consents to injunctive relief without limiting the applicability of any other remedies.

e. If any term of this Agreement is held by a body of competent jurisdiction to be unenforceable, the remaining terms of this Agreement shall continue in full force and effect. In such an event, then in lieu of each term that is unenforceable, there will be added as part of this Agreement an enforceable term that is as similar as possible to the unenforceable term.

f. This Agreement shall be interpreted and enforced in accordance with the laws of the state of Utah, without regard to its conflict of law principles. The exclusive jurisdiction for any action to interpret or enforce this Agreement shall be brought in the courts located in Salt Lake County, Utah. Data Recipient hereby consents to the personal jurisdiction of such courts.

IN WITNESS HEREOF, Data Recipient has read and understands this Agreement and enters into this Agreement voluntarily, wishing to be legally bound.

Data Recipient

Signature: _____

Printed: _____

Company: _____

Title: _____

Date: _____

Email: _____

Please submit an executed copy to support@wecc.org.