Management of NEM connected plant models

December 2024

This explainer provides an overview of how AEMO manages models and related confidential information for National Electricity Market (NEM) connected plant, and addresses some frequently asked questions. It should be read in conjunction with the National Electricity Law (NEL) and the National Electricity Rules (NER), Power System Model Guidelines (PSMG) and other modelling requirements[1].

Please note: The information and processes described in this document may be updated or superseded after publication. This explainer is provided for general information purposes only, as at the time of publication, and does not constitute legal, business, engineering or technical advice. It should not be relied on as a substitute for professional advice on applicable laws, procedures and other instruments, in relation to your specific circumstances[2].

1. Data management overview

In performing its functions as the market and system operator for the NEM, AEMO has access to information that is protected under the NEL[4]. *Protected information* is defined as information which is given to AEMO in confidence, or provided in connection with AEMO's statutory functions and classified in the NER as *confidential information*.

AEMO deals with protected information in many areas of its work. Much of the information that AEMO needs to perform critical functions, including maintaining and planning a secure and reliable power system, is confidential. This includes equipment models and associated information relating to plant that is connected, or to be connected, to the NEM power system. Section 1.3 below contains more specific information about the handling of model information.

AEMO is only authorised to disclose protected information in the circumstances specified in the NEL[5]. Accordingly, protected information is classified by AEMO as 'Restricted', to ensure its use and disclosure is appropriately limited. Further information about data classification is provided in Section 1.1 below.

1.1. Data governance and classification

AEMO has data governance policies and processes in place to guard against unauthorised use or disclosure of protected information that AEMO holds. The classification of information collected will guide the measures AEMO implements to secure that data. All protected information is to be classified as Restricted, requiring the application of access restrictions and protocols specifying where the data can be stored and who can access it.

Periodic reviews are performed to confirm whether the current measures remain robust and appropriate to maintain the confidentiality, integrity and availability of data assets in accordance with the NEL and NER.

AEMO has a dedicated Data Governance function to support best practice in an ever-evolving technology landscape. Governance practices, tools, training, and support materials are tailored to support a culture geared towards managing data effectively in AEMO. This includes regular training to ensure staff are aware of their role in complying with AEMO's obligations, and regular forums with data owners and stewards across each data domain.

---

[1] https://aemo.com.au/energy-systems/electricity/national-electricity-market-nem/participate-in-the-market/network-connections/modelling-requirements

[2] Please also refer to the Disclaimer at the end of this document.

[4] Section 54(1) of the NEL

[5] Section 54A – 54H of the NEL

1.2. Cyber security

AEMO's Cyber Security function implements and operates controls designed to prevent and detect potential cyber incidents and data loss events. This function plays a major role in protecting the confidentiality, integrity and availability of data contained within AEMO systems. This is achieved with a comprehensive, forward-looking strategy and cyber program to continuously improve AEMO's control environment and implement contemporary and fit-for-purpose cyber security capabilities over time.

AEMO works closely with federal and state government partners to prioritise activities that address the most relevant scenarios and threats. AEMO takes a pragmatic approach, recognising that strong cyber security controls will not necessarily prevent all incidents. As such, AEMO has robust cyber incident response plans and playbooks, including a regular program of exercises. These exercises involve scenarios co-developed with government and security agencies to be relevant to AEMO based on threat intelligence and potential risk to our critical systems and data.

1.3. Requirements for connected plant model information

In specified circumstances, the NER require NEM participants to provide models and other confidential information to AEMO and network service providers (NSPs) about the behaviour, responses and capability of connected plant.

AEMO needs this information to be able to model power system behaviour on an ongoing basis. Accurate and up to date models are critical to the maintenance of power system security and network planning and development.

In accordance with the NER, AEMO has published the PSMG to set out AEMO's requirements for the models and other information that must be provided to AEMO and NSPs in the circumstances required by the NER. The PSMG provides further detail on:

- Participant obligations to provide models and other information to AEMO (PSMG Section 2).
- AEMO's obligations to provide models and other information to Registered Participants (PSMG Section 7.4.1).
- Types of data and models AEMO will provide (PSMG Table 7).
- What AEMO considers reasonably required information (PSMG Section 7.4.2).
- NER confidentiality provisions that apply to models and other information (PSMG Section 7.4.3).

Although models and associated information are protected information, the NER requires AEMO to provide some of this information to designated recipients in specific circumstances. Those recipients are obliged to treat the information as confidential in accordance with the NER. One of these required disclosures is in response to requests for information reasonably required to carry out power system simulation studies for planning and operational purposes, including system strength impact assessments[3]. The model information that AEMO shares in response to these requests is primarily in the form of AEMO Modelling Platform (AMP) files and releasable user guides (RUGs). Requests for access to models and other information under these NER provisions are managed by AEMO's Network Modelling and Information team, as set out in the Policy on Provision of Network Data webpage[4].

For model information to be made available for release, the Onboarding and Connections engineer identifies relevant modelling files and checks that these are releasable. Following verification and approval by the relevant Onboarding and Connections Engineering Lead, the relevant model information is uploaded to AEMO's releasable model repository, which is accessible to the Network Modelling and Information team.

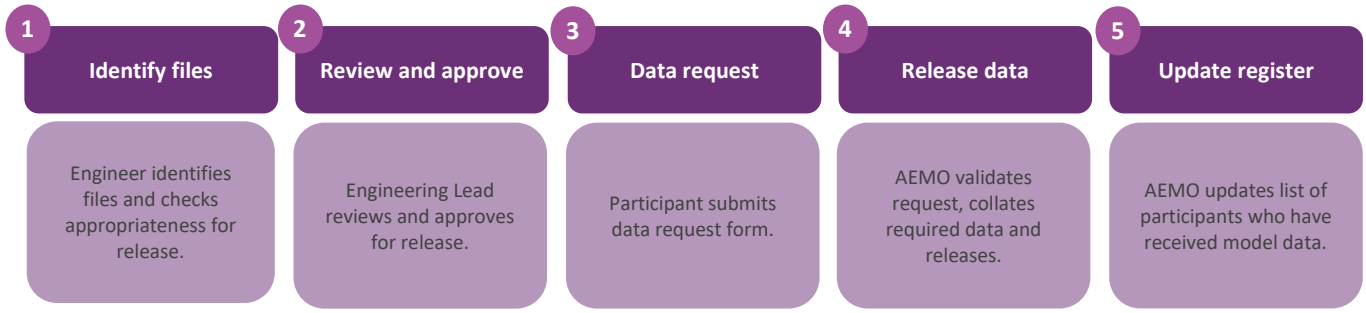
[3] For example, NER 3.13.3(l) and 4.6.6(e).

[4] https://aemo.com.au/en/energy-systems/electricity/national-electricity-market-nem/data-nem/network-data/policy-on-provision-of-network-data

The Network Modelling and Information team keeps a record of all participants to whom model information has been provided. This record is updated monthly and published on AEMO's website.

A high level overview of the process for releasing model data is set out in the below figure.

Figure 1 Model information release process



1.4. AEMO consultants

AEMO leverages external resources to support business needs and provide expert advice. These resources can be engaged as either an embedded consultant or an external consultant, and may access protected information if their role requires it to deliver an AEMO function.

An embedded consultant is a resource engaged for a defined period with a broad scope of work, operating alongside AEMO employees. An embedded consultant undertakes work using AEMO system accounts and hardware and is subject to the same obligations as an AEMO employee when accessing or handling protected information.

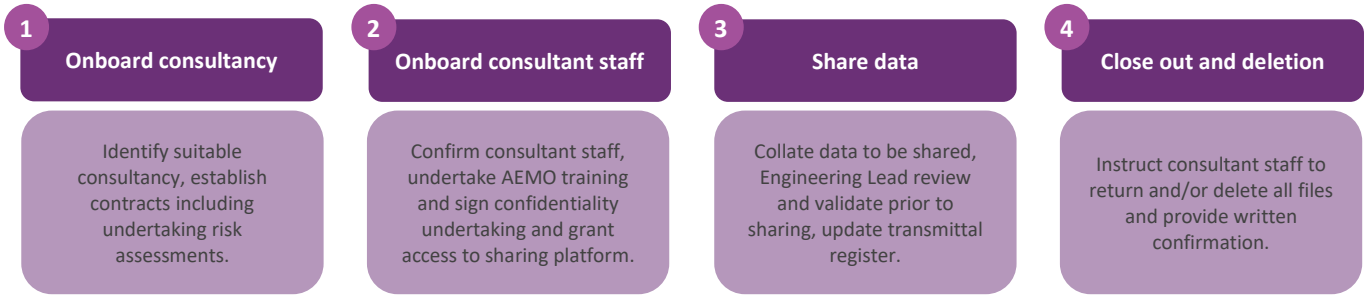
An external consultant is a resource engaged for a specific scope of work, and typically undertakes work outside of AEMO's digital and physical environment. Prior to commencing work, external consultants are onboarded to AEMO's systems (as required for their work) including completing relevant training, and must sign a confidentiality undertaking.

AEMO's standard terms for engaging consultants include strict confidentiality obligations when accessing or handling AEMO data, including protected information, consistent with AEMO's policies and its own obligations under the NEL and NER.

AEMO's internal process requires Onboarding and Connections project managers to log all information shared with external consultants. When the information is no longer required by the consultants to undertake work for AEMO, the relevant project manager must instruct the consultant to return and/or delete all copies of relevant files obtained during the course of their engagement, and obtain written confirmation that this action has been undertaken.

A high level overview of the process for engaging a consultant is set out in the below figure.

Figure 2 Consultant engagement process



2. Model management

Plant models, being protected information, are classified by AEMO as Restricted data, and accordingly AEMO maintains secure storage locations with restricted access, to protect the data from any unauthorised use or disclosure.

The processes for the provision of model information to NEM participants (where required by the NER), and for access by AEMO consultants, are outlined in Sections 1.3 and 1.4 respectively.

Access to plant models managed by Onboarding and Connections is restricted to designated user groups based on established use cases for each model type and status. Membership of those user groups requires justification of the need for access and management approval for both the data custodian and the person requesting access. This process involves identifying the authorised reason for access as part of the staff member's role and, if relevant, the specific model(s) that are being requested for that purpose. User access to these secure locations is reviewed on a quarterly basis.

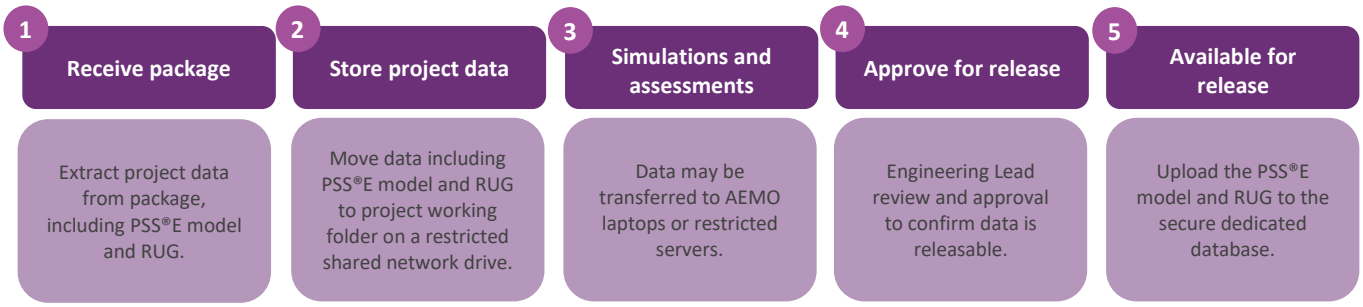
2.1. PSS®E model and Releasable User Guide (RUG)

On receipt of PSS®E models and associated RUGs for a proposed new or altered generating system, AEMO stores the data in a secure location on a restricted shared network drive. The models may be transferred to specific AEMO-issued laptops or restricted servers for the purposes of running simulations and assessments. All storage and working locations have access restricted to authorised AEMO staff and consultants requiring the models to perform their role.

Once the project becomes committed[5], and before the PSS®E model and RUG can be released, the data is reviewed and approved by an AEMO Onboarding and Connections Engineering Lead to confirm it is suitable for release, including ensuring the PSS®E model and RUG meet the release requirements set out in NER 3.13.3(l). The releasable PSS®E model and RUG are then uploaded to a secure database, that is accessible to relevant AEMO teams for operational and planning purposes, as well as for meeting AEMO's data provision obligations under NER 3.13.3(l). The model and RUG within this database are then updated as new iterations are provided throughout the connection process, and during commissioning and ongoing operation.

A high level overview of the process for handling PSS®E model data is set out in the below figure.

Figure 3 PSS®E model data handling



[5] In this context, a project is considered committed when the NSP notifies AEMO that a connection agreement has been entered into under NER 5.3.7(g).

2.2. PSCAD™/EMTDC™ model and RUG

On receipt of PSCAD™/EMTDC™ models and associated RUGs for a new/altered generating system, AEMO stores the data in a secure location on a restricted shared network drive, separate from PSS®E models, RUGs and other project data. Where a non-releasable version[6] of a PSCAD™/EMTDC™ model and RUG is provided, the files are labelled with relevant restrictions, for example "AEMO Only".

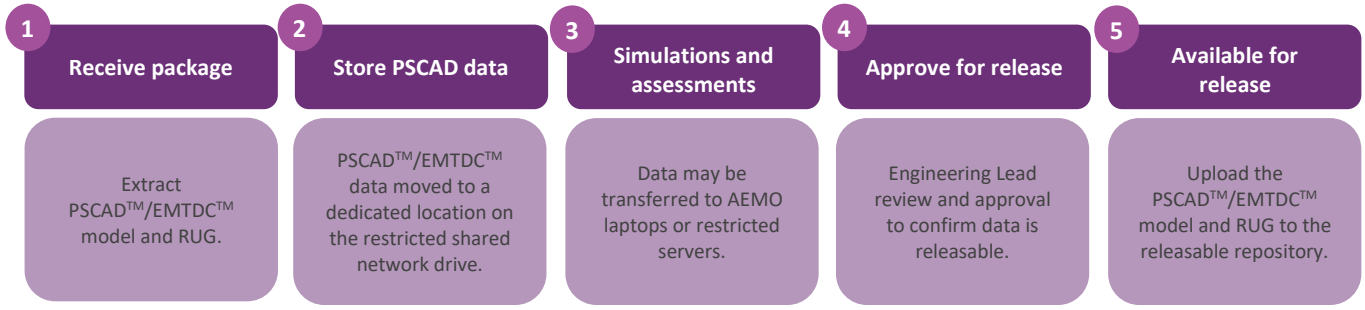
The models may be temporarily transferred to specific AEMO provided laptops or restricted servers for the purposes of running simulations and assessments. All storage and working locations have access restricted to a select group of authorised Onboarding and Connections staff and consultants who require the models to perform their role. Note that due to the nature of PSCAD™/EMTDC™ models and associated files, this select group with access is significantly limited in comparison to those provided with access to PSS®E model data.

Once the project becomes committed, and before the PSCAD™/EMTDC™ model and RUG can be released[7], the data is reviewed and approved by an AEMO Onboarding and Connections Engineering Lead to confirm it is suitable for release. The releasable PSCAD™/EMTDC™ model and RUG are then transferred to a releasable PSCAD™ repository on a restricted shared network drive, that is accessible to relevant AEMO teams for operational and planning purposes, as well as meeting AEMO's data provision obligations under NER 4.6.6(e) and NER 3.13.3 (l).

The models and RUGs within this repository are then updated as new iterations are provided throughout the connection process, and during commissioning and ongoing operation.

A high level overview of the process for handling PSCAD™/EMTDC™ model data is set out in the below figure.

Figure 4 PSCAD™/EMTDC™ model data handling



2.3. PSS®E model source code and block diagrams

AEMO's current process for submission of PSS®E model source code and block diagrams require the relevant participant or applicant (or the OEM on their behalf), to submit the required information to a dedicated mailbox (pssesourcecode@aemo.com.au). AEMO requests submitters to send PSS®E model source code and block diagrams **only to this dedicated mailbox**, not sent or copied to any other AEMO employee or mailbox.

Access to the mailbox is only accessible by two authorised AEMO employees, who are responsible for transferring the PSS®E model source code and the block diagrams to separate restricted locations, as further described below.

2.3.1. PSS®E model source code storage and access

PSS®E model source code is highly confidential, which is why ongoing access is restricted to just two authorised AEMO employees. The PSS®E model source code is stored in AEMO's secured repository.

---

[6] Note that a PSCAD™/EMTDC™ model and RUG that is releasable to NSPs is required to be provided by project proponents, and kept updated throughout the connection process and ongoing operation

[7] Made available for internal AEMO teams and releasable to NSPs.

There are circumstances in which other users may require access to specific model source code, that does not necessitate ongoing access to the full repository. As with all protected information, any further access to and use of source code is subject to detailed justification and manager approval. Where access to specific source code is authorised and approval is granted, strict policy requirements apply to its storage and use, including that the source code must:

- Not be copied to, stored on or synced with network drives, cloud services or any device that is not provided by AEMO.
- Not be shared with any unauthorised person.
- Be permanently deleted from any location other than the designated security repository as soon as work is completed, and provide email confirmation to the data custodian advising that all files have been deleted.

2.3.2. Block diagrams storage and access

Block diagrams are transferred from the restricted mailbox to a secure location on a shared network drive hosted on AEMO local servers. Ongoing access to this location is restricted to a small group of authorised Senior and Specialist employees at AEMO.

Again, further authorisation to access this information on a limited basis is subject to detailed justification identifying the authorised reason for the request. Approval from both the data custodian's accountable manager and the requestor's line manager are required.

3. Frequently asked questions

3.1. Is there a list of Registered Participants who have access to models?

AEMO publishes a list of registered participants (including project developers) to whom modelling information has been requested under NER 3.13.3 (k)(2) or NER 4.6.6(e) and provided[8] under NER 3.13.3(l). The types of modelling information AEMO provides are described in Sections 2.1 and 2.2 above.

This list is published in accordance with NER 3.13.3(p1) and is updated monthly, identifying the name of the recipient and the date information was provided.

3.2. What confidentiality provisions apply to Registered Participants that receive models from AEMO?

Where AEMO is required by the NER to disclose protected information to Registered Participants (including NSPs and other specified participants), they are in turn required to maintain confidentiality in accordance with their obligations in NER 8.6.

3.3 The connection process and associated provisions of the NER focus on protecting confidential information of Connection Applicants/Registered Participants. What provisions are in place to protect OEM models, in the case of an OEM providing model source code and block diagrams directly to AEMO?

AEMO's confidentiality obligations, as set out in Section 1.1 above, apply to *all* information provided to AEMO in confidence, and *all* information that is designated as confidential in the NEL or NER. AEMO currently accepts that OEMs may choose to provide model information on behalf of a Registered Participant or connection applicant for an identified project. AEMO's confidentiality obligations apply where the OEM discloses model information on behalf of the proponent.

[8] Available at https://aemo.com.au/en/energy-systems/electricity/national-electricity-market-nem/data-nem/network-data/policy-on-provision-of-network-data

3.3. Why does AEMO need source code and how is this data used?

AEMO requires access to PSS®E source code to maintain its core functions of managing connections and operations.

The primary use case for source code is to recompile models for later PSS®E software versions. Without source code, AEMO would be locked into a particular version of PSS®E which may become unsupported and superseded over time.

Although infrequent, there are instances when AEMO is required to debug issues through reading and adding debug code into the source code. For example, this may be required in circumstances where PSS®E crashes or issues appear only when a model is integrated into the PSS®E wide area network.

In addition, use of source code and block diagrams may be necessary to investigate operational grid events and non-compliances which are difficult to understand without this information.

3.4. Why does AEMO need block diagrams and how is this data used?

Block diagrams are key to understanding and resolving model issues in certain cases. Depending on coding style and coding standard, source code can be very difficult to interpret without block diagrams, especially if there are potential issues in the source code.

High-quality block diagrams are necessary to understand control logic and source code, identify signal flow and key variables, allow effective modelling problem resolution and to facilitate grid event investigation. It is common practice to understand a control system via block diagrams.

3.5. What process does AEMO follow in the event of an actual or suspected compliance incident?

AEMO implements an array of measures to monitor potential compliance incidents, including (but not limited to) self-reporting by employees, and audit programs.

In the event of potential non-compliance incident, AEMO follows established internal guidelines to identify the root cause, conduct an investigation, and implement corrective and preventative action to reduce the likelihood of an incident re-occurring. During the initial assessment, AEMO will consider if the compliance incident may be externally reportable and what reporting timeframes might apply.

The following diagram provides a general overview of the compliance incident response process.

Figure 5 Incident response process

Where can I find more information?

National Electricity Law	https://www.legislation.sa.gov.au/legislation/acts
National Electricity Rules	https://www.aemc.gov.au/regulation
Modelling Requirements (including Power System Model Guidelines)	https://aemo.com.au/energy-systems/electricity/national-electricity-market-nem/participate-in-the-market/network-connections/modelling-requirements

Version control

Date	Version	Changes
10/12/2024	1.0	First release

Disclaimer

AEMO has made reasonable efforts to ensure the quality of the information in this document but cannot guarantee its completeness.

The information in this document is current at the date of publication but may be subsequently updated or amended and is subject to changes made after this date to the laws, procedures and other instruments referred to in this document.

Accordingly, to the maximum extent permitted by law, AEMO and its officers, employees and consultants involved in the preparation of this document make no representation or warranty, express or implied, as to the currency, reliability or completeness of the information in this document.