Operations Division

SP-EA-1365 Model Confidentiality Management Policy

This Policy is part of the Engineering Assessment (EA) process within Transpower and forms part of the System Operator function. The document can be found in the Operational Documentation Library

Document Status:	**Being Reviewed**
Published Date	[Published Date]

Table of Contents

1 Purpose

Purpose and Objectives

This document sets out how the System Operator manages the storage, access control, and use of confidential power system models submitted for the operational, planning, security assessment and related purposes, GL-EA-716 and GL-EA-1311.

Confidential models include those that providers have explicitly designated as confidential at the time of submission, particularly where confidentiality is due to proprietary content, encryption, or commercial sensitivity.

This should be read in conjunction with the confidentiality obligations set out in the Electricity Industry Participation Code and any applicable confidentiality agreements between the System Operator and the model provider.

External Policy/ Rules & Regulations

Clause 3(2A) of Technical Code A of the EIPC code

Related Internal Policies, Processes and Procedures

The Operations Division's operational procedures are located in the Volt DM.

Operational Documentation (Published)

- GL-EA-716
- GL-EA-1311

Definitions

Descriptions of acronyms and non-standard or uncommon words specific to this document.

Definition	Description
EIPC	Electricity Industry Participation Code (the Code)
EMT	Electromagnetic Transient
PSCAD	Power Systems Computer Aided Design Software package used to conduct EMT type studies
TSAT	Transient Security Assessment Tool Software package used to conduct Realtime frequency studies
WECC	The Western Electricity Coordinating Council

2 Confidentiality Requirements

Storage

Providers of confidential models must submit them to the System Operator according to Appendix C and Appendix D of GL-EA-716 and GL-EA-1311.

The System Operator stores all received confidential models within internally managed secure server environments. These environments are designed to restrict unauthorised access and to protect confidentiality and integrity of the models.

Confidential models must not be removed from the secure server environment under any circumstances, except where required for approved backup, disaster recovery, or archival purposes consistent with the System Operator's internal security policies.

Ownership and intellectual property rights of all submitted models remain with the model provider. Custody of models by the System Operator does not imply any transfer of ownership or licensing rights beyond those necessary for the System Operator to perform its functions.

Access to Confidential Model Storage

Access to secured servers hosting confidential models is strictly controlled and granted on a need-to-know basis in line with security approval processes.

Access may be provided only to System Operator employees and System Operator-engaged contractors who have individual/designated confidential agreements with the System Operator which include network access, security and IT equipment permissions to perform approved operational, planning, or power system security assessment activities on behalf of the System Operator.

To obtain access, a user must:

- Submit a formal request to obtain access to secure server; and
- Submit a formal request to obtain file share access to gain visibility and access to confidential model repositories.

Access rights are granted only after approval and are subject to periodic review.

The System Operator maintains a register of users with access permission to confidential models. Model providers may request to view this register.

The System Operator maintains a register of users who have logged into the secure server and file share. Model providers may request to view this register.

Ownership and governance of the confidential model access group reside within the System Operator's Power Systems Group, which is responsible for approving, monitoring, and revoking access as appropriate.

Access to secure server and file share is removed from System Operator staff and engaged contractors at the end of their employment or contract with the System Operator.

Use and Sharing of Models

Confidential models are used solely for purposes consistent with the System Operator's operational, planning, and security assessment functions.

The System Operator applies different requirements for the use and sharing of models within its environment, depending on model type. Typical use and sharing arrangements are summarised below:

Sr No	Model Type	Sharing Arrangement
1.	PSCAD - encrypted	Not shared outside the secure server.
2.	PowerFactory – unencrypted	Not shared outside the secure server.
3.	PowerFactory - encrypted	Not shared outside the secure server, unless explicitly agreed*
4.	TSAT - encrypted/unencrypted	Stored and utilised within the real-time SCADA advanced applications and operational environments as required by the System Operator.
5.	Generic (e.g. WECC)	Shared openly as part of *Electricity Market Information*

* where model sharing is agreed with the model provider, the sharing will be limited to the minimum scope necessary for the intended purpose (e.g. an fault ride-through study). The sharing remains subject to applicable confidentiality agreement

3 Document Information

3.1 Copyright Information

3.2 Document Feedback

If you find an error in this document or wish to provide feedback about any improvements please submit feedback here or use the QR code.

3.3 Revision History

Link to document review survey https://forms.office.com/r/sYbiNMKMwY

SharePoint Revision	Date	Change	Section
1.0	15/06/2026	Initial issue	All new

3.4 Metadata

Document ID Information

Document ID number:	SP-EA-1365
Document Title:	SP-EA-1365 Model Confidentiality Management Policy
Document Type:	Policy
SharePoint Version:	V1
Document Status:	Being Reviewed
Severity of Consequences:	Moderate
Frequency of use	Daily
Level of Risk:	Choose an item.

DMS Structure

Macro-Process:	Engineering Assessment (EA)	
Process:		
Process Hierarchy:	*L1:* 01 Planning	*L2:* 02 Model System and Grid
	L3: 02-01 Manage Network Model	*L4:* [Business Model L4]
Document Complexity Rating (days)	[Time Reqd for Review (Duration Days)] days	

Document Control

Business Group Owner:	Power Systems Group		
Prepared by (Writer/Reviewer):	Snehalkumar Joshi		
Peer Reviewer	[Peer Reviewer]		
Approved by (Owner 1):	Click or tap here to enter text.		
Approved by (Owner 2):	Click or tap here to enter text.		
Approved by (Owner 3):	Click or tap here to enter text.		
Published Date: *(only changed by Doc Administrator)*	[Published Date]		
Update Type:	BAU Review		
Next Review Date:	Click or tap to enter a date.		
Review Period:	2 Years		
Primary User Group(s):	PSG		
Secondary User Group(s):	Click or tap here to enter text.		
Hardcopy Kept in:	[Control Room Folder/Section]		
To be published on TP Web site	true	Web Area:	Public SO