External Standard: Data Classification

CEOS1220.02i

This document is intended for External Entities and not internal Essential Energy use.

Refer to CEOS1220.02 Operational Standard: Data Classification for internal Essential Energy users.

If working from a printed copy of this document, check Policy Alerts and the Policy Library regularly for updates.

22 October 2026 – Original Issue
Approved By: General Manager of Digital Strategy, Architecture and Data
Next review date: October 2029

Essential Energy

CONTENTS

1.0 PURPOSE **3**
1.1 Audience **3**
1.2 Application **3**
1.3 Control Referencing Convention **3**
2.0 ACTIONS **4**
2.1 Data Classification **4**
2.2 Information Management Markers **4**
2.2.1 Retired Information Management Markers **6**
3.0 CONTROLS **6**
3.1 Participants and Service Providers **8**
4.0 AUTHORITIES AND RESPONSIBILITIES **11**
5.0 DEFINITIONS **11**
6.0 REFERENCES **15**
7.0 REVISIONS **15**

1.0 PURPOSE

This External Standard is a shortened version of the Essential Energy standard CEOS1220.02 Operational Standard: Data Classification, retaining only the content required and useful for External Entities. The purpose of this External Standard is to provide a reference list of data classifications, information management markers, associated labelling and the related data handling requirements to support agreements between Essential Energy (referred to as the Company or Essential Energy throughout this External Standard) and External Entities. Compliance with this External Standard is necessary to ensure Essential Energy data is handled appropriately to enable effective data protection in line with our regulatory and legislative obligations, and community expectations and is also an obligation to be performed by an External Entity under its agreement with Essential Energy (Agreement) in accordance with the terms of the Agreement.

1.1 Audience

This External Standard is intended for persons or entities external to Essential Energy that are recipients of data shared by or on behalf of Essential Energy. This includes but is not limited to contractors, consultants, connection applicants, customers, service providers, and other third-party entities (External Entities).

1.2 Application

This External Standard applies to all data created or handled by or on behalf of Essential Energy.

When data is shared with an External Entity, that External Entity is the Data Custodian for the data shared, and bears the responsibility to apply the controls in this External Standard along with any additional contractual or other controls that may apply to that data in accordance with the Agreement as applicable.

Note that this standard uses the term data rather than information or other related terms. Refer to the definition for data in section 5.0.

1.3 Control Referencing Convention

This External Standard uses the following control naming convention to facilitate referencing. Each control stipulates the criticality of the control by using the term ‘should’ where it is expected to be applied when reasonably practical, and ‘MUST’ where it is mandatory.

Figure 1: Control Reference Convention

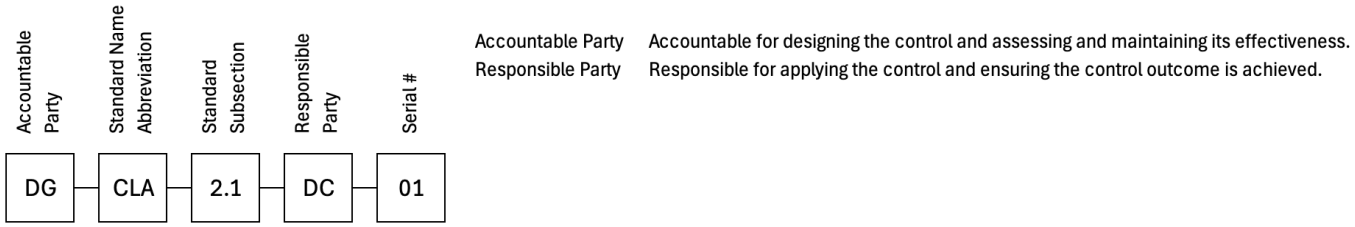


Table 1: Control Reference Convention Abbreviations

ABBREVIATION	DESCRIPTION
DG	Data Governance team
CLA	Classification

ABBREVIATION	DESCRIPTION
DC	Data Custodian

2.0 ACTIONS

2.1 Data Classification

The classifications shown in Table 2 below are in use by the Company and are based on the Australian Government Protective Security Policy Framework (PSPF).

Data Classification provides an easily recognisable risk sensitivity. Each classification has specific handling requirements outlined in section 3.0.

All data to which this External Standard applies will be subject to Data Classification. If any such data is not clearly classified when provided to an External Entity, the External Entity shall advise Essential Energy of this immediately. The absence of any Data Classification does not permit the External Entity to handle, store, disclose or otherwise use the data in any way.

Table 2: Data Classifications

CLASSIFICATION	DESCRIPTION
UNOFFICIAL	Data should be classified UNOFFICIAL when it does not form part of official duty, and would not realistically harm the Company, any individual or organisation if its confidentiality was compromised.
OFFICIAL	Data that is created, sent, or received as part of the Company's work, and that is not sensitive should be classified OFFICIAL. This information is an official record, and it provides evidence of what the Company has done and why.
OFFICIAL: SENSITIVE	Data that is OFFICIAL and is considered sensitive when compromise of its confidentiality may result in limited harm to the Company, organisations, government or individuals. (Note: this classification is substantially equivalent to the PSPF classification OFFICIAL: Sensitive, which may appear on some data)
PROTECTED	Data is considered PROTECTED if compromise of confidentiality would be expected to cause harm to the Company, organisations, government or individuals.

2.2 Information Management Markers

Information Management Markers (IMM's) provide a mechanism for explaining the context for the Data Classification. They assist users in applying appropriate handling controls and understanding specific legal, privacy, regulatory or business obligations associated with the information. Multiple IMM's may be applied to a document where applicable and where system limitations allow. If applying multiple IMM's is not possible the IMM representing the highest risk should be applied and additional IMM's manually applied. Applying an IMM is mandatory in some situations, but not all. Refer to Table 3 and Table 6 for specific requirements.

Table 3: Information Management Markers

IMM	DESCRIPTION
Commercially Sensitive	This IMM should be used where the nature of the data creates commercial risk, such as pricing, rates, tenders, procurement, contract negotiations, commercial strategies, supplier arrangements, or other information that could prejudice the Company's or a supplier's commercial interests if disclosed without authorisation.
Critical Infrastructure[1]	This IMM should be applied to data that includes Sensitive Operational Information[2] related to Essential Energy's Critical Infrastructure that presents a material risk to the function of the electricity network if the information's confidentiality is compromised. This IMM is only required where a reasonable person would consider the data is sensitive and should be kept confidential. This IMM should not be applied merely because data mentions an asset, location, supplier, purchase or routine activity associated with Essential Energy.
Legal Privilege	This IMM should be used if the information is subject to legal professional privilege, and compromise of the information's confidentiality is likely to cause at least limited harm to the national interest, organisations or individuals.
Legislative Secrecy	This IMM should be used where information is subject to confidentiality, secrecy or non-disclosure obligations under legislation, regulation, licence conditions, statutory instruments or enforceable regulatory requirements.
Load Data	This IMM MUST be applied to data that relates to the Company's Load Data, as defined in Table 8 (and in the CILC[3] Data Security clause B.3).
Operational Technology	This IMM MUST be applied to data that relates to the Company's Operational Technology Information, as defined in Table 8 (and in the CILC Data Security clause B.3).
Personal Privacy	This IMM MUST be used if the information is personal information as defined in the *Privacy Act 1988 (Cth)*. The classification applied should reflect the sensitivity, volume, context, identifiability and potential harm arising from unauthorised access, use or disclosure.
External Confidential	This IMM should be applied to data where the data source or obligation creates a confidentiality requirement, such as a Non-Disclosure Agreement, contract, supplier/customer confidentiality obligation, or external Originator marking where no more specific IMM applies.

[1] While data this IMM is applied to may also be Operational Technology Information or Load Data, this IMM should not be used to indicate that it is. Use IMM 'Load Data' and IMM 'Operational Technology' for this purpose.

[2] See Table 8 for definition

[3] CILC refers to the Critical Infrastructure Licence Conditions. Refer to the definitions in Table 8 for details.

2.2.1 Retired Information Management Markers

The Information Management Markers in Table 4 below are no longer to be used. They are included here for reference as they may have been applied to existing data before the date of this External Standard. The minimum data handling requirements below still apply to existing data these are applied to.

Table 4: Retired IMM's

RETIRED IMM	DESCRIPTION
Restricted: Security	This IMM may be found on some data/information but should not be applied in future. A more detailed IMM should be chosen instead.
Restricted: Licencing & Regulations	This IMM may be found on some data/information but should not be applied in future. A more detailed IMM should be chosen instead.

3.0 CONTROLS

Table 5 and Table 6 below articulate the controls required to be actioned in respect of data to which this External Standard applies (in accordance with section 1.2). The responsible entity for each control (as identified in the 'Responsible' column) must apply the control as set out in the 'Statement' column of Table 5 and Table 6.

Data classification and labelling are two separate processes. Classification is the process of determining the sensitivity, while labelling is applying the classification (and IMM if assigned) to the data.

All labels that contain a classification and IMM automatically require the minimum data handling control for the classification, as well as the additional requirements imposed by the IMM. If there is a control that overlaps with another control the more protective control will always take precedence (for example a classification control stating something *MUST* occur, and an IMM saying the same or similar thing *should* occur, then the control MUST occur).

Table 5: Classification and Labelling Controls

CONTROL REF ID	STATEMENT	RESPONSIBLE
OFFICIAL classification		
DG-CLA-2.1-DC-03b	Data classified as **OFFICIAL** should only be shared with those who are likely to require it (i.e. don't share it just because it doesn't have a higher classification).	Data Custodian
OFFICIAL: SENSITIVE classification		
DG-CLA-2.1-DC-04b	Data classified as **OFFICIAL: SENSITIVE** should have access restricted to those that require the information.	Data Custodian
DG-CLA-2.1-DC-04c	Data classified as **OFFICIAL: SENSITIVE** should have access time bound whenever feasible or reviewed regularly.	Data Custodian

CONTROL REF ID	STATEMENT	RESPONSIBLE
PROTECTED classification		
DG-CLA-2.1-DC-05b	Data classified as **PROTECTED** MUST have access strictly controlled to include only those that require the information.	Data Custodian
DG-CLA-2.1-DC-05c	Data classified as **PROTECTED** MUST have access time bound whenever feasible or reviewed regularly.	Data Custodian
General Controls – Classification, Labelling, Handling		
DG-CLA-2.1-DC-06	A classification or protective marking applied by an Originator external to the Company (ie an External Entity) MUST be retained and MUST NOT be removed, replaced or altered unless authorised by the Originator. Where required for internal control purposes, an Essential Energy classification may be recorded as additional metadata without obscuring the original marking.	Data Custodian
DG-CLA-2.1-DC-07	A classification and/or IMM label applied by someone internal to the Company MUST not be changed without authorisation from the Originator (or the relevant Domain Data Steward).	Data Custodian
DG-CLA-2.4-DC-10	Data must be handled such that it achieves the handling requirement based on the classification and IMM assigned.	Data Custodian

Table 6: Information Management Marker Controls

CONTROL REF ID	STATEMENT	RESPONSIBLE
DG-CLA-2.2-DC-01b	Data that is assigned the IMM **Commercially Sensitive** MUST be handled in accordance with all relevant contractual obligations.	Data Custodian
DG-CLA-2.2-DC-02b	Data assigned the IMM **Critical Infrastructure** should have access restricted to those who genuinely require it.	Data Custodian
DG-CLA-2.2-DC-02c	Data assigned the IMM **Critical Infrastructure** should be stored in Australia and not exported.	Data Custodian
DG-CLA-2.2-DC-04b	Data assigned the IMM Legislative Secrecy or subject to one or more legislative secrecy provisions MUST be restricted to authorised recipients. Data MUST not be used, disclosed, copied, forwarded or released unless authorised under the relevant legislation, and approved by the Data Custodian or Essential Energy Head of Risk and Compliance. Suspected unauthorised disclosure MUST be escalated immediately.	Data Custodian

CONTROL REF ID	STATEMENT	RESPONSIBLE
DG-CLA-2.2-DC-05b[4]	Data assigned the IMM **Load Data** or that meets the definition of Load Data in the CILC MUST be held solely within Australia (therefore must NOT be exported or stored overseas), however it may be accessed from overseas.	Data Custodian
DG-CLA-2.2-DC-05c[4]	Data assigned the IMM **Load Data** or that meets the definition of Load Data in the CILC MUST only be accessible by or disclosed to: • a Relevant Person, or • a person who has been authorised in writing by Essential Energy.	Data Custodian
DG-CLA-2.2-DC-06b[4]	Data assigned the IMM **Operational Technology** or that meets the definition of Operational Technology Information in the CILC MUST be held solely within Australia and accessed only from within Australia (therefore must NOT be exported, stored or accessed overseas).	Data Custodian
DG-CLA-2.2-DC-06c	Data assigned the IMM **Operational Technology** or that meets the definition of Operational Technology Information in the CILC MUST only be accessible by or disclosed to a Relevant Person who has also been authorised in writing by Essential Energy.	Data Custodian
DG-CLA-2.2-DC-07b	Data assigned the IMM **Personal Privacy** MUST be handled in accordance with the *Privacy Act 1988 (Cth)* and the Australian Privacy Principles, including taking reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure (APP 11[5]).	Data Custodian
DG-CLA-2.2-DC-08b	Data assigned the IMM **External Confidential** MUST have the related contractual requirements met.	Data Custodian

3.1 Participants and Service Providers

Where an External Entity is a Participant or Service Provider (as per Table 8) and the terms of its Agreement require the External Entity to protect shared data, the External Entity is permitted to do any of the following in respect of Operational Technology Information or Load Data where reasonably required in the following circumstances and for the following purposes only:

1. disclosing the information to the following persons to the extent necessary for them to provide services to the External Entity or an Associate:

[4] Essential Energy data recipients that meet the definition of Participant or Service Provider in Table 8: Definitions may be partially exempted from this requirement. Refer to section 3.1 Participants and Service Providers for details.

[5] See Australian Privacy Principles (APP), in particular APP 11

a. a financial, accounting, insurance, legal, regulatory or other adviser, or

b. auditors, insurers, security trustees and financiers (and each of their advisers),

2. disclosing the information to Participants, regulators, Commonwealth, State or Territory government agencies, and Service Providers in the electricity sector where disclosure of that information is:

   a. in the ordinary course of business,

   b. in accordance with best industry practice, and

   c. required by those persons to provide services or to perform functions, or

3. providing aggregated data that does not permit identification of any customer, Connection Points or a customer's demand characteristics,

provided that:

4. there is a legally binding agreement between the External Entity and their intended data sharing recipient (Data Sharing Agreement) which the External Entity agrees to enforce as directed by Essential Energy or as otherwise required for the External Entity to meet its obligations under the Agreement (including as set out in this External Standard),

5. the terms of the Data Sharing Agreement are no less restrictive than the terms of the Agreement with respect to Load Data and Operational Technology Information (subject to subparagraph 6), and

6. the Data Sharing Agreement prevents the data sharing recipient from further sharing the Load Data and Operational Technology Information without express written permission from Essential Energy,

then **the following Control Ref ID's** only may be varied as per Table 7. All other Control Ref ID's remain as per Table 6.

Table 7: CILC Participant and Service Provider control variations[6]

CONTROL REF ID	STATEMENT	RESPONSIBLE
DG-CLA-2.2-DC-05b	The statement for DG-CLA-2.2-DC-05b is replaced with: Data assigned the IMM **Load Data** or that meets the definition of Load Data in the CILC: - should be held solely within Australia (therefore should NOT be exported or stored overseas), however it may be accessed from overseas. If this is not feasible, then it; - should only be stored overseas for the time necessary to fulfill the function or service.	Data Custodian
DG-CLA-2.2-DC-05c	Not required when this clause 3.1 applies.	Data Custodian
DG-CLA-2.2-DC-06[b]	The statement for DG-CLA-2.2-DC-06b is replaced with: Data assigned the IMM **Operational Technology** or that meets the definition of Operational Technology Information in the CILC:	Data Custodian

[6] This table replaces only the listed Control Ref ID's from Table 6 when the conditions in clause 3.1 apply.

CONTROL REF ID	STATEMENT	RESPONSIBLE
	- should be held solely within Australia and accessed only from within Australia, therefore should NOT be exported, stored or accessed overseas. If this is not feasible, then it; - should be held solely within Australia and therefore should NOT be exported, or stored, but may be accessed overseas. If this is not feasible, then it; - should only be stored overseas for the time necessary to fulfill the function or service.	
DG-CLA-2.2-DC-06c	Not required when this clause 3.1 applies.	Data Custodian

4.0 AUTHORITIES AND RESPONSIBILITIES

POSITION / TITLE	RESPONSIBILITY
General Manager Digital Strategy Architecture and Data	Approving this external standard.
Manager Digital and Data Governance Risk and Compliance	Owns this external standard and is responsible for implementing, reviewing it so it remains up to date and effective, and assuring business awareness of this standard through training and communication. This document must be updated whenever CEOS1220.02 is updated and once approved it must be republished to the appropriate location to enable ongoing access for External Entities.
(External) Data Custodians	Handling data correctly, in compliance with this standard and relevant agreements.

5.0 DEFINITIONS

The definitions below assist with interpretation of this standard. Please follow the hyperlink for a term to view the definition in our corporate business Microsoft Purview, which is the master for terms within the Company.

Table 8: Definitions

TERM	DEFINITION
Associate	As that term is defined in the Critical Infrastructure Licence Conditions (CILC): has the same meaning given to that term in the *Corporations Act 2001* (Cth).
Carrier	As that term is defined in the Critical Infrastructure Licence Conditions (CILC): has the meaning given by the *Telecommunications (Interception and Access) Act 1979* (Cth).
CILC	See Critical Infrastructure Licence Conditions.
Connection Points	As that term is defined in the Critical Infrastructure Licence Conditions (CILC): means, in relation to the premises of a customer(s), the point of connection to an electrical installation supplying electricity to the premises as
Critical Infrastructure Licence Conditions	The Critical Infrastructure Licence Conditions (CILC) contained in Essential Energy's Distributor's Licence issued under the *Electricity Supply Act 1995* (NSW).
Data	A representation of facts, concepts, events, observations or instructions in a form suitable for communication, interpretation or processing by people or technology.

	Data may exist in structured, semi-structured or unstructured forms, and as text, numbers, graphics, images, sound or video.
Data Classification	The assessment and assignment of a classification to data according to its business value, criticality, sensitivity and applicable legal, regulatory or contractual obligations.
Data Custodian	A person or role responsible for managing and safeguarding data assets they directly control. They ensure that data is handled, stored, accessed, and shared securely and in accordance with relevant policies and directives.
Data Governance	The exercise of authority, control and shared decision making (planning, implementation, monitoring and enforcement) over the management of data assets.
Department	As that term is defined in the Critical Infrastructure Licence Conditions (CILC): means the Department of Climate Change, Energy, the Environment and Water.
Distribution System or System	As that term is defined in the Critical Infrastructure Licence Conditions (CILC): means the distribution system of which the Licence Holder is a network operator.
ICT Infrastructure	As that term is defined in the Critical Infrastructure Licence Conditions (CILC): means the information and communications technology equipment. systems, firmware and software directly supporting the Operational Technology environment used for the control of the supply of electricity.
Information	Data that has been organised, contextualised, interpreted or presented in a manner that provides meaning, supports understanding, or enables decision-making.
Information Management Marker	An additional label applied with a classification to identify why the data requires specific handling and any legal, regulatory, privacy, secrecy, privilege, operational or business requirements or restrictions that apply.
Licence Holder	Means Essential Energy.
Load Data	As that term is defined in the Critical Infrastructure Licence Conditions (CILC); means data as to the quantum of electricity delivered, both historical and current load demand from or to any one or more sites, or their Connection Points, which satisfies all of the following criteria: (a) it is not historical data older than 30 days, (b) it is not fault data, (c) it describes a location that allows a customer or Connection Point to be identified, (d) it describes the date and time of the data record, and

	(e) it describes the duration for which a quantum of electricity was delivered.
Operational Technology	As that term is defined in the Critical Infrastructure Licence Conditions (CILC); means technology that directly controls or monitors devices on the System, including: (a) the supervisory control and data acquisition (SCADA) master stations and management systems (where they have operational control functionality of the System) and other associated systems that directly control primary equipment on the System, and (b) the **ICT Infrastructure** used by the systems referred to in paragraph (a) to operate or monitor the devices these systems control.
Operational Technology Information	As that term is defined in the Critical Infrastructure Licence Conditions (CILC); means all information about the **Operational Technology** for example, design specifications and operating manuals.
Originator	Means the entity that initially generated the information. In most cases the Originator is the initial Data Custodian until the information is transferred to a different entity.
Participant	Means a participant in "the electricity sector" and includes: (a) an individual or entity who is registered by the AEMO (or who has been granted an exemption by the AEMO not to be registered) under the National Electricity Rules (NER) in any one or more of the categories listed in NER rules 2.2 to 2.7; or (b) an individual or entity (including any controlling entity) that can reasonably satisfy Essential Energy that it intends to carry out an activity that will result in a connection to the Distribution System. The AEMO website provides useful explanations of the National Electricity Market participant categories.
Relevant Person	As that term is defined in the Critical Infrastructure Licence Conditions (CILC): means: (a)the Licence Holder, (b) a network operator of the System, or (c) any person who is contracted or subcontracted, and approved, by the Licence Holder to work on the System.
Secure Data	As that term is defined in the Critical Infrastructure Licence Conditions (CILC): means: (a) Operational Technology Information; (b) Load Data relating to, or obtained in connection with, the operation of the System by a Relevant Person, and;

	(c) Third Party Data that the Licence Holder stores or processes indirectly because a Carrier or another person transferred the Third Party Data using the Licence Holder's infrastructure.
Sensitive Operational Information [7]	Sensitive Operational Information includes the following (and similar information): • diagrams, schematics, geospatial information, configuration information, operational constraints or tolerances; • protection settings and special protection schemes, telecommunications or network specifications, contingency arrangements, future network plans, or similar information; • connection details, NMI and premise data; • data identifying or assesses a hazard, vulnerability, critical dependency, material risk, control, incident, emergency arrangement or recovery arrangement; • documents how Essential Energy manages, tests, assures or demonstrates compliance with its critical infrastructure security and resilience obligations; that are related to Essential Energy's Critical Infrastructure and the ability of Essential Energy to maintain the supply of electricity.
Service Provider	In the context of the Critical Infrastructure Licence Conditions (CILC), "service provider" refers to a service provider in "the electricity sector" and includes an individual or entity that: a) provides services necessary for the design, construction, operation, management, maintenance, or augmentation of the Distribution System; or b) facilitates connections to the Distribution System. c) will (by the time it receives Secure Data) be contracted to provide a service that is relevant to Distribution System planning, operation, control, or maintenance
Third Party Data	As that term is defined in the Critical Infrastructure Licence Conditions (CILC): means: (a) communications, within the meaning of the *Telecommunications (Interception and Access) Act 1979* (Cth), and (b) closed-circuit television footage.

[7] This definition is intended to meet the requirements of the Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules (LIN 23/006) 2023 (Cth) (CIRMP Rules).

6.0 REFERENCES

INTERNAL
CEOS1220.02- Operational Standard: Data Classification

EXTERNAL
Distributor's Licence issued to Essential Energy under the Electricity Supply Act 1995 (NSW)
Privacy Act 1988 (Cth), and the Australian Privacy Principles
Security of Critical Infrastructure Act 2018 (Cth)
Protective Security Policy Framework

7.0 REVISIONS

ISSUE NO.	SECTION	DETAILS OF CHANGES IN THIS REVISION	CHANGE RISK IMPACT?