

Ausgrid 2018/19 Ring-fencing Compliance Report

31 OCTOBER 2019



Contents

1. Overview	3
2. Measures to ensure compliance.....	4
2.1 Compliance measures	4
2.2 Legal separation	5
2.2.1 Minor repairs.....	5
2.2.2 Cost Allocation Method	6
2.3 Functional separation	7
2.3.1 Discrimination.....	7
2.3.2 Physical separation / co-location	7
2.3.3 Staff sharing	8
2.4 Information and disclosure	8
3. Breaches	10
4. Other services	15
Appendix A – Compliance controls and measures	17
Appendix B – Summary of transactions with PLUS ES	29
Appendix C – Extract from Deloitte’s Ausgrid – Ring-fencing Guideline Compliance Report 1 November 2018	30
C1 Summary of findings.....	30

1. Overview

The Australian Energy Regulator (**AER**) released its latest version (v2) of the Ring-fencing Guideline – Electricity Distribution (**Guideline**) on 17 October 2017. The Guideline is made under clause 6.17.2 of the National Electricity Rules (**NER**) and is binding on all Distribution Network Service Providers (**DNSPs**).

Clause 6.2 of the Guideline requires each DNSP to prepare an annual ring-fencing compliance report each regulatory year. Ausgrid Operator Partnership (ABN 78 508 211 731) (**Ausgrid**) is a DNSP, and this document (**Report**) has been prepared in compliance with clause 6.2 of the Guideline and other applicable provisions.

The regulatory year for this Report is 1 July 2018 to 30 June 2019 (**FY19**).

Ausgrid notes that in April 2019, the AER published the Ausgrid Distribution Determination – 2019 to 2024 (**AER Final Determination**).

Ausgrid is also participating in the AER's current review of the Guideline.

The format and structure of the Report is in accordance with the Guideline's clause 6.2.1(b), in that its purpose is to identify and describe, in respect of FY19:

- i. the measures Ausgrid has taken to ensure compliance with the provisions of the Guideline;
- ii. any breaches of the Guideline by Ausgrid, or which otherwise relate to Ausgrid;
- iii. all other services provided by Ausgrid in accordance with clause 3.1 of the Guideline; and
- iv. [the purpose of] all transactions between Ausgrid and its affiliated entity, PLUS ES (ABN 30 179 420 673) (**PLUS ES**).

Clause 4.1.1 of the AER Electricity Distribution Ring-Fencing Guideline – Compliance reporting best practice manual Version 2 dated July 2019 requires meaningful compliance reporting. That is, the AER “*encourage[s] DNSPs to adhere to the following principles when writing their annual compliance reports:*

- *Report on specific measures, areas of the business, or challenges, rather than describing compliance measures in general, vague, or abstracted terms.*
- *Hone in reporting on areas of the business that carry greater risk of breaches of the Guideline or which have experienced breaches over the course of the regulatory year and focus reporting on those areas.*
- *Avoid jargon and technical language where possible and keep compliance reporting clear and as ‘plain English’ as possible.”*

This Report has been prepared having regard to these principles.

Capitalised terms that are not defined in this Report have the meaning given to those terms in the Guideline.

Nigel Lowry

General Counsel & Company Secretary

Email: nigel.lowry@ausgrid.com.au

2. Measures to ensure compliance

2.1 Compliance measures

Ausgrid adopts a comprehensive and pragmatic compliance program to ensure ring-fencing requirements are met.

This involves firstly, identifying and updating controls and measures for each obligation and disseminating them to relevant staff members, who are required to validate that the controls are in place and effective.

During FY19, Ausgrid enhanced its compliance program by increasing training and awareness and introducing greater controls. Appendix A of the Report provides a full set of controls and measures that Ausgrid has put in place to demonstrate compliance with the obligations of the Guideline.

The following sections of the Report provide a more detailed demonstration of Ausgrid's FY19 compliance controls and measures focusing on the following higher risk areas:

1. Legal Separation;
2. Functional Separation:
 - a. Discrimination;
 - b. Office sharing and staff sharing; and
3. Information access and disclosure.

The higher risk areas have been derived by keeping Ausgrid's values at the forefront, recognising the:

- comments provided in the *AER 2017-18 Annual Compliance Report (AER Report)* on the Electricity Distribution Ring-fencing Guideline dated 21 March 2019;

- "Extract from Deloitte's Ausgrid – Ring-fencing Guideline Compliance Report 1 November 2018";
- breaches of the Guideline which occurred as a result of related events from 1 January 2018 to 30 September 2018, which are described in more detail in Section 3 below (**September 2018 Incidents**); and
- subsequent recommendations provided by Ausgrid's external auditor KPMG following audits conducted on 14 December 2018 and 1 March 2019.

Ausgrid's Values

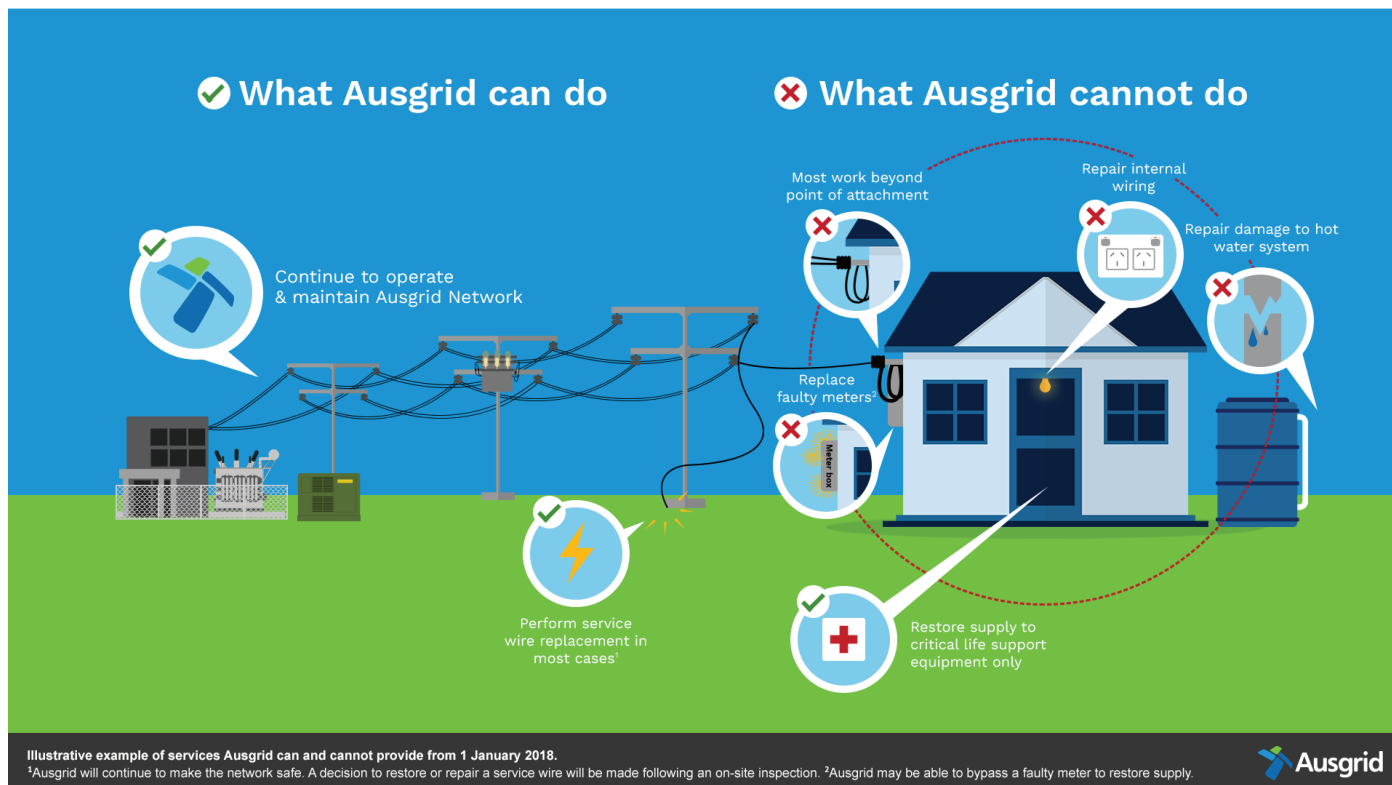
- Work safe, live safe
- Customer-focused
- Commercially minded
- Collaborative
- Honest and accountable
- Respect

2.2 Legal separation

Clause 3.1 of the Guideline permits Ausgrid to provide distribution services and transmission services but prohibits it from providing 'other services'. Accordingly, in order to legally separate distribution services and transmission services from other services, an affiliated entity of Ausgrid, PLUS ES, was created.

PLUS ES is defined in the Guideline as Ausgrid's 'Related Electricity Service Provider' (**RESP**) and unless the exceptions in clause 3.1(d) apply (outlined in Section 4), is the entity through which any 'other services' are provided. This approach is illustrated in **Figure 1**.

Figure 1: Legal Separation at Ausgrid



2.2.1 Minor repairs

As noted in Figure 1, Ausgrid will continue to make the network safe. Prior to the publication of AER Final Determination and up until March 2019, Ausgrid had been notifying the AER of instances where it did not adhere to clause 3.1(b) of the Guideline with respect to undertaking minor repairs for customers' premises for vulnerable customers (who would have otherwise lost power for Ausgrid to make the network safe). These instances are further detailed in Section 3.

As the AER Final Determination includes minor repairs (up to 30 minutes) as a 'common distribution service', since 1 July 2019 Ausgrid has and will continue to perform such work as business as usual (**BAU**), while ensuring that it complies with all obligations imposed by the Guideline.

Prior to undertaking any work, Ausgrid ensures that it follows due processes, including:

1. undertaking an assessment of when Ausgrid is authorised to perform the new distribution service 'rectification of simple customer fault'; and
2. maintaining appropriate record-keeping of the minor repairs performed.

Ausgrid is generally notified of a supply outage or incident at a customer's premises via our telephone contact centre. To ensure Ausgrid meets its duty of care from a safety perspective, such calls are dispatched to an Ausgrid Emergency Service Officer (**EmSO**). The EmSO attending the site/residence is trained to assess the hazards associated with such a situation and make it safe, if required. As the assessment can only be made on-site, the contact centre staff cannot always obtain sufficient information from the caller to discharge Ausgrid's duty of care.

As part of the EmSO assessment, Ausgrid:

- follows its:
 - *Field Services Guideline*, which outlines the circumstances in which the new 'rectification of simple customer fault' service can be offered (i.e. the need for rectification work is discovered in the course of the provision of distribution services, the work performed is the minimum required to restore safe supply, and the work can be performed in less than 30 minutes and does not normally require a second visit);
 - *Vulnerable Customer Protocol*, the purpose of which is to consider the appropriate response by Ausgrid field staff to requests for assistance from vulnerable customers who report full or partial loss of supply;
 - *Technical Guide T0100*, which is referred to by field, technical and engineering staff for minor works for vulnerable customers over 30 minutes or where a fault is determined to relate to a customer installation and Ausgrid is only permitted to carry out simple works to safely reinstate supply such as replacing service fuses or other minor works that can be completed within a 30 minute timeframe; and
 - *EmSO General Advice 39A, AER - Minor Restoration Works Service Classification*, which outlines the process to carry out repair works under 30 minutes for all customer faults in line with the AER's Final Determination for the Regulatory Period 2019-2024; and
- has established a feedback mechanism to obtain a customer's acknowledgment that Ausgrid was requested to provide the service and that no alternative was available to provide satisfactory restoration, given the vulnerability of the customer.

In Focus – Rectification of simple customer fault

An EmSO was dispatched to a partial supply job. Upon arrival, the EmSO found the Safety Switch (RCD) had tripped. The elderly customer advised that they had critical medication in the fridge and that their phone was not operating with the loss of power. Due to the customer's age, medication requirements, inability to leave the premises due to inclement weather, loss of phone/communication capability, and the customer's current state of distress, the Ausgrid EmSO assessed that the health of the customer was at risk.

The defective customer equipment was isolated and danger tagged. The RCD was reset by the EmSO to restore supply after confirming that there were no safety risks associated with re-energisation of the installation. The customer was advised to have the defective equipment inspected and repaired by a qualified electrical contractor. The EmSO advised the customer that this was not normal procedure as Ausgrid does not operate or replace private equipment.

2.2.2 Cost Allocation Method

Ausgrid maintains a clearly distinguishable cost allocation methodology (**CAM**) which attributes costs to either Ausgrid or PLUS ES. The CAM is AER-approved and has recently been reviewed by Ausgrid's Head of Internal Audit, who concluded that Ausgrid's CAM was compliant with the Guideline.

Ausgrid implemented controls to ensure that its CAM complies with the Guideline. These controls are implemented via a corporate services agreement (**CSA**) includes:

- using Ausgrid's accounting system, SAP, which identifies separate legal entities for the purposes of recording transactions between Ausgrid and PLUS ES;
- maintaining monthly journal transfer and reconciliation processes between Ausgrid and PLUS ES; and
- utilising dedicated Ausgrid accounting and finance personnel who ensure that the CAM meets the AER Cost Allocation Guideline, is pragmatically applied, and that the clear separation of accounts between Ausgrid and PLUS ES is maintained.

2.3 Functional separation

2.3.1 Discrimination

Ausgrid takes its obligations not to discriminate in favour of its affiliate seriously. This has been emphasised through specific training and the development of additional information resources, which are available to Ausgrid and PLUS ES staff via their respective intranet sites, displayed on-site (for example, physical posters) and building through efforts to build a ring-fencing compliance culture.

Ausgrid continues to establish new controls and improve existing controls to ensure there is functional separation between Ausgrid and PLUS ES, particularly with respect to physical separation and restricted staff sharing.

2.3.2 Physical separation/co-location

Ausgrid had established various controls in the previous regulatory year and it has further enhanced its ability to comply with clause 4.2.1 of the Guideline by implementing *Procedure – PLUS ES Accommodation and Security (the Separation Procedure)*. The Separation Procedure applies to all Ausgrid and PLUS ES staff, is adopted by Ausgrid's Strategic Property branch, and forms the basis for allocating offices to PLUS ES staff.

The primary focus of the Separation Procedure is to understand and manage the sites where Ausgrid and PLUS ES staff are co-located, specifically noting:

- where the Guideline provides for exceptions under clause 4.2.1(b)¹; and
- the risk level of the co-located sites. That is, certain co-located sites have nil or low risks due to there only being minimal shared amenities (which pose no greater risk of sharing of Electricity Information than other situations such as outside the building or on public transport).

¹ In such instances, Ausgrid maintains up-to-date registers on its website.

To monitor compliance with the Separation Procedure and therefore the Guideline, Ausgrid's Governance, Risk and Compliance team has initiated an analysis which forms a risk heatmap of perceived versus actual risks associated with co-located sites. This heatmap indicates the following:



Completely separated sites



Co-located sites to which Ausgrid has applied the exception under the Guideline



Co-located sites which do not apply the exception under the Guideline but:



- have access-controlled separated sections for core workspaces so they are not shared; and

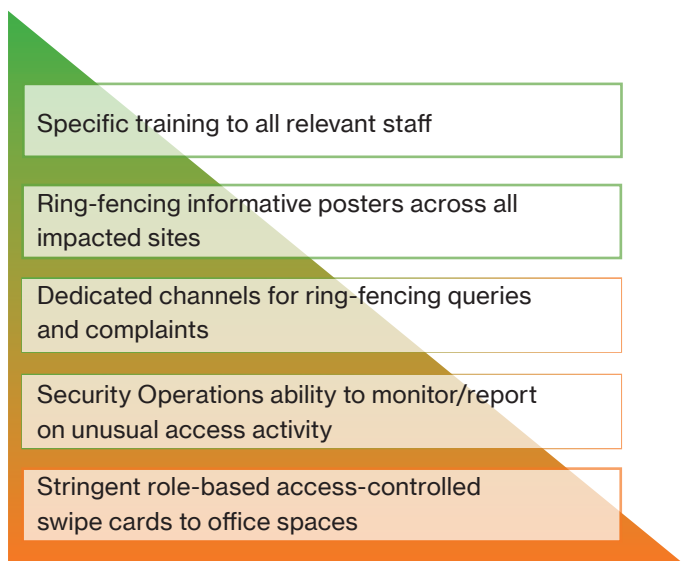


- do not have swipe access to meeting rooms and certain shared amenities such that staff from elsewhere in the building do have unescorted access to them



Only minimal shared amenities such as kitchens, bathrooms/showers, carparks 'from which' PLUS ES does not provide electricity services

Extra controls have been put in place to mitigate any perceived inherent risks. The overarching obligations not to disclose Confidential Information and not to discriminate in favour of PLUS ES are at the heart of the controls. These include:



Ausgrid maintains its office-sharing register in compliance with its obligations under the Guideline.

The above compliance enhancements have been made putting Ausgrid customers first and taking into consideration recommendations from relevant stakeholders such as the AER Report and recommendations from Ausgrid’s external auditor KPMG.

2.3.3 Staff sharing

Throughout FY19 Ausgrid has strengthened its compliance with clause 4.2.2 of the Guideline.

In addition to the controls detailed in Appendix A, Ausgrid’s People and Transformation division has established and now oversees the application of the *Procedure – Temporary supply of Ausgrid staff to PLUS ES (Staff Sharing Procedure)*. The Staff Sharing Procedure:

- adopts the obligations under clause 4.2.2 of the Guideline;
- tightens the process for Ausgrid staff to be shared with PLUS ES;
- identifies the criteria that must be met for Ausgrid staff to be shared with PLUS ES; and
- refers users to Ausgrid’s *Encouraging Competition Through Ring-fencing Policy* for a definition of ‘Electricity Information’ (which forms part of the criteria for staff to be shared with PLUS ES).

Ausgrid’s People and Transformation division apply the tests set out in the Staff Sharing Procedure (as prescribed in clause 4.2.2(b)) and only approve staff sharing arrangements that will comply with the Guideline.

Other controls and measures which have enhanced compliance in this area include:

- restrictions on short term secondments to a minimum;
- greater awareness via training and resource materials for Ausgrid staff on loan to PLUS ES;
- establishment of a process for assessing and changing each employee’s ‘office’ access requirements at the start and cessation of their on-loan arrangement, such as amended access rights on employee ID cards;
- thorough changeover of uniforms, badges, physical branded equipment at the start and cessation of the on-loan arrangements with mandatory PLUS ES magnetic stickers for Ausgrid personnel using their work vehicles whilst on loan; and
- role based security ICT access requirements at the start and cessation of the on-loan period.

These compliance tools also draw from comments and recommendations from the AER Report and the audit reports post the September 2018 Incidents (refer to Section 3). Ausgrid is therefore confident that compliance with this obligation has been achieved.

2.4 Information and disclosure

The obligation not to disclose Confidential Information is given high priority by Ausgrid as an organisation and as a DNSP. Ausgrid systems are in-built with cyber security and other protections which are strengthened by processes and procedures as further outlined in Appendix A.

The Guideline introduces further requirements on how confidential information can be shared, particularly with a distributor’s RESP.

During the first regulatory ring-fencing year, Ausgrid initiated a project with its ICT team to adopt the requirements under clause 4.3 of the Guideline. The aim was to implement new ICT protocols and procedures that only provide PLUS ES staff with access to specific Ausgrid systems where such access is necessary, namely:

- under the Corporate Services Agreements (i.e. for the provision of corporate services by Ausgrid to PLUS ES, for example, ICT, human resources, payroll and legal services); and
- for that staff member to perform their roles, functions or duties.

This involved the following steps:

- undertaking an analysis of which Ausgrid systems contain Confidential Information or electricity information (**affected systems**);
- further analysis of the affected systems to determine the circumstances in which Ausgrid could (in accordance with clause 4.3.3 of the Guideline) share such information with PLUS ES; and
- granting access to the roles which required access in accordance with clause 4.3.3 of the Guideline.

Throughout FY19, Ausgrid has further strengthened its systems and practices to comply with its information and disclosure obligations under the Guideline, including:

- for staff sharing arrangements, performing a role analysis in accordance with the relevant Staff Sharing Procedure (prior to the approval of any on loan arrangement);
- determining if the relevant staff member can be shared, conducting an analysis based on whether they have access to electricity information or an opportunity to use electricity information to discriminate in favour of PLUS ES. This assessment provides Ausgrid with the confidence that staff loaned to PLUS ES do not have access to Confidential Information unless required to under the role and in compliance with clause 4.3.3 of the Guideline;

- the publication of an updated tailored training video for PLUS ES staff, reminding them of their obligations under the Guideline;
- continual improvements to system access controls; and
- the introduction of a robust Data Loss Prevention solution by Ausgrid's Cyber Security team. This solution detects and responds when an end-user data exfiltration event occurs via email (both intentionally/unintentionally).

Along with the above controls, Ausgrid maintains an Information Register and Information Sharing Protocol on its website. The Information Sharing Protocol identifies when Confidential Information is requested and disclosed, who it can be provided to, the assessment made to disclose it, and the consequential steps if Ausgrid receives a request from any third parties to share such information as required under clause 4.3.4 of the Guideline. To date, Ausgrid has not received any such requests nor has it shared Confidential Information to PLUS ES which is not prescribed under clause 4.3.3 of the Guideline.



3. Breaches

Ausgrid has built a ring-fencing compliance management system (**CMS**) modelled on similar existing in-house CMS systems and established protocols for staff to report breaches of the Guideline via numerous channels. The requirement to report of breaches is advised via Ausgrid's *Encouraging Competition Through Ring-Fencing Policy* and has been reinforced by various communications and training programs.

Apart from intentional breaches per the Vulnerable Customer Protocol, Ausgrid has reported four breaches during FY19 to the AER in accordance with the Guideline, with all four breaches resulting from related events.

September 2018 incidents

Clause of Guideline breached	Breach date	Nature of breach
4.2.2	17/09/2018	An Ausgrid staff member assisted PLUS ES with contestable electricity services.
4.1 (b)	17/09/2018	Requests for contestable works came directly from external customers to an employee at Ausgrid, who then referred the request to PLUS ES exclusively.
3.2.2 (a, b)	17/09/2018	Ausgrid did not invoice PLUS ES for shared staff in a timely manner.
4.2.4	17/09/2018	Ausgrid did not include one staff member on its staff register.

In 2018, Ausgrid engaged KPMG to independently assess what management actions were required to prevent future breaches. In March 2019, KPMG provided an independent reasonable assurance confirming that all management actions arising from the previous review were completed.

Intentional breaches per Ausgrid's Vulnerable Customer Protocol

The following table identifies the reported breaches by Ausgrid following its Vulnerable Customer Protocol. In early March 2019, the AER sought Ausgrid's commitment to only provide rectification of simple customer faults where doing so would be in accordance with the scope of the service set out in the AER's draft decision. Following publication of the AER Final Determination, since 1 July 2019 Ausgrid has continued to provide the rectification of simple customer faults in accordance with the scope of the determination (and therefore, not in breach of the Guideline).

Clause of Guideline breached	Breach date	Nature of breach
3.1 (b)	1. 11/07/2018	Service fuse assembly was replaced, and supply was restored
3.1 (b)	2. 17/07/2018	Ausgrid staff carried out work on customer owner consumer mains to 'make safe' and to enable the restoration of supply to the premises, as the customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	3. 3/08/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	4. 25/08/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	5. 29/08/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the temporary restoration of full supply to the premises. The customer was assessed to be vulnerable under Ausgrid's protocol.
3.1 (b)	6. 10/09/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the temporary restoration of full supply to the premises.
3.1 (b)	7. 28/09/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	8. 10/10/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	9. 3/10/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	10. 12/10/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.

Clause of Guideline breached	Breach date	Nature of breach
3.1 (b)	11. 31/10/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	12. 2/11/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	13. 21/11/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	14. 25/11/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	15. 24/11/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	16. 29/11/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	17. 3/12/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	18. 4/12/2018	Ausgrid staff carried out minor work on a customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	19. 30/11/2018	Ausgrid staff provided an oil sample collection and coordinated the laboratory analysis services (via PLUS ES) to Sydney Trains.
3.1 (b)	20. 10/12/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.

Clause of Guideline breached	Breach date	Nature of breach
3.1 (b)	21. 11/12/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	22. 15/12/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	23. 23/12/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	24. 25/12/2018	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	25. 2/01/2019	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	26. 4/01/2019	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	27. 5/01/2019	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	28. 16/01/2019	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	29. 18/01/2019	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.

Clause of Guideline breached	Breach date	Nature of breach
3.1 (b)	30. 24/01/2019	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	31. 25/01/2019	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	32. 9/02/2019	Ausgrid staff carried out minor work on customer owned installation which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.
3.1 (b)	33. 10/02/2019	Ausgrid replaced service fuse cartridges for Gymea Train Station to restore power to enable signals to be working for Monday morning peak travel time.
3.1 (b)	34. 11/02/2019	Ausgrid corrected a defective Meter Service Box instead of disconnecting supply to the affected property because other neighbouring properties would have been affected by the disconnection.
3.1 (b)	35. 27/02/2019	Ausgrid staff performed a temporary repair of a customer's earth which enabled the restoration of supply to the premises. The customer was deemed to be vulnerable under Ausgrid's protocol.

4. Other services

The below table sets out the instances where Ausgrid has provided other services in FY19 in accordance with clause 3.1:

Ref of cl 3.1(d)	Service(s) provided	Purpose/Justification
i	<p>We provided other legal entities (such as telecommunication providers) the rights to use our assets such as:</p> <ul style="list-style-type: none"> • Poles; • Dark fibre; and • Other structural network assets. 	<p>The services are provided under lease arrangements and contracts.</p>
ii	<p>The following corporate services were provided to PLUS ES:</p> <ul style="list-style-type: none"> • General Administration; • General corporate; • Accounting/Finance; • Treasury; • Human Resources/Payroll; • ICT; • Legal/Regulatory; • Procurement; • Fleet; • Health, Safety and Environment; • Company Secretary and Office of CEO; • Audit; • Corporate affairs; and • Property & Facilities. 	<p>In accordance with exception provided in clause 3.1(d) (ii), as well as the services agreements with PLUS ES that was established at an arm's length basis, Ausgrid has provided these corporate services to PLUS ES pursuant to the CSA while adhering to its obligations in clause 3.2 of the Guideline for these arrangements.</p>
iii	<p>The relevant office and staff provided to PLUS ES are noted in the:</p> <ul style="list-style-type: none"> • Office register; and • Staff sharing register. 	<p>In accordance with exception provided in clause 3.1(d)iii as well as the exceptions provided in clauses 4.2.1(b) and 4.2.2(b), Ausgrid has allowed for such services and co-location arrangements in limited and highly controlled circumstances.</p>
iv	<p>Electricity Information was provided to PLUS ES as our contracted service provider for the following services:</p> <ul style="list-style-type: none"> • Metering Services; • Electrical and Fibre Services; and • Network testing Services <p>Electricity Information is also provided to other contracted service providers such as our vegetation management contractors.</p>	<p>As permitted under clause 3.1(d)(iv) and while maintaining compliance with clause 4.3. These services were established at an arm's length basis.</p>

Ref of cl 3.1(d)	Service(s) provided	Purpose/Justification
v	<p>The following services were provided:</p> <ul style="list-style-type: none"> • public lighting and nightwatchman lights (including security light services); • network safety services; • reserve feeder construction high load escorts rectification works to maintain network safety; • planned interruption; • customer requested; • training course for third parties; • related to network access customer-initiated asset relocations; • termination of cable at zone substation; • DNSP required performance minor and legacy metering services (including: meter recovery and disposal, type 5 and 6, distributor arranged outage for the purpose of replacing the meter, and meter consumptions data); • rental and hire services (this covers activities related to 'shared asset facilitation' of distributor assets); and • emergency recoverable work. 	<p>Waiver granted by the AER from 18 December 2017 to 30 June 2019.</p>

Appendix A – Compliance controls and measures

The following table sets out each of Ausgrid’s obligations mapped to one or more controls.

Category	Ref.	Obligation	Controls
Legal separation	3.1 (a)	A DNSP must be a legal entity.	<ul style="list-style-type: none"> △ Ausgrid is a Partnership with a current ABN. △ Ausgrid holds a Distributor’s license issued under the <i>Electricity Supply Act 1995</i> (NSW).
Legal separation	3.1 (b)	A DNSP may provide distribution services and transmission services but must not provide other services.	<ul style="list-style-type: none"> △ Ausgrid has an Encouraging Competition through Ring-fencing Policy. This policy sets out the responsibilities of staff to comply with the Guideline. △ There is a ring-fencing page on the Ausgrid intranet with information for staff on how to maintain compliance with the Guideline, including Ring-fencing Infosheet Do’s and Don’ts. △ There is a Ring-Fencing training program and associated materials to educate and assist staff to understand their obligations under the Guideline. All staff are required to complete the training. △ There is an up-to-date Ausgrid information sheet for ring-fencing communications. △ Templates approved by Legal to be used for all procurement activities include ring-fencing clauses. △ There is a Corporate Services Agreement which demonstrates Ausgrid carries on the business of the distribution and supply of electricity. As an Affiliate, PLUS ES carries on the business of supplying other services. △ Vulnerable customer assessment protocols lead to the work performed under the new Standard Control Service (30-minute rule) process. ▼ We have a dedicated ring-fencing email address which is monitored for any internal or external ring-fencing queries. ▼ There is a contact centre quality report that highlights any ring-fencing related issues when identified. ▷ Any issues of non-compliance are identified and recorded in our database ‘Enablon’. The system triggers notifications to responsible persons.

LEGEND △ Preventative Control ▼ Detective Control ▷ Corrective Control

Category	Ref.	Obligation	Controls
Separate accounts	3.2.1 (a)	A DNSP must establish and maintain appropriate internal accounting procedures to ensure that it can demonstrate the extent and nature of transactions between the DNSP and its affiliated entities.	<ul style="list-style-type: none"> △ The Cost Allocation Methodology (CAM) as approved by the AER is used to apportion costs to PLUS ES. △ The SAP Ausgrid accounting systems, contains separate legal entities for recording transactions between Ausgrid and the affiliate PLUS ES. △ The services agreement for the provision of Corporate Services, Labour Services, Electrical and Fibre and Testing services is used to apportion costs for services provided between Ausgrid and PLUS ES. These costs are invoiced regularly and the invoices paid within the terms of the agreement. ▼ There is a monthly journal transfer and reconciliation process between Ausgrid and PLUS ES.
Cost allocation and attribution	3.2.2 (a), (b)	A DNSP: (a) must allocate or attribute costs to distribution services in a manner that is consistent with the Cost Allocation Principles and its approved CAM , as if the Cost Allocation Principles and CAM otherwise applied to the allocation and attribution of costs between distribution services and non-distribution services; and (b) DNSP must only allocate or attribute costs to distribution services in accordance with clause 3.2.2(a), and must not allocate or attribute other costs to the distribution services it provides.	<ul style="list-style-type: none"> △ The CAM as approved by the AER is used to apportion costs to either Ausgrid or PLUS ES. △ The SAP Ausgrid accounting system contains separate legal accounting entities for recording transactions between Ausgrid and PLUS ES.
Cost allocation and attribution	3.2.2 (c)	A DNSP must establish, maintain and keep records that demonstrate how it meets cost allocation and attribution obligations.	<ul style="list-style-type: none"> △ There is a standard process we follow whereby relevant transactions and invoices are tracked and recorded on a shared drive, maintained by our Finance Policy and Accounting team. △ The services agreement for the provision of Corporate Services, Labour Services, Electrical and Fibre and Testing services is used to apportion costs for services provided between Ausgrid and PLUS ES. These costs are invoiced monthly and the invoices paid within the terms of the agreement. ▼ There is a monthly journal transfer and reconciliation process between Ausgrid and the affiliate.

LEGEND △ Preventative Control ▼ Detective Control ▷ Corrective Control

Category	Ref.	Obligation	Controls
Functional Separation	4.1 (b)	<p>A DNSP must not discriminate (either directly or indirectly) between a related electricity service provider and a competitor (or potential competitor) of a related electricity service provider in connection with the provision of:</p> <p>i) direct control services by the DNSP (whether to itself or to any other legal entity); and / or</p> <p>ii) contestable electricity services by any other legal entity.</p>	<ul style="list-style-type: none"> △ Ausgrid's contact centre utilises script hat refers to contestable electricity service providers generically (with the scripting highlighting that PLUS ES cannot be mentioned specifically). △ Ausgrid's website outlines that it treats all Accredited Service Providers (ASPs) and contractors (including Ausgrid's affiliate entity, PLUS ES) the same when it comes to contestable electricity services. △ Ausgrid's website has a Ring-fencing page which includes a link to the NSW Energy website of ASPs. △ PLUS ES has a Policy – Operating as an affiliated entity to Ausgrid (Ring-fencing). This policy sets out the responsibilities of PLUS ES staff to comply with the Guideline. △ There is a Ring-fencing page on the Ausgrid intranet with information for staff on how to maintain compliance with the Guideline, including Ring-fencing Infosheet Do's and Don'ts. △ Ausgrid has two agreements in place for the provision of the Metering Services which are established on an arms-length basis. △ There is a Ring-fencing training program and associated materials to educate and assist staff to understand their obligations under the Guideline. All staff have completed the training. ▼ We have a dedicated ring-fencing email address which is monitored for any internal or external ring-fencing queries. ▼ There is a contact centre quality report that highlights any ring-fencing related issues when identified. ▷ Any issues of non-compliance are identified and recorded in our database 'Enablon'. The system triggers notifications to responsible persons.

LEGEND △ Preventative Control ▼ Detective Control ▷ Corrective Control

Category	Ref.	Obligation	Controls
Functional Separation	4.1 (c)	<p>Without limiting its scope, clause 4.1(b) requires a DNSP to:</p> <ul style="list-style-type: none"> i) in dealing or offering to deal with a related electricity service provider, treat the related electricity service provider as if it were not a related electricity service provider (that is, as if it had no connection or affiliation with the DNSP); ii) in like circumstances, deal or offer to deal with a related electricity service provider and a competitor (or potential competitor) of the related electricity service provider on substantially the same terms and conditions; iii) in like circumstances, provide substantially the same quality, reliability and timeliness of service to a related electricity service provider and a competitor (or potential competitor) of the related electricity service provider; and iv) subject to clause 4.3.3(b), not disclose to a related electricity service provider information the DNSP has obtained through its dealings with a competitor (or potential competitor) of the related electricity service provider where the disclosure would, or would be likely to, provide an advantage to the related electricity service provider. 	<ul style="list-style-type: none"> △ Ausgrid has an Encouraging Competition through Ring-fencing Policy. This policy sets out the responsibilities of staff to comply with the Guideline. △ There is a Ring-fencing training program and associated materials to educate and assist staff to understand their obligations under the Guideline. All staff are required to complete the training.

LEGEND	△ Preventative Control	▼ Detective Control	▷ Corrective Control
---------------	------------------------	---------------------	----------------------

Category	Ref.	Obligation	Controls
Offices, staff, branding and promotions	4.2.1 (a)	A DNSP must use offices that are separate from any offices from which a related electricity service provider provides contestable electricity services.	<ul style="list-style-type: none"> △ There is an Ausgrid procedure for all new employees to ensure staff are only provided access to locations relevant for their role and entity. △ There is a PLUS ES – Accommodation analysis providing a risk assessment of co-locations where amenities are shared. △ The procedure – PLUS ES Accommodation and Security addresses the accommodation and security for PLUS ES to ensure compliance with the Guideline. △ Ausgrid has provided PLUS ES with its own branch of keying systems to separate it from the rest of Ausgrid. △ PLUS ES has separate identification cards to differentiate between their employees and Ausgrid employees. The cards only permit access to PLUS ES offices (with authorised exceptions). △ Ausgrid and PLUS ES have separate physical workspaces for staff with work locations restricted through electronic access controls. △ There is a checklist for Ausgrid staff who are loaned to PLUS ES to ensure thorough changeover of uniforms, badges and physical branded equipment at the start and cessation of the loans.
Staff sharing	4.2.2 (a)	A DNSP must ensure that its staff involved in the provision or marketing of direct control services are not also involved in the provision or marketing of contestable electricity services by a related electricity service provider.	<ul style="list-style-type: none"> △ There have been ring-fencing communications to staff advising them of what should be done to comply with the Guideline. △ When supplying staff to PLUS ES, staff follow an Ausgrid Checklist and PLUS ES Induction form. This procedure ensures the sharing of staff with PLUS ES is compliant with the Guideline. △ The procedure – Temporary supply of Ausgrid staff to PLUS ES ensures that due process is followed when sharing Ausgrid staff with PLUS ES in accordance with the Guideline exception. △ Ausgrid has an Encouraging Competition through Ring-fencing Policy. This policy sets out the responsibilities of staff to comply with the Guideline. △ There is a Ring-fencing page on the Ausgrid intranet with information for staff on how to maintain compliance with the Guideline, including Ring-fencing Infosheet Do's and Don'ts. △ PLUS ES has a Policy – Operating as an affiliated entity to Ausgrid (Ring-fencing). This policy sets out the responsibilities of staff to comply with the Guideline. △ There is a Ring-fencing training program and associated materials to educate and assist staff to understand their obligations under the Guideline. All staff are required to complete the training.

LEGEND △ Preventative Control ▼ Detective Control ▷ Corrective Control

Category	Ref.	Obligation	Controls
Staff sharing	4.2.2 (c)	The remuneration, incentives and other benefits (financial or otherwise) a DNSP provides to a member of its staff must not give the member of staff an incentive to act in manner that is contrary to the DNSP's obligations under this Guideline.	△ Ausgrid has a Performance and Recognition Guideline that does not incentivise staff to act contrary to the Guideline.
Staff sharing	4.2.3 (a)i	A DNSP must use branding for its direct control services that is independent and separate from the branding used by a related electricity service provider for contestable electricity services, such that a reasonable person would not infer from the respective branding that the DNSP and the related electricity service provider are related.	△ There are Ausgrid brand guidelines and PLUS ES brand guidelines which ensure the separation of branding between the two services, including separate PLUS ES marketing and branding staff.
Branding and cross-promotion	4.2.3 (a) ii	A DNSP must not advertise or promote its direct control services and its contestable electricity services that are not direct control services together (including by way of cross-advertisement or cross-promotion).	△ Ausgrid has an Encouraging Competition through Ring-fencing Policy. This policy sets out the responsibilities of staff to comply with the Guideline.
Branding and cross-promotion	4.2.3 (a) ii	A DNSP must not advertise or promote its direct control services and its contestable electricity services that are not direct control services together (including by way of cross-advertisement or cross-promotion).	<p>△ There is a Ring-fencing page on the Ausgrid intranet with information for staff on how to maintain compliance with the Guideline, including Ring-fencing Infosheet Do's and Don'ts.</p> <p>△ There is a Ring-fencing training program and associated materials to educate and assist staff to understand their obligations under the Guideline. All staff are required to complete the training.</p>

LEGEND △ Preventative Control ▼ Detective Control ▷ Corrective Control

Category	Ref.	Obligation	Controls
Branding and cross-promotion	4.2.3 (a) iii	A DNSP must not advertise or promote contestable electricity services provided by a related electricity service provider other than the DNSP itself.	<ul style="list-style-type: none"> △ PLUS ES has a Policy – Operating as an affiliated entity to Ausgrid (Ring-fencing). This policy sets out the responsibilities of staff to comply with the Guideline. ▷ There is a contact centre quality report that highlights any ring-fencing related issues when identified. ▷ We have a dedicated ring-fencing email address which is monitored for any internal or external ring-fencing queries. ▼ Any issues of non-compliance are identified and recorded in our database 'Enablon'. The system triggers notifications to responsible persons.
Office and staff registers	4.2.4	A DNSP must establish, maintain and keep a register that identifies: <ul style="list-style-type: none"> (a) the classes of offices to which it has not applied clause 4.2.1(a) by reason of clause 4.2.1(b)i or 4.2.1(b)iii; and (b) the nature of the positions (including a description of the roles, functions and duties) of its members of staff to which it has not applied clause 4.2.2(a) by reason of clauses 4.2.2(b)i.a., 4.2.2(b)iii or 4.2.2(d); and must make the register publicly available on its website. 	<ul style="list-style-type: none"> △ The Governance, Risk and Compliance (GRC) team manage the ring-fencing registers published on the Ausgrid website. △ GRC team monitors changes that might trigger the action on requirements currently not applicable.
Protection of confidential information	4.3.2	A DNSP must: <ul style="list-style-type: none"> (a) keep confidential information confidential; and (b) only use confidential information for the purpose for which it was acquired or generated. 	<ul style="list-style-type: none"> △ Allowable uses of Confidential Information are defined as per privacy guidelines and documented in relation to data stored in ICT systems, customer records, HR records and financial records. △ Ausgrid has a Policy – Encouraging Competition through Ring-fencing which defines Confidential Information per the Guideline. △ Behaviours related to handling of Confidential Information are defined in a Code of Conduct. △ There is an Information Sharing Protocol on the Ausgrid website that sets out the terms and conditions that apply to information sharing. △ Ausgrid has a Privacy (Personal Information) Policy. △ Ausgrid has a Procedure – Information classification, labelling and handling.

LEGEND △ Preventative Control ▼ Detective Control ▷ Corrective Control

Category	Ref.	Obligation	Controls
Disclosure of information	4.3.3	<p>A DNSP must not disclose confidential information to any person, including a related electricity service provider, unless:</p> <p>(a) the DNSP has first obtained the explicit informed consent of the relevant customer, or prospective customer, to whom the confidential information relates;</p> <p>(b) the disclosure is required by, or for the purpose of complying with any law;</p> <p>(c) the disclosure is necessary to enable the DNSP to provide its distribution services, its transmission services or its other services (including by acquiring services from other legal entities);</p> <p>(d) the information has been requested by or on behalf of a customer, or potential customer, of another legal entity, and the disclosure is necessary to enable the legal entity to provide its transmission services, contestable electricity services or other services to the customer or potential customer;</p> <p>(e) the disclosure is solely for the purpose of providing assistance to another Network Service Provider in response to an event (such as an emergency) that is beyond the other Network Service Provider's reasonable control;</p> <p>(f) the disclosure is solely for the purposes of research by a legal entity other than a related electricity service provider of the DNSP; or</p> <p>(g) a related electricity service provider of the DNSP has requested the disclosure and the DNSP complies with clause 4.3.4 in relation to that confidential information.</p>	<ul style="list-style-type: none"> △ Allowable uses of confidential information stored in ICT systems, customer records, HR records and financial records are defined as per information security and acceptable use of technology policies. △ Behaviours related to handling of confidential information are defined in a Code of Conduct. △ There is an ICT system access analysis, which identifies the ICT systems across Ausgrid which have Confidential Information and/or Electricity Information and ICT staff ensure access controls based on this. △ Ausgrid and PLUS ES intranet sites have restrictions on content to ensure that PLUS ES does not have access to Electricity or Confidential Information. △ There is a PLUS ES usage system document which identifies the PLUS ES roles which require access to certain Ausgrid systems for the purpose of disclosure to provide other contracted services. △ ICT have implemented 'Role Based Access Controls' for the key systems containing Confidential Information, such as metering and customer data. ▼ User Access Reviews occur monthly to identify and remove terminated users. ▷ The Identity Access Management Solution has been implemented, which revokes access based upon termination dates including role changes. ▼ Security Incident Event Management Monitoring has been implemented, which monitors events that have been customised based upon our cyber risk appetite e.g. failed login attempts.

LEGEND △ Preventative Control ▼ Detective Control ▷ Corrective Control

Category	Ref.	Obligation	Controls
Disclosure of information	4.3.4	<p>Subject to clause 4.1(c)iv and this clause 4.3.4, where a DNSP shares confidential information with a related electricity service provider, or where confidential information that a DNSP has disclosed under clause 4.3.3(f) is then disclosed by any person to a related electricity service provider of the DNSP, the DNSP must provide access to that confidential information (including the derived information) to other legal entities on an equal basis.</p> <p>(b) A DNSP is only required by clause 4.3.4(a) to provide information to a legal entity where:</p> <ul style="list-style-type: none"> i. the legal entity has requested that it be included on the information register in respect of information of that kind; and ii. the legal entity is competing, or is seeking to compete, with the DNSP, or a related electricity service provider of the DNSP, in relation to the provision of contestable electricity services. <p>(c) A DNSP is not required by clause 4.3.4(a) to provide information to a legal entity where the DNSP has disclosed the information in the circumstances set out in clauses 4.3.3(a) to (e).</p> <p>(d) Without limiting clause 4.3.4(a), a DNSP must establish an information sharing protocol that sets how and when it will make the information referred to in clause 4.3.4(a) available to legal entities, and must make that protocol publicly available on its website.</p> <p>(e) Where a DNSP discloses information referred to in clause 4.3.4(a) to any other legal entity under this clause 4.3.4, it must do so on terms and conditions that require the other legal entity to comply with clause 4.3.2 and 4.3.3(a) to (d) in relation to that information as if the other legal entity was a DNSP.</p>	<p>△ There is an Information Sharing Protocol on the Ausgrid website that sets out the terms and conditions that apply to information sharing in accordance with the Guideline.</p>

LEGEND △ Preventative Control ▼ Detective Control ▷ Corrective Control

Category	Ref.	Obligation	Controls
Information register	4.3.5 (a)	<p>A DNSP must establish, maintain and keep a register of all:</p> <ul style="list-style-type: none"> i. related electricity service providers; ii. other legal entities who provide contestable electricity services but who are not affiliates of the DNSP who request access to information identified in clause 4.3.4(a), and must make the register publicly available on its website. <p>(b) For each legal entity that has requested that a DNSP provide access to information identified in clause 4.3.4(a), the DNSP's information register must:</p> <ul style="list-style-type: none"> i. identify the kind of information requested by the legal entity; and ii. describe the kind of information requested by the legal entity in sufficient detail to enable other legal entities to make an informed decision about whether to request that kind of information from the DNSP. <p>(c) A legal entity may request that the DNSP include it on the information register in relation to some or all of the kinds of information that the DNSP is required to provide under clause 4.3.4(a), and the DNSP must comply with that request.</p>	<ul style="list-style-type: none"> △ The GRC team manage the ring-fencing registers published on the Ausgrid website. △ The GRC team maintain an Information Sharing Register on the Ausgrid website.
Conduct of service providers	4.4.1 (a)	<p>A DNSP:</p> <p>(a) must ensure that any new or varied agreement between the DNSP and a service provider, for the provision of services to the DNSP that enable or assist the DNSP to supply direct control services, requires the service provider to comply, in providing those services, with:</p> <ul style="list-style-type: none"> i. clauses 4.1, 4.2.1, 4.2.2 and 4.3.2 of this Guideline; and ii. clause 4.2.3 of this Guideline in relation to the brands of the DNSP; <p>as if the service provider was the DNSP.</p>	<ul style="list-style-type: none"> △ Templates approved by Legal are to be used for all procurement activities, and include ring-fencing clauses that comply with the Guideline. Ausgrid ensures that any contracts between Ausgrid and other parties include obligations for the counterpart to comply with the Guideline.
	4.4.1 (b)	<p>A DNSP (b) must not, directly or indirectly, encourage or incentivise a service provider to engage in conduct which, if the DNSP engaged in the conduct itself, would be contrary to the DNSP's obligations.</p>	<ul style="list-style-type: none"> △ Ausgrid has an annual corporate scorecard that does not incentivise actions contrary to the Guideline.

LEGEND △ Preventative Control ▼ Detective Control ▷ Corrective Control

Category	Ref.	Obligation	Controls
<p>The AER will not grant a waiver of an obligation under this Guideline other than in accordance with this clause 5</p>	5.2	<p>A DNSP may apply in writing to the AER for a waiver. An application for a waiver must contain all information and materials necessary to support the DNSP's application, including:</p> <ul style="list-style-type: none"> (a) the obligation in respect of which the DNSP is applying for a waiver; (b) the reasons why the DNSP is applying for the waiver; (c) details of the service, or services, in relation to which the DNSP is applying for the waiver; (d) the proposed commencement date and expiry date (if any) of the waiver and the reasons for those dates; (e) details of the costs associated with the DNSP complying with the obligation if the waiver of the obligation were refused; (f) the regulatory control period(s) to which the waiver would apply; (g) any additional measures the DNSP proposes to undertake if the waiver were granted; and (h) the reasons why the DNSP considers the waiver should be granted with reference to the matters specified in clause 5.3.2(a), including the benefits, or likely benefits, of the grant of the waiver to electricity consumers. 	<ul style="list-style-type: none"> △ There is an Ausgrid Waiver Application Template which addresses these requirements.
	5.7 (a)-(b)	<p>A DNSP must establish, maintain and keep a register of all waivers (including any variation of a waiver) and must make the register publicly available on its website.</p> <p>The register established under clause 5.7(a) must include:</p> <ul style="list-style-type: none"> i. the description of the conduct to which the waiver or interim waiver applies; and ii. the terms and conditions of the waiver or interim waiver; as set out in the AER's written decision, provided by the AER to the DNSP, to grant (or vary) the waiver or interim waiver. 	<ul style="list-style-type: none"> △ All Ring-fencing waivers are on the Ausgrid website.

LEGEND △ Preventative Control ▼ Detective Control ▷ Corrective Control

Category	Ref.	Obligation	Controls
Maintaining compliance	6.1	A DNSP must establish and maintain appropriate internal procedures to ensure it complies with its obligations under this Guideline.	<ul style="list-style-type: none"> △ Procedure – Temporary supply of Ausgrid staff to PLUS ES ensures that due process is followed when sharing Ausgrid staff with PLUS ES in accordance with the Guideline exception. △ Procedure – PLUS ES Accommodation and Security addresses accommodation and security for PLUS ES to ensure compliance with the Guideline. △ Ausgrid has an Encouraging Competition through Ring-fencing Policy. This policy sets out the responsibilities of staff to comply with the Guideline.
Annual compliance report	6.2.1 (a)-(c)	A DNSP must prepare an annual ring-fencing compliance report each regulatory year.	<ul style="list-style-type: none"> △ A regulatory reporting calendar is established and monitored by the GRC team.
Compliance breaches	6.3	A DNSP must notify the AER in writing within 5 (five) business days of becoming aware of a material breach of its obligations under this Guideline.	<ul style="list-style-type: none"> △ The GRC team maintains a Non-compliance/Breach Register who also notifies the regulator within the required timeframes. △ Ausgrid maintains a Non-compliance/Breach Register that is maintained and monitored by the GRC team. The GRC team notifies the AER within the timeframes required by the Guideline. △ Ausgrid has an Encouraging Competition through Ring-fencing Policy. This policy sets out the responsibilities of staff to comply with the Guideline.
Transitional arrangements	7.1 (b)	Where a distribution determination applicable to a DNSP results in a change in the classification of a distribution service provided by the DNSP, and that change puts the DNSP in breach of an obligation under this Guideline, the DNSP must comply with that obligation within 12 months of the commencement date of the distribution determination.	<ul style="list-style-type: none"> ▼ Subject Matter Expert's assigned responsibility to monitor changes in regulations associated with their business area and modify controls as needed. ▷ Any issues of non-compliance are identified and recorded in our database 'Enablon'. The system triggers notifications to responsible persons.
LEGEND	△ Preventative Control	▼ Detective Control	▷ Corrective Control

Appendix B – Summary of transactions with PLUS ES

PLUS ES provides the following range of services to Ausgrid:

Transactions	Purpose
<p>Electrical and Fibre Services:</p> <ul style="list-style-type: none"> • Ausgrid Fibre Optic Network; • External third-Party Fibre Optic Duct Study Request – Facilities Access; • Customer Works Associated with Substation Replacement/Removal; • Undergrounding of Service Mains; • Property STN Maintenance; and • Specialist Projects. 	<p>Ancillary to its own distribution and transmission services, Ausgrid contracts with specialised providers to receive certain services.</p>
<p>Testing Services:</p> <ul style="list-style-type: none"> • Chemical Testing Services; • Calibration Services; • Electrical Testing Services; • Conduct of Tests – Electrical Testing; • Test Documentation – Electrical Testing; • Record Retention and Ownership – Electrical Testing; • Applicability of Reports and Certificates – Electrical Testing; • Postponement of Testing – Electrical Testing; and • Consulting Services – Electrical Testing. 	<p>Ancillary to its own distribution and transmission services, Ausgrid contracts with specialised providers to receive certain services.</p>
<p>Metering Related (Alternative Control Services)</p>	<p>Provide Metering Services to enable Ausgrid to provide Alternate Control Services and related Ancillary Network Services.</p>
<p>Metering Related (Standard Control Services)</p>	<p>Provide Metering and related Services to enable Ausgrid to provide Standard Control Services with respect to the Metering Points.</p>

These are provided under the terms of four non-exclusive service agreements.

Appendix C – Extract from Deloitte’s Ausgrid – Ring-fencing Guideline Compliance Report 1 November 2018

C1 Summary of findings

The following table summarises observations and recommendations against the obligations where an exception is identified. The rating of each obligation has been applied in accordance with **Section 2.2**. Management response to the observations and recommendations are in Section 5.

Category	GL Ref.	Deloitte Recommendations	Ausgrid actions
Offices, staff, branding and promotions	4.2.1 (a)	<p>We recommend management:</p> <ul style="list-style-type: none"> Design and implement monitoring processes to confirm that only authorised personnel are able to access Ausgrid offices and assets and for the approved time period (for example to carry out approved tasks per work orders). Periodically test employee access to ensure DNSP and related electricity service providers cannot access the offices of the other. We further recommend management develop adequate controls for on-boarding and off-boarding staff or contractors to achieve compliance against this location-sharing obligation. 	<ol style="list-style-type: none"> There is a procedure for all new employees to ensure staff are only provided access to locations relevant for their role and entity. Installation of further restrictions of site doors with swipe-only access. System enhancements to enable identification of all doors across Ausgrid and PLUS ES sites. System capability to monitor unauthorised activity i.e. PLUS ES employee attempting access to Ausgrid doors. Carried out testing of employee access to Ausgrid doors in December 2018, March 2019 and April 2019 with a view to perform periodic testing every 6 months. Established Procedure – PLUS ES Accommodation and Security. Undertaken risk assessment of co-locations where amenities are shared per the PLUS ES – Accommodation analysis. There is a checklist for Ausgrid staff who are loaned to PLUS ES to ensure thorough changeover of uniforms, badges and physical branded equipment at the start and cessation of the loans.
Staff sharing	4.2.2 (a)	<p>We recommend management:</p> <ul style="list-style-type: none"> Formalise a short-term secondment process and ensure all staff movement is monitored, organised and documented in line with the Guideline. 	<ol style="list-style-type: none"> Implemented the Procedure – Temporary supply of Ausgrid staff to PLUS ES which ensures that due process is followed in accordance with the Guideline.

Category	GL Ref.	Deloitte Recommendations	Ausgrid actions
Protection of confidential information	4.3.2 (a) (b) and 4.3.3 (a)-(g)	<p>We recommend management:</p> <ul style="list-style-type: none"> • Apply access limitations to all employees to the extent required to perform the responsibilities of each role. • Periodically test employee system access to ensure DNSP and related electricity service providers cannot access the systems which contain Ring-fenced sensitive information. • Undertake a task identifying systems containing confidential information and allocating access restrictions to these systems. 	<ol style="list-style-type: none"> 1. Role Based Access Controls have been implemented for the key systems containing Confidential Information, such as metering and customer data. 2. User Access Reviews occur monthly to identify and remove terminated users. 3. An Identity Access Management Solution (IAM) has been implemented, where the IAM will revoke access based upon termination dates, and role changes. 4. Security Incident Event Management Monitoring (SIEM) has been implemented, which monitors events that have been customised based upon our cyber risk appetite e.g. failed login attempts. 5. A thorough analysis has been undertaken to identify all systems containing confidential information and which of these PLUS ES should or should not have access to.



Ausgrid