

OUR CUSTOMER TERMS CLOUD SERVICES - COMPLIANCE

CONTENTS

1	ABOUT THIS PART	2
2	COMPLIANCE WITH STANDARDS GENERALLY	2
	Scope of compliance	2
	Nature of compliance	2
	Charges.....	3
	Audit.....	3
3	COMPLIANCE WITH TECHNOLOGY INDUSTRY STANDARDS	4
	Amendments to Technology Industry Standards	5
4	COMPLIANCE WITH CUSTOMER INDUSTRY STANDARDS	5
	Compliance with Payment Card Industry (PCI) Data Security Standards	5
	Compliance with Prudential Standard APS 231 and Prudential Standard GPS 231	7
	Amendments to Customer Industry Standards.....	8
5	SUPPLIER ACCREDITATIONS	8
6	SPECIAL MEANINGS	8

OUR CUSTOMER TERMS

CLOUD SERVICES - COMPLIANCE

Certain words are used with the specific meaning set out in the General Terms of the Network Computing Services section of Our Customer Terms, or in the General Terms of Our Customer Terms.

1 ABOUT THIS PART

- 1.1 This is Compliance part of the Cloud Services section of Our Customer Terms. Depending on the nature of the products and services you are receiving under this Cloud Services section, provisions in other parts of the Cloud Services section, as well as in the General Terms of Our Customer Terms at <http://www.telstra.com.au/customer-terms/business-government/index.htm>, may apply.
- 1.2 See section one of the General Terms of Our Customer Terms at <http://www.telstra.com.au/customer-terms/business-government/index.htm> for more detail on how the various sections of Our Customer Terms are to be read together.
- 1.3 See section one of the General Terms part of the Cloud Services section for more detail on how the various parts of the Cloud Services section are to be read together.

2 COMPLIANCE WITH STANDARDS GENERALLY

Scope of compliance

- 2.1 This section only applies to Cloud Services operated and maintained by us, which include Cloud Infrastructure and Tailored Infrastructure. This section does not apply to the third party products and services which we resell but are operated and maintained by the third party. Compliance with any technical or industry standards is at the discretion of the third party. Please refer to the applicable third party's website for details of compliance with standards for that particular product or service.

Nature of compliance

- 2.2 In Your Agreement, we may agree to comply with particular Standards in accordance with this Compliance part, to the extent those Standards are applicable to the relevant products and services you receive.
- 2.3 These Standards may be:
 - (a) Technology Industry Standards, which we may agree to comply with in the provision of certain relevant products and services provided to you in accordance with section 3; or
 - (b) Customer Industry Standards, which are standards with which you may be required to comply, and in respect of which we agree to comply with particular aspects of those Standards in our provision of certain services to you in accordance with section 4.
- 2.4 We will determine, at our sole discretion, the method(s) by which we comply with the Standards. The method(s) by which we comply with the Standards may change at any time.
- 2.5 We are not responsible for compliance with any obligation under a Standard with which you solely must comply.
- 2.6 We may cease to comply with the Standards in relation to your services at any time (for

OUR CUSTOMER TERMS CLOUD SERVICES

PART H - COMPLIANCE

example due to changes in the standards), unless otherwise agreed with you. We will notify you if we are no longer able to comply with the Standards

Charges

- 2.7 If we agree to comply with any of the Technology Industry Standards in accordance with section 3 with respect to the provision of services to you, we will not charge an additional amount for our compliance.
- 2.8 If we agree to comply with any of the Customer Industry Standards in accordance with section 4, we may charge an additional amount for our compliance as set out in Your Agreement.

Audit

- 2.9 We acknowledge that from time to time you may be required to, or may wish to, audit the extent to which we are complying with any agreed Standards with respect to our provision of the agreed services to you.
- 2.10 Subject to you paying our reasonable expenses, and as long as there is no risk to, or detrimental impact upon, our security, privacy, OH&S or confidentiality requirements or any of our customers (including you), you may have your internal auditor, or an independent external auditor who is not our competitor (including a representative of the organisation administering the relevant Standard), audit our performance in providing the following products and services to you:

- (a) Tailored Infrastructure
- (b) Cloud Infrastructure

in accordance with the agreed Standards.

- 2.11 On receiving reasonable notice from you of a request to audit, we will:
- (a) permit the auditor access, including pre-arranged on-site inspection of the relevant products and services performed by us;
 - (b) provide information requested by the auditor, acting reasonably, considered necessary in order to satisfy themselves of our compliance with the applicable Standard; and
 - (c) allow the auditor to inspect such information held by us as the auditor, acting reasonably, considers necessary in order to satisfy themselves of the adequacy of our compliance with the applicable Standard,

subject to compliance by the auditor with our standard site requirements (including as to security, privacy, OH&S and confidentiality). For the avoidance of doubt, the intention of this clause is to provide the auditor with the same rights as you, but not more.

- 2.12 We may have our internal auditor or other representative(s) present at an audit.
- 2.13 Any access and information provided to the auditor is subject to compliance by the auditor

OUR CUSTOMER TERMS CLOUD SERVICES

PART H - COMPLIANCE

with our standard requirements (including as to security, privacy, OH&S and confidentiality).

2.14 You may request no more than one audit per calendar year.

3 COMPLIANCE WITH TECHNOLOGY INDUSTRY STANDARDS

3.1 Table 1 below sets out the Technology Industry Standards with which we may agree to comply, the scope of our compliance and the relevant products and services to which that compliance relates.

3.2 If, and to the extent, we agree, we will comply with the standards in Table 1 for the relevant products and services you receive.

Table 1 (“Technology Industry Standards”)

TIS	Scope of TIS	Applicable services	Location	Validity
ISO 27001:2013	Data Security	Tailored Infrastructure	Pitt St Data Centre (Sydney) Ultimo Data Centre (Sydney) Exhibition St Data Centre (Melbourne) (information about additional backup data centres available upon request)	Number MEL4000406/A Original certificate: 16 Apr 2012 Certificate expiry: 16 April 2021
		Cloud Infrastructure	St Leonards Data Centre (Sydney) Clayton Data Centre (Melbourne) Gnangara Data Centre (Western Australia) (information about additional backup data centres available upon request)	
ASIO T4 Protective Security	Data Centre	Data Centres	Deakin Data Centre (Canberra)	Number eA1028938 issued on 22 Feb 2007
DSD/I-RAP	Government Data Centre Internet Gateway	Government Data Centre Internet Gateway	Deakin Data Centre (Canberra)	Issued Nov 2011

OUR CUSTOMER TERMS CLOUD SERVICES

PART H - COMPLIANCE

Amendments to Technology Industry Standards

- 3.3 Where we have agreed to comply with a Technology Industry Standard and that standard is re-issued or varied:
- (a) if we decide to comply with the re-issued or varied standard, we agree we will bear the costs of compliance with the re-issued or varied standard; and
 - (b) if you request that we comply with the re-issued or varied standard earlier than the time we intend to do so or in circumstances where we were not going to comply, we may charge you an additional reasonable amount for our compliance with the re-issued or varied standard at that earlier time.

4 COMPLIANCE WITH CUSTOMER INDUSTRY STANDARDS

- 4.1 PCI compliance is no longer available from 24 March 2016. For those customers with whom we agreed to provide PCI compliance prior to 24 March 2016, we will continue to comply with the obligations referred to below.
- 4.2 The following are Customer Industry Standards:
- (a) Payment Card Industry (PCI) Data Security Standards (Number PCI DSS v2.0 issued on 28 Oct 2010);
 - (b) Prudential Standard APS 231 – Outsourcing (Number APS 231 issued on Oct-2006); and
 - (c) Prudential Standard CPS 231 – Outsourcing (Number CPS 231 issued on July 2011), (“Customer Industry Standards”).
- 4.3 You are responsible for compliance with the Customer Industry Standards.
- 4.4 If we agree, we will comply with specified obligations under the Customer Industry Standards, as identified below or as agreed between you and us, to enable you to comply with a Customer Industry Standard.
- 4.5 You acknowledge that our agreement to supply certain relevant products or services in accordance with any of the Standards does not guarantee end-to-end compliance with those Standards, and we do not and cannot assume your compliance obligations under all or any of the Standards.

Compliance with Payment Card Industry (PCI) Data Security Standards

- 4.6 Under the Payment Card Industry Data Security Standards, unless we otherwise agree, we are each respectively responsible for complying with the obligations as set out in Table 2:

Table 2 (“**PCI Obligations**”)

OUR CUSTOMER TERMS CLOUD SERVICES

PART H - COMPLIANCE

Obligations	Responsibilities	
	Infrastructure as a Service	Software as a Service
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	You	Us (excluding 1.1.4, 1.1.5 and 1.4)
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	You	Us (excluding 2.1, 2.2.1, 2.3)
Requirement 3: Protect stored cardholder data	You	You
Requirement 4: Encrypt transmission of cardholder data across open, public network	You	You
Requirement 5: Use and regularly update anti-virus software or programs	You	Us
Requirement 6: Develop and maintain secure systems and applications	You	You
Requirement 7: Restrict access to cardholder data by business need-to-know	Us (in relation to our premises only)	Us (in relation to our premises only)
Requirement 8: Assign a unique ID to each person with computer access	You	Us
Requirement 9: Restrict physical access to cardholder data	Us (excluding 9.6 - 9.7.2 and 9.9.1 - 9.10.2)	Us (excluding 9.6 - 9.7.2 and 9.9.1 - 9.10.2)
Requirement 10: Track and monitor all access to network resources and cardholder data	You	Us (excluding 10.2.2 - 10.3.6)
Requirement 11: Regularly test security systems and processes	You	Us (excluding 11.2 - 11.3.2)

OUR CUSTOMER TERMS CLOUD SERVICES

PART H - COMPLIANCE

Obligations	Responsibilities	
	Infrastructure as a Service	Software as a Service
Requirement 12: Maintain a policy that addresses information security for employees and contractors	Us (12.2, 12.5.3 - 12.5.4, 12.9.2 - 12.9.6 only)	Us (12.2, 12.5.3 - 12.5.4, 12.9.2 - 12.9.6 only)

Compliance with Prudential Standard APS 231 and Prudential Standard GPS 231

4.7 In relation to APS 231 or GPS 231 (as applicable to you), if, and to the extent, we agree, we will comply with the following obligations.

Subcontracting

4.8 If we subcontract any part of the services to a third party, we agree that we remain responsible for the provision of the service including for liability for any failure on the part of the subcontractor.

Insurance

4.9 We agree to maintain Public Liability and Professional Indemnity insurance (or otherwise maintain adequate self insurance arrangements) to a value of at least twenty million dollars (\$20,000,000) and upon your reasonable request will provide a certificate of currency (if applicable) in respect of applicable insurance policies held by us relating to the provision of the service.

Regulatory Body Access

4.10 We acknowledge and agree that, subject to you paying our reasonable expenses, representatives of a Regulatory Body, on reasonable written notice, may be permitted to:

- (a) request access to us and that such access will not be unreasonably withheld; and
- (b) pre-arrange on site inspections if the Regulatory Body considers this necessary in its role as prudential supervisor and we will not disclose or advertise that the Regulatory Body has conducted such visits, except as necessary to coordinate with other institutions regulated by the Regulatory Body which are our existing clients or customers; and/or
- (c) request any information the Regulatory Body, acting reasonably, considers necessary to satisfy itself as to the adequacy of the risk management systems used by us; and/or
- (d) to inspect such information held by us as the Regulatory Body, acting reasonably, considers necessary in order to satisfy themselves of the adequacy of our risk management systems.

OUR CUSTOMER TERMS CLOUD SERVICES

PART H - COMPLIANCE

- 4.11 You agree to take reasonable steps to ensure that the Regulatory Body will comply with our standard requirements (including as to security, privacy, OH&S and confidentiality) when exercising any of its rights set out in clause 4.10 above.

Amendments to Customer Industry Standards

- 4.12 Where a Customer Industry Standards is re-issued or varied and we have agreed to comply with specified obligations under that standard, we will continue to comply with those obligations only, unless we otherwise agree.
- 4.13 We may charge an additional reasonable amount for our compliance with additional or varied obligations to enable you to comply with re-issued or varied Customer Industry Standards.

5 SUPPLIER ACCREDITATIONS

- 5.1 A list of the current suppliers for which we are accredited can be provided upon request.
- 5.2 We will determine at our sole discretion the supplier accreditations which we will obtain or maintain.
- 5.3 Our supplier accreditations are subject to change without notice, unless we have expressly agreed with you that we will hold a specific supplier accreditation in which case we will provide you with notice either in advance of the change or as soon as practicable thereafter.
- 5.4 We may charge an additional amount for agreeing to obtain or maintain any supplier accreditation as set out in Your Agreement.
- 5.5 Upon receiving a written request from you, we will provide you with evidence, that we hold the relevant accreditation.

6 SPECIAL MEANINGS

Agreement means your customer services agreement with us.

Customer Industry Standards means the standards identified in section 4.1 of this Compliance part of the Cloud Services section of Our Customer Terms.

Regulatory Body means any government body with jurisdiction over you or us.

Standards means one or more of the Technology Industry Standards and the Customer Industry Standards as the context requires.

Technology Industry Standards means the standards identified in Table 1 in section 3 of this Compliance part of the Cloud Services section of Our Customer Terms.