TELSTRA CLOUD SERVICES RESPONSIBILITIES GUIDE

V11.0

IT'S HOW WE CONNECT

WELCOME TO TELSTRA CLOUD SERVICES

Telstra Cloud Services offers a growing range of infrastructure, backup and software cloud products and services.

NEED GENERAL SERVICE SUPPORT?

For general service support, call 1800 620 345 or email any questions to ***cloudservices@team.telstra.com***.

Service support is available Monday to Friday, 9AM to 5PM (AEST).

NEED TECHNICAL SUPPORT?

For general technical support, call 1800 620 345 or email any questions to ***cloudservicessupport@online.telstra.com.au***.

Technical support is available 24/7.

> Note: we don't provide assistance with issues specific to a customer's local network, servers, operating systems and software (post-installation). Specialist technical support may be charged as an additional service.

CONVENTIONS USED IN THIS GUIDE

The following typographical conventions are used in this guide for simplicity and readability:

Web addresses, e-mail addresses and hyperlinks are shown in ***bold italics***, for example ***www.telstraenterprise.com.au***.

Button names and titles/features on your computer screen are shown in *italics.*

User input is shown in `typewriter` font.

Responsibilities Guide, Version 11.0

WHAT'S INSIDE

CHAPTER 1
ABOUT THIS GUIDE

There are a number of terms, conditions, requirements, roles and responsibilities associated with the purchase and use of Telstra Cloud Services.

This guide outlines both yours and our roles and responsibilities regarding each cloud solution.

Requirements are split according to:

- Software
- Infrastructure
- Data centres

This guide is the companion document to the Cloud Services section of ***Our Customer Terms***.

Our Customer Terms set out the terms and conditions relating to how we provide Cloud Services subscription plans, products and services.

SERVICE CHANGES

This guide is also used to inform you of any service changes that may happen from time to time. All service charges are outlined in your Cloud Services application form, responsibilities guide and/or separate agreement with us.

REQUIREMENTS – NEW CUSTOMERS

If you are a new Cloud Services customer, you are expected to manage and use your cloud solution according to the requirements outlined in this guide.

If you choose not to follow these requirements, we will not be responsible for any loss or inconvenience experienced if your cloud solution is disrupted. In this circumstance, we may charge you additional fees in order to fix your cloud solution.

REQUIREMENTS – EXISTING CUSTOMERS

If you are an existing Cloud Services (formerly called 'Network Computing Services') customer, you are expected to adhere to your current service requirements until the end of any initial term for your Network Computing Service, unless you choose to migrate to Cloud Services.

If you migrate to Cloud Services, you will automatically be expected to manage and use your cloud solution according to the requirements outlined in this guide.

If you choose to migrate to Cloud Services prior the end of your initial term, you may be required to pay any applicable early termination fees.

REQUIREMENTS – ALL CUSTOMERS

You are required to provide us with all applicable information, data, consents, authorisations, decisions and approvals in order to activate service requests.

You can make changes to your cloud solution using the Cloud Services management console.

It's your responsibility to identify any moves, adds or changes relevant to your cloud solution and submit the appropriate requests.

You are also required to identify when you need assistance from your assigned Telstra account executive and to submit the appropriate requests.

OUR REQUIREMENTS

We're required and committed to providing services according to the requirements outlined in this guide.

Our services are backed by service level agreements to help ensure maximum availability and performance so you get the most out of your cloud solution.

We're also required to provide service support (as outlined in your Cloud Services agreement), notify you of any service changes and let you know when a service request has been completed.

KEEPING YOUR CONTACT DETAILS UP TO DATE

From time to time we'll need to get in contact with you regarding your cloud solution, so it's important that you keep your organisation's details up to date.

As a Cloud Services customer, you need to ensure that the following contact details are correct and kept up to date:

Commercial contact: the authorised staff member who acts on your business's behalf regarding all commercial matters associated with your cloud solution. Note: your Telstra account executive may call these contacts the 'primary contact' when buying cloud services on your behalf.

Technical contact: the authorised person who answers any technical questions associated with your cloud solution on your behalf.

You can update your contact details via the management console or by calling 1800 620 345.

GENERAL REQUIREMENTS

REQUIREMENT	RESPONSIBILITY	
If you believe we have not satisfactorily completed a service or product installation, inform us within five business days of completion.		Customer
Report any faults with your products by contacting the service desk and providing us with the following details: • Company name • Account ID • Password (if applicable) • Unique identifier of the affected device, such as an IP address • Description of fault • Any other information we reasonably ask for		Customer
Monitor and respond to infrastructure alarms relating to the relevant service level as set out in Our Customer Terms.	Telstra	

Provide updates on the progress of all reported faults within the relevant service level as set out in Part A (General) of the Cloud Services section of Our Customer Terms.	Telstra	

SERVICE LEVELS

The various levels of service activations and modifications all have different corresponding timelines depending on the complexity of the action required.

These timelines can also be affected by factors such as volume. For example, creating a virtual server is a relatively minor piece of work, while creating 100 virtual servers can take an additional amount of time.

REQUIREMENT	RESPONSIBILITY	
SERVICE ACTIVATION		
MINOR A simple service activation that will be delivered within five business days. Examples include: • Add or delete one or more Telstra managed virtual servers • Modify an existing virtual server • Provide a new virtual server instance Data centre examples include: • A request for additional power (adding equipment to a rack) • Connect an existing data service to an existing rack	Telstra	
STANDARD A standard service activation that will be delivered within 20 business days. Examples include: • Add, modify or cancel VLAN configurations to an existing environment • Make changes to an existing or new IPSEC VPN Data centre examples include: • Install a new rack • Update a power feed	Telstra	
MAJOR A service activation involving greater complexity than a standard activation. An infrastructure example includes: • Deploy a new service requiring a new network environment to be terminated within Telstra cloud data centres A data centre example includes: • Request for bespoke cabling	Telstra	

REQUIREMENT	RESPONSIBILITY	
SERVICE ACTIVATION		
PRE-DEFINED MODIFICATIONS The tailored infrastructure section of the Cloud Services management console has a list of predefined service requests you can make. The list includes some associated prices and target timeframes and others which require a quote from us.	Telstra	
PROJECTS Requests not included in abovementioned section of the Cloud Services management console are automatically handled and managed as a project for which we provide you with a quote and estimated timeframe.	Telstra	

CHAPTER 2
APPLICATIONS

GENERAL REQUIREMENTS

REQUIREMENT	RESPONSIBILITY	
Create login accounts.		Customer
Manage login accounts.		Customer
Install applications purchased from us (excludes ***Hybrid Disaster Recovery*** software).	Telstra	
Install applications purchased separately from us or from another supplier.		Customer

BUSINESS APPLICATIONS

MICROSOFT OFFICE 365

REQUIREMENT	RESPONSIBILITY	
Register a suitable domain name with an accredited domain name registrar and pay all charges associated with the registration and maintenance.		Customer
Configure spam filtering rules.		Customer
Manage email and mailbox size.		Customer
Manage email volume to stay below your storage allowance.		Customer
Review suspected spam sent to your junk mail folder.		Customer
Move incorrectly classified emails from the junk folder to your mailbox.		Customer

ENTERPRISE APPLICATIONS

MICROSOFT EXCHANGE MAIL

REQUIREMENT	RESPONSIBILITY	
Register a suitable domain name with an accredited domain name registrar and pay all charges associated with the registration and maintenance.		Customer
Configure spam filtering rules.		Customer
Manage email and mailbox size.		Customer
Manage email volume to stay below your storage allowance.		Customer
Review suspected spam sent to your junk mail folder.		Customer
Move incorrectly classified emails from the junk folder to your mailbox.		Customer

CLOUD COLLABORATION – MICROSOFT

MICROSOFT EXCHANGE, SHAREPOINT AND LYNC

REQUIREMENT	RESPONSIBILITY	
Manage service availability, monitoring and support.	Telstra	
Register a suitable domain name with an accredited domain name registrar and pay all charges associated with the registration and maintenance.		Customer
Configure spam filtering rules.		Customer
Manage users, resources, mailboxes and distribution lists (via Telstra portal)		Customer
Manage email and SharePoint volume to stay below your storage allowance.		Customer
Desktop client software (such as Microsoft Outlook)		Customer
Create and manage SharePoint site collections and content		Customer

CHAPTER 3
INFRASTRUCTURE

VIRTUAL SERVER (SHARED)

REQUIREMENT	RESPONSIBILITY	
Install and maintain the platform software that you will use to create and administer your virtual server instances.	Telstra	
Allocate and configure public subnets and address ranges for your virtual server environment.	Telstra	
Create virtual server instances.	Telstra	
Install virtual server operating system(s), software and agents.	Telstra	
Analyse and install selected security fixes and operating system hot fixes applicable to your virtual server(s).		Customer
Manage the operating system software configuration and maintenance of your virtual server(s).		Customer
Check and correct operating system-related errors applicable to your virtual server(s).		Customer
Maintain any documentation related to virtual server configuration management and operational and recovery procedures for the operating system applicable to your virtual server(s).		Customer
STORAGE		
Monitor your virtual server's data storage capacity and request increases if required.		Customer
Create your own file systems, databases or applications that utilise the storage capacity.		Customer
Remove all your data from storage before deleting a server.		Customer
BACKUP		
At your request, notify you by email when we've successfully restored your data.	Telstra	

Periodically test application recovery processes and procedures to make sure you can recover your application environment in the event of a major system failure or data corruption.		Customer
Request for us to restore backups subject to any restoration limitations applicable to the virtual server configuration.		Customer
Regularly test any recovery plan you may have that is dependent upon backup restoration.		Customer
Install compatibility software or hardware on your servers to activate backups.		Customer
Update compatibility software or hardware when required.		Customer

CLOUD AND TAILORED INFRASTRUCTURE – GENERAL

REQUIREMENT	RESPONSIBILITY	
Notify you of planned infrastructure changes.	Telstra	
Apply change control practices to all in-scope infrastructures.	Telstra	
Issue notification of planned infrastructure changes.	Telstra	
Select, purchase, install and maintain the physical service infrastructure.	Telstra	
Select, purchase, install and maintain the platform software that enables the operation of your server(s) and associated infrastructure.	Telstra	
Periodically update hypervisors and firmware to ensure the platform supports current operating systems or software for your virtual server instances.	Telstra	
Monitor and respond to errors and failures related to the physical service infrastructure.	Telstra	
Monitor and respond to errors and failures related to the platform software that enables operation of your server(s).	Telstra	
Manage the operating system file system structures, log files and available storage capacities applicable to your server(s).		Customer
Remove all your data from storage before deleting a server.		Customer
Maintain valid licenses for all software and/or software license keys you provide.		Customer

Load and manage your data.		Customer
STORAGE		
Submit a request to change the amount of storage your server(s) require.		Customer
Create your own file systems, database or applications that use the storage service.		Customer
Remove all your data from storage before you request storage de-allocation.		Customer
Nominate one of your dedicated server(s) to act as a directory server if you require the use of a data import storage device as part of your Cloud Services solution.		Customer
BACKUP		
Request additional detailed back up and restoration requirements.		Customer
Specify the period of time in which a backup should commence.	Telstra	
Notify you by email of scheduled back up success/failure.	Telstra	
At your request, notify you by email when we've restored and loaded your data.	Telstra	
Periodically test application recoverability processes and procedures to ensure you can recover your data in the event of a system failure.		Customer
Install compatibility software or hardware on your servers to activate backups.		Customer
Update compatibility software or hardware when required.		Customer
Notify you of any specific procedures required to back up your data.	Telstra	
Initiate ad hoc backup of your designated data files.		Customer
Initiate restoration of backups older than three months as required.	Assist	Customer
Initiate restoration of backups up to three months old as required.		Customer
Regularly test any recovery plan you may have that is supported by back up.		Customer
Consult with us before updating or upgrading your application environment.		Customer

NETWORK		
Monitor the internet connection capacity utilisation and create additional capacity as required by the customer's total usage.	Telstra	
Determine the IP addressing scheme for your private network connection to Cloud Services.	Telstra	
Allocate, configure and test public and/or private IP addresses.	Telstra	
Resolve IP address conflicts involving our allocated IP addresses to you.	Telstra	
Reclaim IP addresses upon release by you or by termination/expiration of your contract.	Telstra	

VIRTUAL SERVER (DEDICATED)

REQUIREMENT	RESPONSIBILITY	
Create virtual server instances.		Customer
Install virtual server operating system(s), software tools and agents.		Customer
Analyse and install selected security fixes and operating system hot fixes applicable to your virtual server(s).		Customer
Manage the operating system software configuration and maintenance applicable to your virtual server(s).		Customer
Check and correct operating system-related errors applicable to your virtual server(s).		Customer
Maintain required documentation for server configuration management, operational and recovery procedures for the operating system applicable to your virtual server(s).		Customer
Complete a service request to prioritise any Telstra-planned upgrade to VMware software, such as VCenter Server, for your virtual server(s) to support your operating system software configuration		Customer
Consult with us before updating or upgrading your application environment.		Customer
Determine and provide us your storage capacity utilisation thresholds.		Customer
Monitor your capacity utilisation and notify you if your specified thresholds are exceeded.		Customer

HYBRID DISASTER RECOVERY		
Provide disaster recovery infrastructure.		Customer
Ensure sufficient failover storage at disaster recovery site.		Customer
Provision at least one virtual server dedicated to the Hybrid Disaster Recovery service at both the primary and disaster recovery site with specifications that support the service's software.		Customer
Install Hybrid Disaster Recovery software onto servers in both the primary and disaster recovery environments.		Customer
Release Hybrid Disaster Recovery software upgrades into customer environments.	Telstra	
Ensure connectivity at the primary and disaster recovery site, including ensuring the servers hosting the disaster recovery software are always on and available.	Telstra	Customer
Set up a disaster recovery plan via the disaster recovery console, including activating the service and selecting and pairing which servers to protect.		Customer
Test disaster recovery plan.		Customer
Provide technical support if software, data replication, restoration or installation fails.	Telstra	
For tailored infrastructure customers, to provide Telstra with service pre-activation requirements before activation, including VMware® vCenter Server™ IP addresses and private network range details.		Customer
For a customer wishing to purchase the service for a tailored infrastructure environment, ensure the customer's virtual server (dedicated) service has the required communication with the Hybrid Disaster Recovery management environment and VMware® vCenter Server™.	Telstra	

VIRTUAL SERVER (DEDICATED) GEN2

REQUIREMENT	RESPONSIBILITY	
Create virtual server instances.		Customer
Install virtual server operating system(s), software tools and agents.		Customer
Analyse and install selected security fixes and operating system hot fixes applicable to your virtual server(s).		Customer
Manage the operating system software configuration and maintenance applicable to your virtual server(s).		Customer
Check and correct operating system-related errors applicable to your virtual server(s).		Customer
Maintain required documentation for server configuration management, operational and recovery procedures for the operating system applicable to your virtual server(s).		Customer
Complete a service request to prioritise any Telstra-planned upgrade to VMware software, such as VCenter Server, for your virtual server(s) to support your operating system software configuration		Customer
Consult with us before updating or upgrading your application environment.		Customer
Determine and provide us your storage capacity utilisation thresholds.		Customer
Monitor your capacity utilisation and notify you if your specified thresholds are exceeded.		Customer

MANAGED VIRTUAL SERVER (DEDICATED) - *EXCLUDES GEN2*

This solution is available at data centres in Australia, London, Hong Kong and Singapore, but not available to Telstra Global customers.

REQUIREMENT	RESPONSIBILITY	
Create virtual server instances.	Telstra	
Install virtual server operating system(s), software tools and agents.	Telstra	
Analyse and install selected security fixes and operating system hot fixes applicable to your virtual server(s).	Telstra	

Manage the operating system software configuration and maintenance applicable to your virtual server(s).	Telstra	
Check and correct operating system-related errors applicable to your virtual server(s).	Telstra	
Maintain required documentation for server configuration management, operational and recovery procedures for the operating system applicable to your virtual server(s).	Telstra	
Consult with us before updating or upgrading your application environment.		Customer
Determine and provide us your storage capacity utilisation thresholds.		Customer
Monitor your capacity utilisation and notify you if your specified thresholds are exceeded.	Telstra	

MANAGED PHYSICAL SERVER (DEDICATED)

REQUIREMENT	RESPONSIBILITY	
Install physical server operating system(s), software tools and agents.	Telstra	
Analyse and install selected security fixes and operating system hot fixes applicable to your physical server(s).	Telstra	
Analyse and install selected security fixes and operating system hot fixes applicable to your virtual server(s).	Telstra	
Manage the operating system software configuration and maintenance applicable to your physical server(s).	Telstra	
Check and correct operating system related errors applicable to your physical server(s).	Telstra	
Manage the operating system software configuration and maintenance applicable to your physical server(s).	Telstra	
Check and correct operating system related errors applicable to your physical server(s).	Telstra	
Manage the operating system software configuration and maintenance applicable to your physical server(s).	Telstra	
Check and correct operating system related errors applicable to your physical server(s).	Telstra	
Consult with us before updating or upgrading your application environment.	Telstra	

Determine and provide us your storage capacity usage thresholds.		Customer
Monitor your capacity usage and notify you if your specified thresholds are exceeded.	Telstra	
SECURITY		
Create and manage login accounts for users of the management console.	Telstra	
Access and customise reports via the management console.		Customer
Log any firewall configuration and/or policy changes within management console.		Customer
Configure firewall hardware and software to the relevant specifications.	Telstra	

CHAPTER 4
SOFTWARE

SOFTWARE PURCHASED FROM A THIRD PARTY

There are a number of rules and requirements around manually installing and managing your existing software or adding pre-installed software to your cloud solution.

REQUIREMENT	RESPONSIBILITY	
Install and configure your software.		Customer
Manage installation, configuration and maintenance of your software.		Customer
Ensure your software is compatible with the operating system installed on your server(s).		Customer
Check and correct software-related errors applicable to your server(s).		Customer
Maintain required documentation for configuration management, operational and recovery procedures for applications on your server(s).		Customer
Periodically test recovery processes and procedures to ensure you can recover your software in the event of a major system failure or data corruption.		Customer
Manage directory services such as user accounts, access privileges and passwords for users of your server(s) and applications.		Customer

SOFTWARE PURCHASED THROUGH TELSTRA FOR YOUR VIRTUAL SERVER (SHARED) AND MANAGED VIRTUAL SERVER (DEDICATED) SOLUTION

There are a number of rules and requirements around ordering and managing the software you've purchased from us via the Cloud Services management console and that we install on your cloud infrastructure. Once you've submitted an installation request to us, we install the software on your nominated virtual server(s) within three business days for the **virtual server (shared)** service and within four business days for the **managed virtual server (dedicated)** service.

REQUIREMENT	RESPONSIBILITY	
Request software and provide the correct parameters to assist the software installation. Parameters may include the number of server(s) the software will be installed on, operating system credentials and number of users.		Customer

Install software based on the parameters you've provided.	Telstra	
Before software is requested and installed, ensure any pre-requisites are met.		Customer
Manage configuration and maintenance of the software, including sourcing help for set-up, configuration, usage, upgrades and ongoing management of the software.		Customer
Check software faults applicable to server(s) and contact Telstra if there's an issue.		Customer
Report software faults to the software provider.	Telstra	
Ensure server(s) has sufficient resources (e.g. CPU, RAM and storage) for optimum software usage.		Customer
Request an increase or decrease to the number of users or CPU registered with the software.		Customer
Notify us whenever any Telstra-purchased software is uninstalled so we can cancel the software licence on your behalf and cease billing.		Customer
Ensure accurate reporting of software user numbers i.e. the number of users of a software service purchased through us must not exceed the number of users registered with us.		Customer
As an existing Microsoft Volume Licensing customer covered by Microsoft Software Assurance, submit a request for licence mobility to Microsoft and ensure Microsoft terms are adhered to.		Customer

CHAPTER 5
CLOUD SECURITY

SECURITY ON AND AFTER 15 SEPTEMBER 2014

REQUIREMENT	RESPONSIBILITY	
CUSTOMER SECURITY PORTAL		
Create login accounts for end users on the customer security portal		Customer
Manage login accounts for end users on the customer security portal		Customer
Access and customise reports via the customer security portal		Customer
Create login accounts for end users on the customer security portal		Customer
GATEWAY PROTECTION ADVANCED (GPA)		
Provide access to Cloud Infrastructure tenancy for Telstra staff for the installation of GPA and remove the access after the instrallation where the Cloud Infrastructure tenancy has been purchased by the customer.		Customer
Installation of GPA onto the Cloud Infrastructure tenancy	Telstra	
Ensure Cloud Infrastructure access credentials are not used to access or modify the GPA service by any other parties other than Telstra or partners identified by Telstra for the management of GPA		Customer
Undertake acceptance testing of the firewall configuration	Telstra	Customer
Log any configuration or policy changes within the customer security portal		Customer

Activating your Cloud Direct Connection / Cloud Gateway product to use GPA from your Next IP network service		Customer
Enabling the Internet usage on your Cloud Infrastructure service for your GPA service		Customer
Provide networking and security policy requirements for your GPA service		Customer
FIREWALL – VIRTUAL & DEDICATED		
Undertake acceptance testing of the firewall configuration	Telstra	Customer
Log any firewall configuration or policy changes within the customer security portal		Customer
Specify firewall settings such as ports, filters, traffic direction, rules and network address translations		Customer
Specify firewall VPN site-to-site and/or client-to-site IPSEC/SSL specifications		Customer
Configure firewall hardware and software to the relevant specifications as per design	Telstra	
Administer changes to the firewall	Telstra	
Inform the customer of intrusion vulnerabilities detected within their service	Telstra	
Schedule and apply changes to settings as needed to mitigate vulnerabilities within their service	Telstra	
Back up the specified firewall settings and restore settings in the event of a failure	Telstra	
INTRUSION PROTECTION - VIRTUAL		
Inform the customer of security events	Telstra	
Undertake acceptance testing of the IPS/IDS configuration	Telstra	Customer

Log any IPS/IDS configuration or policy changes within the customer security portal		Customer
Specify IPS/IDS settings (critical, medium, low event specifications)		Customer
Specify any network changes that may affect the IPS/IDS appliance		Customer
Configure IPS/IDS hardware and software to the relevant specifications as per design	Telstra	
Administer changes to the IPS/IDS appliance	Telstra	
Inform the customer of intrusion vulnerabilities detected within their service	Telstra	
Schedule and apply changes to settings as needed to mitigate vulnerabilities within their service	Telstra	
Back up the specified IPS/IDS settings and restore settings in the event of a failure	Telstra	
The customer will always be notified at least five days in advance by Telstra for schedule maintenance within the product, including the customer portal	Telstra	
Every second Sunday of every month, between 0.00am (midnight) – 12.00pm, maintenance may occur within the product, including on the customer portal. Notice of this maintenance will be provided to the customer primary point of contact.	Telstra	
Should emergency maintenance be required on the product or the customer portal, the customer primary point of contact will receive notification within 30 minutes of initialisation of the emergency maintenance and within 30 minutes of the completion of any emergency maintenance	Telstra	

INTRUSION PROTECTION – DEDICATED (Intrusion Protection – Dedicated is not available to new customers on and from 1 June 2015. We will continue to support adds, moves and changes for Intrusion Prevention (Dedicated) services existing prior to 1 June 2015 and which have not been cancelled.)		
Inform the customer of security events	Telstra	
Undertake acceptance testing of the IPS/IDS configuration	Telstra	Customer

Log any IPS/IDS configuration or policy changes within the customer security portal		Customer
Specify IPS/IDS settings (critical, medium, low event specifications)		Customer
Specify any network changes that may affect the IPS/IDS appliance		Customer
Configure IPS/IDS hardware and software to the relevant specifications as per design	Telstra	
Administer changes to the IPS/IDS appliance	Telstra	
Inform the customer of intrusion vulnerabilities detected within their service	Telstra	
Schedule and apply changes to settings as needed to mitigate vulnerabilities within their service	Telstra	
Back up the specified IPS/IDS settings and restore settings in the event of a failure	Telstra	
The customer will always be notified at least five days in advance by Telstra for schedule maintenance within the product, including the customer portal	Telstra	
Every second Sunday of every month, between 0.00am (midnight) – 12.00pm, maintenance may occur within the product, including on the customer portal. Notice of this maintenance will be provided to the customer primary point of contact.	Telstra	
Should emergency maintenance be required on the product or the customer portal, the customer primary point of contact will receive notification within 30 minutes of initialisation of the emergency maintenance and within 30 minutes of the completion of any emergency maintenance	Telstra	

FIREWALL AND INTRUSION PREVENTION SERVICE DEFINITION	
Simple policy change request acknowledgement	Customer notified at the time the customer requests the change via the online portal
Simple policy change request implementation	Customer notified from the time that Telstra acknowledges the customer's request for a change
Simple emergency policy change implementation	Customer notified from the time that Telstra acknowledge the customer's request for a change

Security incident alert notifications	Customer notified from the time that Telstra identifies a security incident
Device health alerting	Customer notified from the time that Telstra determines the customer's firewall service is not available
Content signature update (intrusion prevention service only)	Telstra will provide the customer with the valid security signatures from the time the update is published, as generally available by the vendor

FIREWALLS

FEATURES	VIRTUAL		DEDICATED	
	BASIC	ADVANCED^	BASIC	ADVANCED
Customer portal availability	99.9%	99.9%	99.9%	99.9%
Authorised security contacts	3 users	3 users	3 users	3 users
Log and event archival (data retention)	Up to 1 year	Up to 7 years	Up to 1 year	Up to 7 years
Simple policy change request (1)	2 per month	8 per month	2 per month	20 per month
Simple policy change request acknowledgement	2 hrs	2 hrs	2 hrs	2 hrs
Simple policy change request implementation (1)	24 hrs	8 hrs	24 hrs	8 hrs
Simple emergency policy change request	N/A	1 per month	N/A	1 per month
Simple emergency policy change implementation	N/A	2 hrs	N/A	2 hrs
Complex policy change request(1)	N/A	1 per month	N/A	1 per month
Device health alerting	N/A	NA	30 mins	15 mins
Security incident alert notifications	N/A	15 mins	30 mins	15 mins
Site-to-site VPN	N/A	Up to 100	2 tunnels (1)	Up to 100 (1)

FEATURES	VIRTUAL		DEDICATED	
	BASIC	ADVANCED^	BASIC	ADVANCED
Client-to-site VPN (IPSEC/SSL)	N/A	Up to 400	N/A	Up to 400 (1) (2) (3) (4)
Threat intelligence service	For 1 user	For 1 user	For 1 user	For 1 user
Vulnerability discovery	N/A	N/A	N/A	N/A
High availability	Yes	Yes	Yes	Yes
Out of band	N/A	N/A	Option	Option

^ Firewall Virtual Advanced is not available to new customers on and from 1 June 2015. We will continue to support adds, moves and changes for Firewall Virtual Advanced services existing prior to 1 June 2015 and which have not been cancelled.

INTRUSION PREVENTION

FEATURES	VIRTUAL	DEDICATED^
Customer portal availability	99.9%	99.9%
Authorised security contacts	3 users	3 users
Log & Event Archival (data retention)	Up to 7 years	Up to 7 years
Security event monitoring	Automated plus real-time 24x7 human analysis	Automated plus real-time 24x7 human analysis
Simple policy change request (1)	Fixed policy for all customers	Up to 20 per month
Simple policy change request acknowledgement	N/A	2 hrs
Simple policy change request implementation	N/A	8 hrs
Simple emergency policy change request via customer portal	N/A	1 per month
Simple emergency policy change implementation	N/A	2 hrs
Complex Policy Change Request via Customer Portal	N/A	1 per month
Device health alerting	N/A	15 mins

FEATURES	VIRTUAL	DEDICATED^
Security incident alert notifications	15 mins	15 mins
Content signature update	48 hrs	48 hrs
Threat intelligence service	For 1 user	For 1 user
Vulnerability discovery	N/A	N/A
High availability	Yes	Yes
Out of band	N/A	Option

^ Intrusion Protection – Dedicated is not available to new customers on and from 1 June 2015. We will continue to support adds, moves and changes for Intrusion Prevention (Dedicated) services existing prior to 1 June 2015 and which have not been cancelled.

N/A - Not applicable
(1) All policy changes to be submitted via the online customer portal.
(2) VPN tunnels are based on the device capabilities – refer to vendor specifications.
(3) Client-to-site VPN (IPSEC/SSL) support: customer is responsible for management, administration and end-user support issues, including the installation of the VPN client software and software socialability testing on your endpoint. Note: SSL is vendor-dependent and may not be available on certain firewall types. Only IPSEC is available on the virtual firewall.
(4) Only five client-to-site profiles are included in the deployment.

SECURITY PRIOR TO 15 SEPTEMBER 2014

CONTENT SECURITY

FEATURES	STANDARD PLAN
Configuration changes policy	4 (per month)
Change requests are implemented during a fixed change window	✓

FIREWALLS

FEATURES	VIRTUAL		DEDICATED	
	STANDARD	SELECT	STANDARD	SELECT
Configuration changes policy	2	8	2	Unlimited
Emergency policy or configuration changes	N/A	2 (per month)	N/A	1 (per month)
Data storage retention period	1 year	Up to 7 years	1 year	Up to 7 years

FEATURES	VIRTUAL		DEDICATED	
	STANDARD	SELECT	STANDARD	SELECT
Quarterly vulnerability assessment	N/A	N/A	1 device	3 devices
Site-to-site VPN connections	2	Unlimited	2	Unlimited
Available on some platforms	No	✓	No	✓
Site-to-client VPN support	N/A	N/A	Available as an option	✓
Excluding end user support	N/A	N/A	Yes, standalone option not in conjunction with virus filtering or SPAM filtering	✓
Security event monitoring available when using firewall equipment which supports deep packet inspection or an IPS blade	1 seat	1 seat	1 seat	1 seat
Internal web, virus and SPAM filtering licence	✓	✓		

INTRUSION PROTECTION

FEATURES	VIRTUAL	DEDICATED (NETWORK)		DEDICATED (HOST)	
	SELECT	STANDARD	SELECT	STANDARD	SELECT
Security event monitoring including real time 24/7 human analysis on the Select plan	✓	✓	✓	✓	✓
Policy or configuration changes made through the online portal	N/A	2 changes per month	Unlimited	2 changes per month	Unlimited
Data storage retention period	Up to 7 years	1 year	Up to 7 years	1 year	Up to 7 years
Quarterly vulnerability assessment	N/A	1 device	2 devices	N/A	N/A
Threat analysis and intelligence service through one of your nominated customer portal accounts	1 seat	1 seat	1 seat		N/A

FEATURES	VIRTUAL	DEDICATED (NETWORK)		DEDICATED (HOST)	
	SELECT	STANDARD	SELECT	STANDARD	SELECT
Change requests are implemented during a fixed change window from 1AM to 3AM each Sunday and Wednesday (AEST)	✓				

VPN

FEATURES	STANDARD PLAN
Configuration changes policy	4 (per month)
Change requests are implemented during a fixed window from 1AM to 3AM each Sunday and Wednesday (AEST)	✓

DEDICATED DISASTER RECOVERY

REQUIREMENT	RESPONSIBILITY	
Business impact assessments		Customer
Business continuity and disaster recovery plans and policies beyond the disaster recovery service		Customer
Update and communicate changes to the disaster recovery plan		Customer
Maintain a copy of the disaster recovery plan	Telstra	
Update and maintain the *Site Recovery Manager Configuration Guide*	Telstra	
Notify Telstra of contact names and numbers of people authorised to request a failover, and ensure details are kept up to date		Customer
Monitor and alarm disaster recovery-protected servers at their current active site	Telstra	
Perform the failover of disaster recovery-protected servers to the paired distant second site in the event of a disaster	Telstra	

Application readiness for disaster and application failover		Customer
Notify Telstra if you make a change that impacts your disaster recovery service and ensure disaster recovery plans are updated		Customer
Protect the disaster recovery service during platform changes and update disaster recovery plans if required	Telstra	
Request a failover test through a service request		Customer
Perform the failover of disaster recovery-protected servers in the event of a catastrophic disaster, prior to customer authorisation	Telstra	

SAN REPLICATION

REQUIREMENT	RESPONSIBILITY	
Replication of data to the paired distant second site	Telstra	
Application readiness for disaster and application failover		Customer
Request failover to second site through a service request		Customer
Request failover test through a service request		Customer
Provide instructions for failover		Customer

CHAPTER 6
DATA CENTRES

COLOCATION

Refer to the Colocation User Guide for more information.

REQUIREMENT	RESPONSIBILITY	
Install cabinet service.	Telstra	
Install equipment into the customer rack.		Customer
Successfully complete the online Telstra network induction. The online Physical Security course must be successfully completed every three years.		Customer
Attend the relevant colocation data centre's on-site induction briefing.		Customer
Nominate each one of your employees, consultants and contractors who are authorised to access their specific racks. Maintenance of customer access lists is your sole responsibility.		Customer
Submit power deployment requests to us for approval. (Addition, removal or relocation of equipment within your racks.)		Customer
Submit equipment lists and specifications to us (initial installation and any subsequent changes).		Customer
Equipment, connections, cabling or material updated or installed in a data centre managed by us should be: • Outlined in the application form • Specified to the service desk in time for scheduled data centre visits, and presented, identified and logged with our staff and/or site security guard • Labelled with your name (and we may need you to apply, maintain and update other labels on or near the customer equipment) • Operating in accordance with all electrical, heat and telecommunications standards and any other standards that apply • Registered with us and approved by Telstra Cloud Services product management in advance (you must supply us with all information about the customer equipment) • Operating in accordance with the site specifications and other reasonable requirements that we need from time to time.		Customer
Review and approve the customer equipment list.	Telstra	Assist

Cabling between or external to your racks.	Telstra	
Cabling wholly within your racks (approved customer cabling).		Customer
Install, setup, administer and maintain customer equipment.		Customer
Customer to ensure their equipment does not exceed their site specifications.		Customer
Ship customer equipment to our managed data centre(s).		Customer
Manage your colocation power consumption within your contracted power allocation. If you exceed your contracted power allocation you will be charged $1,000 (plus GST) per 0.5KVA over your contracted power allocation.		Customer

CHAPTER 8
DEFINITIONS

ITEM	DESCRIPTION
Business day	As defined in Our Customer Terms to mean: any day other than a Saturday, Sunday or recognised public holiday in the capital city of the Australian state or territory in which your premises are located.
Our data centres	Our data centres are located in: • Sydney (Pitt Street, Ultimo, Homebush and St Leonards) • Melbourne (Exhibition Street, Box Hill and Clayton) • Perth (Wellington) • Brisbane (Woolloongabba) We also own and/or operate other data centres from time to time.
Our Customer Terms	Our Customer Terms set out the terms and conditions relating to how we provide virtual server plans, products and services. They also outline the terms and conditions for other broader services in the Cloud Services portfolio.
Service desk	Our service desk can be contacted on 1800 620 345 Monday to Friday, 9AM to 5PM (AEST) or email any questions to ***cloudservices@team.telstra.com***. For general technical support, call 1800 620 345 or email any questions to ***cloudservicessupport@online.telstra.com.au***. Technical support is available 24/7.