TELSTRA CLOUD SERVICES RESPONSIBILITIES GUIDE

V12.0

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 12.0

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	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

MANAGED VIRTUAL SERVER (DEDICATED)

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
NETWORK SERVICES

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 7
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)		
PREPARATION FOR THE ACTIVATION OF GPA		
Provide authorised Telstra personnel access to Cloud Infrastructure tenancy (incl. vCenter Server) for the installation of GPA. Remove the access after the installation (where the Cloud Infrastructure tenancy has been purchased by the customer).		Customer
Ensure Cloud Infrastructure access credentials are not used to access or modify the GPA service by any parties other than Telstra or partners authorised by Telstra for the management of GPA.		Customer
To use the GPA solution, ensure connectivity is activated on your Cloud Gateway service between your Telstra IP network and your Cloud Infrastructure		Customer
Support activation of Cloud Gateway between your Telstra IP network and your Cloud Infrastructure to use the GPA solution.	Telstra	

<table>
<tr><td>Make available two blades in the Cloud Infrastructure Virtual Server (Dedicated) Gen2 tenancy for the installation of the GPA virtual appliance Next Generation Firewalls in a High Availability configuration.</td><td></td><td>Customer</td></tr>
<tr><td>Provide an adequate allocation of virtual server (VM) resources on Cloud Infrastructure Virtual Server (Dedicated) Gen2 blades for the installation and operation of the GPA product.
2 x virtual servers (VMs) with each VM having a minimum allocation of:<table><tr><th>Resources</th><th>Small GPA</th><th>Medium GPA</th></tr><tr><td>Cores (dedicated physical/virtual)</td><td>2</td><td>4</td></tr><tr><td>RAM (GB)</td><td>6.5</td><td>10</td></tr><tr><td>Storage (GB)</td><td>60</td><td>60</td></tr></table>
Each of the two virtual server (VMs) to be deployed onto 2 x separate blades (hosts) within a tenancy/cluster.</td><td></td><td>Customer</td></tr>
<tr><td>Provide the means to capture the Cloud Infrastructure networking requirements and the security policies (“Detailing workbook”) to configure the GPA product at initial setup.</td><td>Telstra</td><td></td></tr>
<tr><td>Provide the Cloud Infrastructure networking requirements and security policies (“Detailing workbook”) to configure the GPA product at initial setup.</td><td></td><td>Customer</td></tr>
<tr><td>Assign a single point of contact to manage the delivery of the GPA solution.</td><td>Telstra</td><td></td></tr>
<tr><td>Conduct a project kickoff meeting/workshop and provide a delivery plan for the GPA solution.</td><td>Telstra</td><td></td></tr>
<tr><td>Agree on and approve a timeline for GPA onboarding.</td><td>Telstra</td><td>Customer</td></tr>
<tr><td>Provide a set of predefined standard GPA design templates.</td><td>Telstra</td><td></td></tr>
<tr><td>Select a design from a predefined set of standard GPA templates or develop/agree customised design.</td><td>Telstra</td><td>Customer</td></tr>
<tr><td>Onboarding of GPA</td><td></td><td></td></tr>
<tr><td>Provide test cases to verify the configuration of the GPA product for onboarding.</td><td></td><td>Customer</td></tr>
</table>

Ensure that Telstra Cloud Infrastructure Virtual (Dedicated) Gen2 has been appropriately configured to announce a default route on private network for the GPA product.		Customer
Provide support for the onboarding of the GPA product that may include, but is not exclusive of: • access to technical teams • project support • change control aprovals • organisation change communications • management support.		Customer
Provide confirmation that access and onboarding requirements are sufficient for the onboarding of the GPA product.	Telstra	
Install GPA onto the Cloud Infrastructure tenancy.	Telstra	
Implement the networking and security policies (“Detailing workbook”) to configure the GPA product provided at initial setup.	Telstra	
Implement the Next Generation Firewall components of the GPA product in a High Availability with Active/Standby configuration.	Telstra	
Provide (at initial setup) all requirements for the GPA service which may include, but is not limited to: firewall configuration, customer network infrastructure access/information, Active Directory (AD) account info (user name, password, domain, base/bind DN, Active Directory servers, IP addresses), Active Directory profiles, tunnel details, endpoint details, mobile security details and any applicable certificates.		Customer
Configure the firewall for external authentication using customer network infrastructure and customer supplied authentication/Active Directory information/certificates.	Telstra	
Configure the firewall for Mobile Security gateway using customer network infrastructure and customer supplied authentication/Active Directory information/certificates.	Telstra	
Configure the firewall for GlobalProtect Portal customer network infrastructure and customer supplied authentication/Active Directory information/certificates.	Telstra	

Configuration of firewall to enable Mobile Security clients using customer customer network infrastructure and customer supplied authentication/Active Directory information/certificates.	Telstra	
Configure firewall to enable Mobile Devices Management using customer network infrastructure and customer supplied authentication/Active Directory information/certificates.	Telstra	
Configure firewall to enable Host Information Profiling using customer network infrastructure and customer supplied authentication/Active Directory information/certificates.	Telstra	
Implement Palo Alto firewall generated certificates at initial integration (if required).	Telstra	
Set up and manage any hardware/software outside of the firewall e.g. customer network, appliances, servers, and endpoint clients/agents particularly defining authentication and tunnelling configurations.		Customer
Provide all information required for firewall configuration, incuding customer network infrastructure access/information, Active Directory account info (username, password, domain, base/bind DN, AD servers IP addresses etc), Active Directory profiles, tunnel details, endpoint details, and any applicable certificates.		Customer
Define and provide (at setup) all security policies that need to be implemented.		Customer
For GlobalProtect related issues or escalations, nominate an authorised person to act as a single point of contact. For example, an IT help desk staff member or administrator for enterprise users.		Customer
Provide first-level support for enterprise users in relation to GlobalProtect client software installed on their endpoint devices.		Customer

Configuration of customer network infrastructure (e.g. authentication servers, certificates etc.) and smart device apps.		Customer
Download, update and manage mobile device security agent (both laptop client and smart device apps).		Customer
Undertake acceptance testing of the GPA implementation from point of handover.		Customer
Complete all acceptance testing and provide signoff of the implemented design within 10 days after the date of handover of the GPA product.		Customer
Provide up to 10 days of support during acceptance testing.	Telstra	
Provide support for the cutover of the GPA product.	Telstra	
Provide a user guide for the GPA product.	Telstra	
Facilitate a one-hour administration workshop (not including Palo Alto Network appliance training) for up to three administrators on functionality of the GPA user interface. Delivered via a web virtual meeting.	Telstra	
Arrange and undertake required training on GPA web interface and administration.		Customer
Provide sign-off on the conclusion of the GPA product onboarding.		Customer
Start billing for GPA solution after completion of acceptance test period.	Telstra	
Configure any products or services that may interact with, but are not part of, the GPA prouct which may include: • External directory servers • Customer-owned networks • Customer-owned Telstra Virtual Server (Dedicated) Gen2 • SIEM integration • Load-balancing configurations		Customer
GPA ONGOING MANAGEMENT		
Apply any configuration or policy changes within the customer security portal.		Customer

Provide details of any **essential security policies and configuration items** required for the GPA product to operate in accordance with defined specification and service levels.	Telstra	
Ensure that the **essential GPA security policies and configuration items (refer to**"Detailing workbook"- DO NOT Touch items) are not modified at any time during the lifetime of the service.		Customer
Ensure that **essential configuration items** in Telstra Cloud Infrastructure Virtual (Dedicated) Gen2 required to provide the GPA service are maintained and not modified or changed at any time during the lifetime of the GPA service.		Customer
Monitor the GPA product for availability and capacity management purposes and undertake any required software patching of the Next Generation Firewall components.	Telstra	
Monitor the security policies implemented on the GPA product.		Customer
GPA SUPPORT		
Report any faults with your GPA product via Telstra Cloud Services support.		Customer
POLICY CHANGE AND CONFIGURATION MANAGEMENT (PCCM)		
PCCM ONBOARDING ACTIVITIES		
Provide an access method to submit PCCM requests.	Telstra	
Provide details of the PCCM change request process and procedures in the user guide.	Telstra	
Commence billing for PCCM on service activation.	Telstra	
PCCM ONGOING MANAGEMENT		

Log any PCCM requests as per access method and details specified.		Customer
Specify settings, such as ports, filters, traffic direction, rules and network address translations for the firewall policy.		Customer
Specify VPN tunnels: site-to-site IPSEC and client-to-site IPSEC/SSL specifications.		Customer
Apply policy change and configuration as per PCCM request.	Telstra	
Advise Telstra of any changes to your product contact notifications for requests.		Customer
Test completed changes.		Customer
Provide sign-off on completion of PCCM changes.		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 in a customer's service.	Telstra	
Back up the specified firewall settings and restore settings in the event of a failure.	Telstra	
INTRUSION PROTECTION - VIRTUAL & DEDICATED		

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 in 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 scheduled maintenance within the product, including the customer portal.	Telstra	
Every second Sunday of each month, between 0.00am (midnight) – 12.00pm (midday), maintenance may occur within the product, including on the customer portal. Notice of this maintenance will be provided to the customer's primary point of contact.	Telstra	
Should emergency maintenance be required on the product or the customer portal, the customer's 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

FEATURES	VIRTUAL		DEDICATED	
	BASIC	ADVANCED	BASIC	ADVANCED
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)
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

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

FEATURES	VIRTUAL	DEDICATED
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
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

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
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

FEATURES	VIRTUAL	DEDICATED (NETWORK)		DEDICATED (HOST)	
	SELECT	STANDARD	SELECT	STANDARD	SELECT
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
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	

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.